DELAWARE STATE BAR ASSOCIATION

CONTINUING LEGAL EDUCATION

DNA: DO NOT ACCESS OR DON'T NEED APPROVAL?

LIVE DSBA SEMINAR WITH ZOOM OPTION

SPONSORED BY THE DELAWARE STATE BAR ASSOCIATION

TUESDAY, DECEMBER 13, 2022 | 2:00 P.M. – 4:00 P.M.

2.0 Hours CLE credits with 0.5 Hour in Enhanced Ethics for Delaware and Pennsylvania Attorneys

ABOUT THE PROGRAM

As DNA databases continue to grow, law enforcement and prosecutors are finding a treasure of information help solve current crimes and cold cases. The Founding Fathers never imagined the scenarios by which an individual's right to privacy or to legal search and seizure might be implicated by this fast-moving area of evidence and law. Join a panel of the best criminal minds in Delaware as they explore the various investigative techniques, suppression issues, and admissibility arguments. This seminar will take an in-depth look at the leading Delaware cases and persuasive law from other states. Program Highlights: Suppression Motions; Introduction of the Technology and Rise of DNA testing through Genealogical Sites as an Investigative Technique; Case Law: DNA, Daubert, Cellular, Geofences; Issues for the Future; Q & A.

CLE SCHEDULE

Topics

DNA: Do Not Access or Don't Need Approval? A look at the Rising Law Surrounding DNA Information 2022

Familial DNA/ Genealogy /sites and the 4th Amendment

Moderator

The Honorable Jan R. Jurden, President Judge
Superior Court of the State of Delaware

Panelists

Kevin J. O'Connell, Esquire
Chief Defender
Office of Defense Services of the State of Delaware

Thomas A. Pedersen, Esquire
Thomas A. Pedersen, Attorney at Law

Sonia Augusthy, Esquire
Office of Defense Services of the State of Delaware

John S. Taylor, Esquire
Delaware Department of Justice of the State of Delaware

Jenna R. Milecki, Esquire
Delaware Department of Justice of the State of Delaware

Matthew C. Bloom, Esquire
Delaware Department of Justice of the State of Delaware

Visit https://www.dsba.org/event/dna-do-not-access-or-dont-need-approval-2022/ for all the DSBA CLE seminar policies.

Please note that the attached materials are supplied by the speakers and presenters and are current as of the date of this posting.

Moderator

The Honorable Jan R. Jurden, President Judge
Superior Court of the State of Delaware

Jan R. Jurden, President Judge, Superior Court of Delaware

The Honorable Jan R. Jurden, a Delaware native, was appointed President Judge of the Superior Court of Delaware in 2015. After proudly serving three years in the United States Army overseas following high school, PJ Jurden received her B.A. *summa cum laude* from Muhlenberg College in 1985, and her J.D. from the Dickinson School of Law in 1988, where she was an Articles Editor of the *Dickinson Law Review*. Judge Jurden joined the Superior Court bench in 2001 after practicing law for 13 years with the law firm of Young, Conaway, Stargatt & Taylor. Judge Jurden launched the first felony Mental Health Court in Delaware (which she presided over for nine years), is founder and Chair of the Sisters in Success Program, Vice-Chair of the Human Trafficking Interagency Council, Chair of the Criminal Justice Special Needs Population Committee, and a member of the Domestic Violence Coordinating Council and Criminal Justice Council. She is actively involved in criminal justice mental health, Veterans' Treatment Court and Community Court initiatives.

Panelists

Kevin J. O'Connell, Esquire
Chief Defender
Office of Defense Services of the State of Delaware

Thomas A. Pedersen, Esquire
Thomas A. Pedersen, Attorney at Law

Sonia Augusthy, Esquire
Office of Defense Services of the State of Delaware

Panelists

John S. Taylor, Esquire
Delaware Department of Justice
of the State of Delaware

Jenna R. Milecki, Esquire
Delaware Department of Justice
of the State of Delaware

Matthew C. Bloom, Esquire
Delaware Department of Justice
of the State of Delaware

December 13 CLE – Speaker Bios

Sonia Augusthy lives and works in Wilmington. For the past three years, she has been working as an assistant public defender with the Office of Defense Services. Prior to that, she worked for the Delaware Department of Justice for eleven years, serving in various roles within the Criminal Division and ending her time in the office with the Civil Rights and Public Trust Division. She earned her Juris Doctor from The Delaware Law School.

Matthew Bloom is a Deputy Attorney General and the Assistant Unit Head for the Appeals Unit at the Delaware Department of Justice, where he represents the State in criminal post-conviction matters, including direct appeals, motions for post-conviction relief, and federal habeas corpus proceedings. Since joining the Appeals Unit in 2019, Mr. Bloom has written briefs implicating constitutional issues and argued appeals before the Delaware Supreme Court. Prior to joining the Appeals Unit, Mr. Bloom prosecuted felony trials in New Castle County from 2016 to 2019 and managed the misdemeanor criminal and traffic calendars in the Court of Common Pleas from 2015 to 2016. Before joining the Delaware DOJ, Mr. Bloom worked in the corporate litigation section of Young Conaway Stargatt & Taylor in Wilmington. He graduated from the University of Virginia School of Law in 2012 and the University of North Carolina at Chapel Hill in 2009.

Jenna Milecki is a Deputy Attorney General at the Delaware Department of Justice and is the current Unit Head of the Domestic Violence Unit. She has worked as a prosecutor in New Castle County, Delaware since graduating from Widener Law School in 2012. During her time at the DOJ, she has tried cases in various units within the office, ranging from misdemeanor offenses to sexual assault and homicide cases. In her current position, she handles domestic violence felony cases, as well as the supervision of domestic violence prosecutors who handle intimate partner and familial violence cases and child abuse cases in Superior Court, Family Court, and the Court of Common Pleas. She also addresses issues in domestic violence cases throughout the State. In her time in the Special Victims Unit and in her current position in the Domestic Violence Unit, she has

focused her career on the protection of vulnerable victims, including women and children. She hopes to continue to support victims in the cases she prosecutes and to improve the criminal justice process for those affected by crime.

Kevin O'Connell is the Chief Defender of the Office of Defense Services. He has been with ODS since 2005. Prior to that, Kevin was in private practice where he was engaged primarily in criminal defense. Kevin has been a member of the Delaware bar since 1984. He is a proud graduate of Concord High School, Vanderbilt University and The Delaware Law School.

Tom Pedersen is a criminal defense attorney, representing clients from his office in Georgetown, Delaware. He has been a criminal defense attorney since 1998, but he began his career working as a prosecutor from 1992 to 1998. Throughout his career, he has participated in numerous murder and death penalty cases, gaining valuable insight from both sides. He earned his Juris Doctor from Widener Law School, and his undergraduate degree from West Chester University.

J.S. Taylor is a Deputy Attorney General in the Criminal Division of the Delaware Department of Justice. He is currently assigned to the Homicide Unit. He has been a criminal prosecutor for nine years. He was previously a civil litigator at a boutique complex litigation firm here in Wilmington.

30 Geo. Mason U. Civ. Rts. L.J. 177

George Mason University Civil Rights Law Journal
Spring, 2020

Comment
Jennie F. O'Hara [a1]

Copyright © 2020 by George Mason University Civil Rights Law Journal Association; Jennie F. O'Hara

23, ME, AND THE POLICE: THE FOURTH AMENDMENT IMPLICATIONS OF FAMILIAL DNA SEARCHING

INTRODUCTION

On April 24, 2018, a seventy-two-year-old man was escorted out of his Citrus Heights, California home in handcuffs. [1] This man, Joseph DeAngelo--now infamously known as the Golden State Killer--will likely spend what remains of his life in prison, finally paying for the rapes and gruesome murders of dozens of victims throughout the state of California in the 1970s and 80s. [2] DeAngelo's crimes had gone unsolved for over four decades, until savvy police investigators--still invested after all of that time--decided to experiment with a newly conceived investigatory technique: familial DNA searching. [3] Using this method, investigators were able to track down DeAngelo by matching DNA he had discarded at the scene of his crimes with the DNA of his distant relative, uploaded to a genealogy website. [4]

From this anecdotal scenario, it is simple to assume that familial DNA searching by police investigators can yield immeasurable positive outcomes. Although this may be true, it is also easy to imagine the myriad of ways in which law enforcement could weaponize this ***178** level of intrusion against the privacy rights of American citizens. Under the current Fourth Amendment framework, few safeguards are in place that would effectively protect the privacy rights of individuals who actively participate in public genealogy websites. [5] Furthermore, any existing state regulatory protections are sparse and highly varied. [6] In order for both law enforcement and the general public to benefit from the possibilities and potential advantages of familial DNA searching in criminal investigations, the government must implement uniform regulations. [7]

This Comment will suggest the implementation of federal legislation specifically designed to provide strict standards concerning familial DNA searching in criminal investigations. First, this Comment will discuss background concepts and information pertinent to the current framework of the Fourth Amendment as well as the modern use of DNA evidence generally. Specifically, Part I will discuss in detail the Golden State Killer case and investigation, including the use of familial DNA searching that led to DeAngelo's arrest. Part II will provide a historical overview of the use of DNA analysis in police investigation, including its current utility as an investigative tool. Part III will provide a general overview of Fourth Amendment jurisprudence, defining the scope of the law regarding search and seizure. Part IV will address the business operations of several popular genealogy websites, delving particularly into the privacy and general use disclosures supplied to people who utilize the websites' services. Part IV will also analyze the current landscape of federal regulation with regard to familial DNA testing of genealogy websites. Finally, Part V will conclude the background section by focusing on Colorado's familial DNA searching regulations and policies, as the leading state in terms of this technology.

Next, this Comment will analyze the Fourth Amendment implications surrounding the use of genetic information in the Golden State Killer investigation under the current regulatory scheme. This Comment will then apply the same facts to the Colorado model's framework to determine its effectiveness in real-world scenarios. Finally, this Comment concludes that it is necessary for Congress to enact further ***179** legislation to regulate the use of private individual genetic information at the federal level, and specifically suggests federal implementation of the Colorado model.

BACKGROUND

I. THE GOLDEN STATE KILLER

In the early morning hours of June 18, 1976, a twenty-three-year-old woman lay on the floor of her Rancho Cordova, California bedroom with her hands bound behind her back. [8] Despite her bindings, she was able to reach her telephone and call the police, to whom she recounted her horrific ordeal in vivid detail. [9] She stated that she awoke to a man "about five nine, moderately muscular, wearing a navy blue, short-sleeved T-shirt and gray canvas gloves" standing in the doorway of her bedroom, wearing a tight white ski mask to disguise his face. [10] This man went on to rape her before ransacking her home and fleeing the scene. [11] Investigators soon discovered that this man was careful and calculated in the planning and execution of his crimes. [12] They also discovered that he was incredibly cautious not to reveal his identity to his victims. [13]

This man's meticulous nature would prove effective, as this fateful night would go down in infamy as the beginning of his horrifying rampage throughout California over the next decade. [14] What began in 1972 as home invasions quickly turned into rapes, which became violent rapes and tortures, and, eventually, murders. [15] Because of the multi-jurisdictional nature of his crimes throughout California, investigators were initially unaware that they were perpetrated by a single offender. [16] This allowed the offender to commit his crimes undetected ***180** from 1972 to 1986 before inexplicably vanishing into thin air. [17] The elusive villain stalking California homes received many monikers during that span of time, including--"The Cordova Cat Burglar," "The Visalia Ransacker," "The East Area Rapist," and "The Original Night Stalker." [18] Decades later, after forty-two years, investigators across the state would finally learn that all of these widespread atrocities were the work of a single man: Joseph DeAngelo, the Golden State Killer. [19]

The last known crime attributed to the individual who would become the Golden State Killer occurred in 1986, an era of infantile forensic DNA technology. [20] Although the killer had "left his DNA all over the place" [21] at each crime scene, forensic analysts at the time did not possess the necessary technology to yield any viable leads. [22] It was not until 2011, after years of failed attempts, that police were able to use the DNA left at the crime scenes to create a general profile of the killer. [23] Nevertheless, this profile was not a match with any of the known felons in the Combined DNA Index System (CODIS), the Federal Bureau of Investigation's (FBI) DNA database. [24]

However, many who studied and investigated this case in great detail still believed that pursuing DNA evidence was the best way to "get out of the maze of the Golden State Killer." [25] One such individual was Michelle McNamara, the late author of the novel, *I'll Be Gone in the Dark: One Woman's Obsessive Search for the Golden State Killer*. [26] After McNamara suddenly passed away while writing this novel, her assistants and fellow researchers used compilations of her notes, research, and hard drives to continue her diligent work. [27] In ***181** those notes, McNamara stated that she believed one potentially fruitful path for DNA analysis was through familial DNA searching. [28] Her notes recognized that although CODIS could not match the crime scene DNA to the Golden State Killer himself, if a member of the perpetrator's family happened to be in the system, police could potentially see a match in trace DNA markers shared by close family members. [29] Even though this line of inquiry rendered no useful results at that initial stage, after just a few more years of dedicated research into the field of DNA technology, this idea would ultimately prove to be the key to solving the case. [30]

On April 24, 2018, just shy of forty-two years after the Golden State Killer's first attack, police in Citrus Heights--a suburb of Sacramento, California--arrested seventy-two-year-old Joseph DeAngelo in his home. [31] Under a familial DNA-driven line of inquiry, California law enforcement had developed a new tactic--familial searching through a "no-frills" site used by amateur genealogists called GEDmatch.com (GEDmatch). [32] Authorities began using GEDmatch, a public genealogical database used to search for relatives and ancestors online, after the traditional route of searching through state and federally run criminal DNA databases did not yield results. [33] According to longtime Contra Costa County District Attorney investigator Paul Holes, after authorities uploaded the Golden State Killer DNA profile to the site, they were able to obtain an extended list detailing the extent to which the DNA uploaded by various individuals on GEDmatch resembled the DNA of the killer--the closer the match in

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

DNA sequences, the more closely related the individuals are. [34] Because GEDmatch users willingly upload their DNA profiles to the site for public use, authorities did not need a court order to access the familial data. [35]

From these results, Chief Deputy District Attorney Steve Grippi stated that police were able to "zero in on DeAngelo" using a DNA ***182** profile uploaded by a distant relative. [36] Once authorities had a small pool of possible suspects derived from the public GEDmatch profiles, investigators used the results to explore these family trees and find men who were roughly the right age and height, and were living in California when the crimes occurred. [37] From this point, police were able to hone in on DeAngelo. [38] Specifically, investigators obtained samples of DeAngelo's DNA from his car door handle while he shopped at a local craft store, as well as from a tissue discarded in his trash. [39] Finally, after decades of tireless searching by authorities across the state of California, the Golden State Killer had a name and a face.

When news sources began to report that law enforcement used a public genealogy website to solve a murder investigation, the public's reaction to this revelation was mixed, at best. [40] A large portion of the populace seemed to have been unaware that the information uploaded to databases such as GEDmatch "could later be used to incriminate a relative." [41] As Joel Winston, a New Jersey consumer protection lawyer and former deputy state attorney general, opined, "DNA databases are relatively new, but nobody thinks they'll ever be used in [that] manner." [42] Potential ethical concerns aside, scholars and law enforcement alike have been left to wonder about the legality of using DNA samples from genealogy companies to investigate crimes. State privacy laws may carry some weight, but they are often rebutted because most, if not all, DNA samples supplied to genealogy websites are voluntarily submitted. [43] Because of the inherent infringement these searches have on individual privacy, however, it is imperative to consider the Fourth Amendment implications of this policy.

*183 II. HISTORY OF THE USE OF DNA EVIDENCE IN POLICE INVESTIGATIONS

A. *British Development of the Method*

The use of DNA evidence in its modern form did not arise publicly in the court system until 1986 when Dr. Alec Jeffreys, a geneticist at the University of Leicester, United Kingdom, proposed the radical idea that his recently developed method of genetic testing could be used to apprehend criminals. [44] Jeffreys discovered his method accidentally--the result of a failed attempt at studying the progression of illness through family lineage--when he attached DNA that he had extracted from human cells to photographic film and allowed the film to develop. [45] Each developed film reel bore the image of a unique sequence of bars, which Jeffreys soon realized allowed him to distinguish between the DNA patterns of different individuals with extraordinary precision. [46] Initially, Jeffreys' technique was used as a means to establish the paternity of various children in British immigration disputes. [47] However, police officers soon requested Jeffreys' assistance in identifying the perpetrator behind the rape and murder of two teenage girls in the village of Narborough, Leicestershire, who had managed to evade capture for over two years. [48] After a local teenage boy named Richard Buckland confessed to the crimes, but shortly thereafter recanted, Jeffreys was tasked with comparing the blood and semen the killer left at the crime scenes with a sample of Buckland's DNA. [49] Jeffreys' method led to Buckland's exoneration, as the results confirmed that although the two girls were killed by the same man, that man was not Buckland. [50]

This setback did not hinder police enthusiasm to find the killer, however, and investigators continued pursuing the possibilities Jeffreys' innovative method offered. [51] Police began collecting voluntary ***184** blood samples from men throughout the neighborhood, and eventually amassed a database of over 5,000 samples. [52] However, this too yielded no direct match. [53] It was not until August 1987, over a year since the second victim's body was discovered, that a local man notified police that he had overheard another man in a pub discussing how he had supplied a blood sample on behalf of a workmate named Colin Pitchfork. [54] Police quickly brought Pitchfork in for questioning, and he confessed immediately to the rape and murder of the two young women. [55] For the first time in recorded history, DNA testing had led to the successful conviction of a murderer. [56]

B. *DNA Evidence in the United States*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Dr. Jeffreys' innovative new technique quickly made its way to the United States and began weaving its way into the lexicon of criminal investigative techniques. In 1987, a DNA test was able to confirm that a blood sample extracted from Tommie [57] Lee Andrews perfectly matched traces of semen left at the scene of a rape, leading to America's first DNA-based conviction. [58]

Initially, the admissibility of evidence gained through DNA testing was not frequently disputed in court. [59] However, as prosecutors more widely used the practice as a means to secure convictions, defense attorneys began to question the admissibility of DNA evidence in criminal trials, because they doubted the validity of the techniques used to produce DNA profiles. [60] In 1989, one of the first public challenges against using DNA evidence came before the New York State Supreme Court, Appellate Division, in *People v. Castro*, when the court considered the admissibility of a DNA identification ***185** test that would prove that blood found on the defendant's watch belonged to the victim of a murder, tying him directly to the crime. [61] At that time, no appellate court in the state had ruled on the admissibility of DNA evidence in criminal trials, so the court turned to standards for determining the admissibility of new scientific evidence articulated by the U.S. District Court for the District of Columbia in *Frye v. United States* and by the New York Court of Appeals in *People v. Middleton*. [62] The court found that DNA tests satisfied the rule set forth in *Frye*, stating that "the test is not whether a particular procedure is unanimously indorsed [sic] by the scientific community, but whether it is generally acceptable as reliable." [63] In making this determination, the *Castro* court developed a three-prong analysis to aid in its final decision: (1) "Is there a theory, which is generally accepted in the scientific community, which supports the conclusion that DNA forensic testing can produce reliable results?"; (2) "Are there techniques or experiments that currently exist that are capable of producing reliable results in DNA identification and which are generally accepted in the scientific community?"; and (3) "Did the testing laboratory perform the accepted scientific techniques in analyzing the forensic samples in this particular case?" [64] The court was able to discuss the first two prongs with relative ease, concluding first that "[t]here is general scientific acceptance of the theory underlying DNA identification," and second that "DNA forensic identification techniques and experiments are generally accepted in the scientific community and can produce reliable results." [65] Therefore, the court largely decided the case upon consideration of the third prong, holding that "[a] pretrial hearing should be conducted to determine if the testing laboratory substantially performed the scientifically accepted tests and techniques, yielding sufficiently reliable results to be admissible as a question of fact for the jury." [66]

With a clear standard for the admissibility of DNA evidence in court proceedings in place, police and prosecutors were then free to ***186** develop and utilize the technology within the ever-evolving criminal justice system. [67] In 1989, the Virginia Division of Forensic Sciences became the first state crime laboratory to implement a policy of DNA testing in all of its criminal investigations. [68] The following year, the Virginia General Assembly passed the first state law requiring all individuals with felony convictions to submit DNA samples for inclusion in a state DNA database. [69]

The constitutionality of this state database quickly came into question before the Fourth Circuit in *Jones v. Murray*, one of the earliest cases considering this issue. [70] In *Jones*, the court upheld the constitutionality of Virginia's DNA database system, holding:

> Considering the inmates' questionable claim of privacy to protect their identification and the minimal intrusion resulting from taking a small sample of blood, the Commonwealth's interest in combatting and deterring felony recidivism justifies the involuntary taking of the sample and the creation of the DNA data bank as reasonable in the context of the Fourth Amendment. [71]

Following this favorable decision, each of the other forty-nine states began developing their own DNA database systems--and all fifty states actively maintain their systems through the present day. [72] However, the various state laws creating and regulating the databases are largely inconsistent with one another. [73] For example, four state laws require DNA samples from only those defendants convicted of a felony, while at least eight other states require certain individuals convicted of misdemeanor offenses to also supply DNA samples. [74] Additionally, states inconsistently regulate the procedures through which law enforcement may access the databases. [75] While most states allow for the automatic search of their databases in assistance of criminal ***187** investigations, some others are much stricter, allowing police to search the databases only in regard to violent crimes. [76]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

In 1990, in an effort to provide a remedy for this inconsistency, the FBI developed CODIS, a streamlined, nationwide database that law enforcement from any state could access.[77] Initially developed as a pilot program implemented in fourteen state and local crime laboratories within the United States, CODIS is now utilized by over ninety crime laboratories across fifty countries.[78] CODIS enables crime laboratories at the federal, state, and local levels to communicate and share information and DNA samples to facilitate effective criminal investigation.[79] In 1994, the DNA Identification Act[80] established the National DNA Index System (NDIS), a national database containing all of the DNA profiles supplied by the federal, state, and local crime laboratories participating in CODIS.[81] Officially implemented in 1998, the NDIS actively participates with all fifty U.S. states, the District of Columbia, and Puerto Rico.[82] The establishment of the NDIS also helped to resolve the inconsistencies resulting from state-by-state laws surrounding access to DNA databases.[83] According to the FBI, "[i]f a state has signed the Memorandum of Understanding ... to participate in NDIS, that state has agreed to comply with the Federal DNA Identification Act, including the limited access requirements."[84]

*188 III. FOURTH AMENDMENT JURISPRUDENCE

A. *Development of Traditional Fourth Amendment Analysis*

The Fourth Amendment to the United States Constitution guarantees:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[85]

Before the Supreme Court's landmark decision in *Katz v. United States* in 1967, courts tended to limit the extension of Fourth Amendment protection to instances in which law enforcement *physically* trespassed on private property to complete a search or seizure, framing the Amendment to focus mainly on property rights.[86] The Supreme Court rejected this viewpoint in *Katz*, holding that the Fourth Amendment "protects people, not places."[87] Specifically, the Court stated, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[88] The Court has upheld that the reasonableness of an expectation of privacy depends on two factors: (1) the individual must have manifested a subjective expectation of privacy in the object of the challenged search; and (2) society must be willing to recognize that expectation of privacy as reasonable.[89] In *Katz*, the Court found that an individual manifests a subjective expectation of privacy in the objects and locations which he seeks to preserve as private.[90] Therefore, if the individual has displayed a reasonable expectation of privacy, the Court will evaluate "whether ***189** the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment."[91]

Because the *Katz* reasonableness standard inherently allows for some case-by-case variation in analysis, the definition of a search or seizure can vary for the purposes of Fourth Amendment protection.[92] However, the Supreme Court has concretely provided that a "search" occurs when an individual manifests a subjective expectation of privacy in something, which society is willing to recognize as reasonable, and that item is observed visually, or by the use of sense-enhancing technology not in general public use.[93] The Court has also stated that a "seizure" occurs "when [an] officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen."[94] Returning to the significance of the reasonableness consideration, the Court clarified this point to include that "the police can be said to have seized an individual only if, in view of all the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave."[95]

As previously mentioned, the Fourth Amendment has historically been inextricably linked with property rights.[96] Despite the extension of this point beyond strict property in *Katz*, a trespass analysis is still often invoked in consideration of constitutional protection under the Fourth Amendment. For example, in *United States v. Jones,*[97] the Court ruled in favor of a defendant

who had a GPS tracker placed on his vehicle by the government, specifically citing the Fourth Amendment language that notes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." [98] The Court reasoned that a person's vehicle is undoubtedly an "effect" as covered under this clause and, therefore, the government's "installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search." [99] This theory is directly ***190** derived from property law, as the Court noted that there was no doubt "that such a physical intrusion would have been considered a 'search' within the [original] meaning of the Fourth Amendment." [100]

B. *Exceptions*

Various exceptions to the reasonable expectation of privacy requirement for constitutional protection have arisen throughout the span of Fourth Amendment jurisprudence. One notable exception, the abandonment principle, also derives from the Fourth Amendment's traditional focus on property law. [101] As articulated by the Third Circuit in *United States v. Harrison,* "a person can lose his reasonable expectation of privacy in his real property if he abandons it." [102] Whether the owner has abandoned his reasonable expectation of privacy in his property is a determination that "must be made from an objective viewpoint, and proof of intent to abandon must be established by clear and unequivocal evidence." [103] To determine this, the court will look to "the totality of the facts and circumstances." [104] The Supreme Court has extended this principle to trash left on the curb outside an individual's home in *California v. Greenwood*, holding that because trash is sufficiently exposed to public view, it cannot rise to the level of Fourth Amendment protection. [105] Discarded items will only rise to the level of constitutional protection if the manner in which those items were discarded nevertheless constitutes an expectation of privacy that society is prepared to accept as objectively reasonable. [106] With regard to seizures of physical DNA evidence abandoned by a perpetrator at the scene of a crime, scholars have explained that there is no need to afford any constitutional protection to such evidence, because where there is no suspect in mind, there is no Fourth Amendment right to protect. [107] State courts have also articulated this ***191** standard. For example, in *State v. Athan*, police used a suspect's saliva left on an envelope to identify him. [108] There, the Supreme Court of Washington held that "[t]he analysis of DNA obtained without forcible compulsion and analyzed by the government for comparison to evidence found at a crime scene is not a search under the Fourth Amendment." [109]

Another prominent exception to the reasonable expectation of privacy requirement has been referred to as the third-party doctrine, which largely stems from inferences derived from the abandonment principle. The Supreme Court articulated this doctrine in *Smith v. Maryland* when it ruled that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." [110] In *Carpenter v. United States,* the Supreme Court explained that "[t]he third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another." [111] However, the "diminished privacy interests" associated with the third-party doctrine do "not mean that the Fourth Amendment falls out of the picture entirely." [112] Instead, courts should consider "the nature of the particular documents sought to determine whether there is a legitimate expectation of privacy concerning their contents." [113]

IV. USER AGREEMENTS AND CURRENT FEDERAL REGULATIONS OF POPULAR GENEALOGY WEBSITES

The use of genealogy websites by the general public has skyrocketed in recent history. In fact, genealogy is currently the second most popular hobby in the United States, with genealogy websites being the second most frequently visited category of internet sites. [114] Despite genealogy websites' growing popularity, it is unclear whether individuals who willingly upload their DNA to these various services are fully ***192** informed of how their information may be stored and used in the future. [115] For example, following the news surrounding the Golden State Killer case, GEDmatch was forced to release a statement specifying that users' genetic information, though primarily used to find distant relatives, *might* be used for other purposes, as it is not considered private under the third-party doctrine. [116]

Each genealogy website provides the public with information pertaining to their privacy policies and legal obligations with varying degrees of specificity and detail. [117] These measures largely are disclosed to indemnify the companies from legal action

if personal user data is released to third parties. [118] Privacy policies also are disclosed to inform the public at large to which federal regulations these websites and the data stored therein are subject. [119] Each of the three genealogy websites discussed in this Comment vary in terms of the information provided in their privacy statements and terms of service in some respects, but there is some significant overlap with regard to federal statutes.

A. *23andMe*

23andMe, a popular genealogy website, says in its privacy security statement that the company "believes genetic information, as well as the systems put in place to protect it, deserve the highest level of security." [120] For this reason, 23andMe affirms that it will not give personal user data to any third party under any circumstances without explicit user consent, unless a valid warrant mandates the disclosure. ***193** [121] 23andMe explicitly promises its users that it will not provide private user information to "law enforcement or regulatory authorities unless required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information." [122]

The average 23andMe user may find it difficult at first glance to find any relevant statutory constraints on legal liability for the website. In fact, users must first navigate through five separate web pages on 23andMe's website to find the company's "Guide for Law Enforcement" to understand the statutory underpinnings of 23andMe's privacy policy. [123] Although clearly not labeled to attract the attention of the typical user, this guide details to law enforcement all of the necessary steps they must take and the constraints they must overcome before the company will release private user data. [124] This page begins by stating that, "23andMe will only review inquiries as defined in 18 U.S.C. § 2703(c)(2) related to a valid trial, grand jury subpoena, warrant or order." [125] This subsection of the U.S. Code--under the general heading "Required disclosure of customer communications or records" [126] --requires the mandatory disclosure to law enforcement of certain records concerning electronic communications or remote computing services. [127] Under 18 U.S.C. § 2703(c)(2), providers of electronic communication or remote computing services must disclose the name, address, records of session times and durations, length of service, types of services utilized, subscriber number, and means and source of payment for the service to government entities upon a valid request. [128]

Additionally, the Guide for Law Enforcement states that 23andMe will consider releasing additional user information outside of the aforementioned statutory categories if they are prompted to do ***194** so under a court order issued pursuant to 18 U.S.C. § 2703(d). [129] In relevant part, this subsection states that a court may issue such an order "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought are relevant and material to an ongoing criminal investigation." [130] The webpage then cites to 18 U.S.C. § 2703(f) to note that the company has never received a request to preserve information potentially relevant to legal proceedings pursuant to that subsection. [131] 18 U.S.C. § 2703(f) mandates that certain material requested under court order must be preserved for a ninety-day period. [132] Finally, 23andMe states that it will make every effort to notify a user if law enforcement has requested his personal data from the company, unless it is forbidden to do so by a Delayed Notice Order under 18 U.S.C. § 2705(b). [133] This statute states that a governmental entity, under certain circumstances, may apply for a "court order commanding a provider of electronic communications service[s] or remote computing service[s] ... not to notify any other person of the existence of the warrant, subpoena, or court order [directed to them]." [134]

B. *Ancestry DNA*

The Ancestry DNA Guide for Law Enforcement contains the exact same protections and statutory constraints stated by 23andMe except that it does not mention 18 U.S.C. § 2703(f). [135] Therefore, under these two companies, users can expect that their personal data and information will be protected from third-party inquiry except under the extreme circumstance of a valid court order in criminal investigations. This language and statutory scheme is consistent with the Fourth Amendment's protection against unreasonable searches and seizures without a proper warrant issued "upon probable cause, ***195** supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." [136]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Ancestry DNA cites three governing privacy principles: transparency, simplicity, and control. [137] Ancestry DNA also ensures that there are "measures in place to protect against inappropriate access, loss, misuse, or alteration of personal information under [its] control," although it does not clarify what specific "measures" are in place. [138] Additionally, Ancestry DNA offers the assurance that if law enforcement compels it to disclose any user's personal information, its first priority will be to provide the user with advance notice so long as it is permissible under law. [139] Ancestry DNA further provides all visitors--whether they have signed up to use their service or not--with access to an annual transparency report disclosing all law enforcement requests for user data over the preceding year. [140] The 2018 report revealed that Ancestry DNA responded to seven out of a total of ten valid law enforcement requests in that year, all of which were related to investigations of credit card misuse or identity theft. [141] In sum, Ancestry DNA and 23andMe both prioritize user privacy, at least as far as they are legally permitted to do so.

C. *GEDmatch*

GEDmatch's privacy policy paints a wholly different picture of privacy than those articulated by both 23andMe and Ancestry DNA. [142] Unlike the more professional-looking 23andMe and Ancestry DNA websites, GEDmatch provides only a low-tech and minimalist user interface. Its terms of service and privacy policy pages were initially updated in May 2018, one month after the Golden State Killer case was solved. [143] Although much of the initial language of this page ***196** espouses a heightened importance in the protection of individual privacy, the true nature of the website is revealed under a heading titled "GEDmatch Purpose." [144] This section reads:

> GEDmatch exists to provide DNA and genealogy tools for comparison and research purposes. It is supported entirely by users, volunteers, and researchers. DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this Site agree that their information will be shared with other users.

Therefore, unlike the typical legal protections enjoyed by users of more regulated websites, like 23andMe and Ancestry DNA, users of GEDmatch can expect that fellow users, any member of the general public, and even law enforcement may access the genetic information they have freely uploaded to the site.

GEDmatch, conversely, does not claim any statutory protection over its genetic content. GEDmatch brands itself largely as a public forum, rather than strictly a genealogy service. [145] Although it cites no statutory authority, GEDmatch does first establish that it "may disclose [users'] raw data, personal information, and/or genealogy data if it is necessary to comply with a legal obligation such as a subpoena or warrant." [146] The site even offers some possible alternative uses beyond simple genealogy research that users may access--including "familial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains." [147]

Further, GEDmatch's policy was recently updated on December 9, 2019, following the company's acquisition by Verogen, Inc. [148] The revised policy reflects a shift in the company's branding practices in the wake of the Golden State Killer investigation. Specifically, the policy now includes four options for users when uploading their DNA profiles to the website: "Private," "Public + opt-in," "Public + opt-out," and "Research." [149] Notably, the "Public + opt-out" option allows users to upload their DNA profiles for public comparison by ***197** other general users, but hides those profiles from users with profiles identified as having been uploaded "for Law Enforcement purposes." [150] Nevertheless, in this most recent revision, GEDmatch still fails to cite statutory authority for its policies, and retains portions of its policy notifying users of the inherent public nature of its product.

This policy stands in stark contrast to those outlined in the previous two websites. GEDmatch attempts to make it explicitly clear to users that the company is in no way responsible for breaches of information that is publicly accessible on its site. Under this scheme, the website functions largely like a social media platform, in which a majority of user data is voluntarily uploaded under the understanding that it can be freely accessed for any and all purposes.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

V. THE COLORADO MODEL

In 2009, Colorado began to formally implement a policy of statewide familial DNA searching in criminal investigations, making it the first state in the U.S. to formally recognize familial DNA as an investigative resource. [151] Since then, Colorado's policy has become the gold standard for state familial DNA searching, with many states following suit in modeling their own policies after it. [152] Colorado has developed and proliferated its own familial DNA searching software, which is regularly tested and retested to ensure accuracy of results. [153] As of 2017, this software has been shared with local police departments in six additional states and has the capability of being fully downloaded and usable within an hour. [154] Users begin by uploading DNA profile data from the crime scene into the software's database. [155] The software then calculates ratios indicating the likelihood of familial relatedness between samples for all profiles in the system. [156] The software is also capable of organizing this data by familial relationship-- such as parent-child, siblings, etc.--as well as race. [157] Finally, ***198** based on the previously mentioned likelihood ratios, the software will export a table which displays the top selected profiles derived from comparison to the inputted DNA. [158]

There is no specific state legislation in Colorado that either explicitly prohibits or allows the use of familial DNA searches in criminal investigations, because the policy did not originate in the state legislature. [159] The policy of familial DNA searching was first proposed in the state by the Colorado Bureau of Investigations (CBI) and governed by the "CBI DNA Familial Search Policy." [160] After the CBI developed this policy, the state Attorney General approved and put it into effect state-wide in October of 2009. [161] The CBI policy defines familial DNA searching as "a deliberate search for biologically-related relatives of a contributor of an evidentiary profile conducted with specialized (non-CODIS) software designed for this purpose." [162] Because of the obvious privacy concerns and implications the new policy would surely elicit, the CBI was careful to implement incredibly specific and detailed procedures for state law enforcement to follow with each initial familial DNA search request. [163]

First, the request must originate from one of two sources: (1) "analysts within the [CBI or Denver PD Crime] lab identify cases they think are good candidates for [familial DNA searching] and go to their lab director requesting permission;" or (2) directly from a law enforcement agency. [164] Requests under either circumstance must meet a number of strict criteria. [165] First, not only must the case have already undergone a CODIS search with no results, but the lab must also be confident that the law enforcement agency has fully exhausted *all* alternative investigative leads. [166] Second, the request is subject to the professional opinion of the lab staff before familial DNA searching can be approved. [167] In this determination, lab staff will consider a number of factors, including "public safety implications, the age of the case, and the types of evidence available" to ensure that the case is ***199** sufficiently compelling to justify the significant monetary and time expenditure of familial DNA search analysis. [168] In circumstances where the request comes directly from law enforcement, lab staff will meet with the officers to fully inform them of the familial DNA search process. [169] After all relevant information has been shared with the officers, they are required to sign a form indicating their understanding of the procedure and relevant factors surrounding it before any analysis can commence. [170] This form also indicates a commitment from the officers that if a match or lead is discovered through familial DNA searching, officers must continue their investigation of the case so as to not have wasted lab resources. [171] This penultimate step in the process has been cited by both law enforcement entities as well as the Denver PD Crime Lab as one of the most integral parts of the request policy--the formal agreement between parties to take and maintain responsibility of the case so that neither party feels as though their time, finances, or energy is wasted. [172] Finally, the prosecutor of each case will be added to the formal familial DNA searching process to ensure the proper follow-up of any leads produced, continuing the chain of responsibility. [173] Ultimately, the crime lab's director makes the final decision of whether a familial DNA search will be conducted on any given case. [174]

ANALYSIS

This section sets forth a model framework based on the Colorado Model which, if implemented through federal legislation, would provide a uniform request and analysis process for investigative use of familial DNA searching that would afford

heightened protections of the privacy rights of individuals. Specifically, this Part will first provide a comprehensive analysis of the Fourth Amendment implications in the Golden State Killer case under current legal standards. Then, this Part will apply these same facts to the processes and procedures of the Colorado Model. Finally, this Part will discuss the differing outcomes ***200** of these two methods and ultimately conclude that the Colorado Model provides for a more streamlined, thorough, and uniform request system. Federal implementation of the Colorado Model would, therefore, provide for greater constitutional privacy protections for individuals while also improving upon the current process of familial DNA searching.

I. FOURTH AMENDMENT IMPLICATIONS IN THE GOLDEN STATE KILLER INVESTIGATION & PENDING TRIAL

Under the current regulatory scheme surrounding the Fourth Amendment, it is unlikely that any significant constitutional impediments will arise in Joseph DeAngelo's upcoming trial. Assuming, *arguendo*, DeAngelo does assert a constitutional claim, the court will likely begin its analysis by determining whether DeAngelo had a reasonable expectation of privacy in the DNA he shed at the initial crime scene or the more recent DNA he shed on his car door handle and in his trash. [175] Under the abandonment standards articulated in *Greenwood* and *Athan*, the inquiry would likely end at this preliminary juncture. [176] Under *Athan*, as well as under conventional wisdom in police investigations, DeAngelo has no reasonable expectation of privacy in the DNA left in the commission of his original crimes and collected during the course of routine police investigation. [177] Further, in addition to the abandoned DNA later collected by police from a tissue discarded in his trash, the DNA retrieved from the handle of his car--parked in a public parking lot-- would not survive Fourth Amendment scrutiny because both were discarded and subject to public view, therefore constituting a lower manifest privacy interest. [178] Because all three of these samples do not meet the objective reasonableness standard from the perspective of society, DeAngelo could have no reasonable expectation of privacy that would afford him Fourth Amendment protection. [179]

***201** However, it is also important to view this constitutional question from the perspective of the innocent distant family member whose DNA led to the capture and arrest of the perpetrator. This inquiry is much murkier in the Fourth Amendment context. Assuredly, if the DNA had been uploaded to one of the more secure websites, such as 23andMe or Ancestry DNA, the question of reasonableness of the objective expectation of privacy would be more clear based on the safeguards promised in their privacy statements. [180] However, given the objectively lower standard articulated by GEDmatch, there is a significant likelihood that a court would find no Fourth Amendment violation resulting from the police action here. [181] Fourth Amendment protection extends to intrusions of constitutionally protected areas unless the technology used to conduct the search was in general public use. [182] GEDmatch is well within public use as it is marketed as an open-source database in which "information will be shared with other users." [183] The website's very nature facilitates public use, and no user who willingly shares personal data with such a public forum can reasonably expect such data to remain confidential. GEDmatch makes no secret that users may find numerous other uses for the data uploaded to the website and therefore openly employs a "participate at your own risk" policy. Under current Fourth Amendment precedent, there is likely no chance that a court would uphold a constitutional claim purported by the willing GEDmatch user in this case.

II. APPLICATION OF THE COLORADO MODEL TO THE GOLDEN STATE KILLER INVESTIGATION

Unlike the application of Fourth Amendment analysis, the Colorado standard, if applied strictly, could produce vastly different results in the DeAngelo case. Under the Colorado framework, the request for familial DNA searching in this case would come from the policy's second stated source category--directly from law enforcement. [184] Under a federally mandated Colorado-style policy, California state investigators handling the Golden State Killer case could submit a formal ***202** request for familial DNA search analysis of the DNA retrieved from the crime scene. Then, this request would be tested under the strict Colorado criteria. First, law enforcement officials must verify to the crime lab that the DNA had already been put through a CODIS search and yielded no results. [185] As previously discussed, the DNA profile yielded by police using the crime scene DNA left behind by the Golden State Killer was not a match with any of the known felons in the CODIS database. [186] Next, the crime lab would determine whether law enforcement had exhausted all other possible leads. [187] Here, it is clear that after nearly forty years of deliberate investigation, all possible leads had been thoroughly examined. After passing this initial inquiry, the request would then be subject to the professional evaluation of the crime lab analysts. [188] The Golden State Killer case, having gone cold after a period of nearly forty years, is clearly of a significant public interest in terms of safety implications. [189] Under a cost-benefit

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

analysis of the necessity for familial DNA searching in this case, any rational crime lab would undoubtedly move forward, given the sheer amount of lives lost and compassion for the families still suffering. Thereafter, the crime lab analysts would meet with representatives from the California law enforcement agencies who submitted the formal request to fully apprise them of the nature of familial DNA searching and to garner a contractual obligation to continue the investigation if results are successfully yielded. [190] Finally, if a prosecutor had been assigned at that point, she too would be added to this agreement so that all parties share in accountability for the resources expended. [191] Under this scenario, the same results would be produced as would be under the current framework. Even so, the positive implications stemming from the strict scrutiny and accountability standards employed in the Colorado model cannot be diminished. Under these standards, there is an assurance of thoroughness, attention to detail, and accountability, thus ensuring the protection of the rights of all parties involved to the fullest extent possible.

*203 III. THE IMPERATIVE NEED FOR COMPREHENSIVE FEDERAL REGULATION

It is clear from this analysis that no current federal regulations effectively protect the privacy rights of individuals with regard to familial DNA searching in the same comprehensive manner as the Colorado Model. As demonstrated, a simple Fourth Amendment analysis will often fail to extend to such specific instances as those presented here, so long as the DNA collected and tested is publicly available. Additionally, the statutes cited by both 23andMe and Ancestry DNA serve as insufficient guidance for the intricacies involved in DNA retrieval and analysis. The federal legislation contained in 18 U.S.C. § 2703 too broadly covers inquiries with regard to "required disclosures of customer communications or records" in a "remote computing" setting. [192] This incredibly wide-sweeping language is intended to touch upon a variety of web-based communications and does not inherently evoke any cognizant relation for genealogy websites or familial DNA searching. However, the sheer lack of federal guidance or legislation is not surprising given the relative recency and popularity of such services. As the court stated in *United States v. Jones*, "dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes." [193] With this change in popular attitude must come a change in law.

Specific federal legislation aimed at familial DNA searching would provide a uniformity in the request and analysis process that affords heightened protections of the privacy rights of individuals. Instead of allowing for variances in state-implemented policies, cohesive federal regulations would work directly with existing technology, such as CODIS, to produce the most efficient and accurate results. Federal implementation of the Colorado Model would accomplish these objectives. As previously stated, the Colorado familial DNA searching policy has served as a pioneer for other state policies across the country. [194] The FBI could easily implement the process of carrying out this policy in the same way the CBI conducts it within Colorado. Using the highly sophisticated crime labs already in regular use ***204** within the FBI, analysts could begin implementing the Colorado Model's strict scrutiny standards to requests received from all over the country immediately upon adoption. These standards, applied at the federal level, would more closely align with the goals and purposes of the Fourth Amendment, and would provide the necessary vetting and consideration needed before permitting the encroachment upon those rights. In addition to this enhanced Fourth Amendment protection, this policy would produce more efficient and accurate results through familial DNA searching, allowing federal agents to successfully solve more crimes like the Golden State Killer case.

CONCLUSION

The right to privacy is an integral tenant of the freedoms guaranteed to American citizens in the Constitution. However, the current legal restrictions pertaining to familial DNA searching through genealogy websites provide for little substantive protection of this right. Under the current framework, virtually all law enforcement requests for familial DNA data will survive a constitutional challenge in court, as most samples are submitted voluntarily, and police necessity typically takes precedence over arbitrary and attenuated privacy claims in voluntarily uploaded DNA profiles. Additionally, the current standard does not require any formal process by which police must exhaust other options, nor does it require a cost-benefit analysis of privacy concerns. Therefore, the present system places police necessity--arbitrary or otherwise-- above the individual privacy rights of American citizens. The Colorado Model, conversely, maintains a viable option for police access for familial DNA data, while keeping in mind the sanctity of an individual's right to privacy. By requiring proof of police exhaustion of alternative methods, as well as a thorough interest-balancing analysis, this model would lead to greater police accountability while providing a clear and formulaic process for familial DNA requests. Federal implementation of the Colorado Model would provide a clear and uniform federal standard for familial DNA searching. This proposal would provide a viable solution to the inherent privacy concerns that arise from the growing use of genealogy websites for investigatory purposes. A solution such as this will only

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

become more necessary as public genealogy technology continues to expand. Otherwise, an individual's right to privacy as it currently exists will diminish as it is forced to adapt to police demands.

Footnotes

a1 George Mason University Antonin Scalia Law School, J.D. expected, 2020. This Comment is dedicated in memory of Michelle McNamara, whose tireless search for justice was integral in the Golden State Killer's ultimate apprehension.

1 Juan Carlos Guerrero, *TIMELINE: A Look Back at the Golden State Killer's Crime Spree that Lasted a Decade*, ABC7 (May 23, 2018), https://abc7news.com/timeline-looking-back-at-golden-state-killer-crimes/3391867/.

2 *See* Michelle McNamara, *In the Footsteps of a Killer*, L.A. MAG. (Feb. 27, 2013), https://www.lamag.com/longform/in-the-footsteps-of-a-killer/.

3 Laurel Wamsley, *In Hunt for Golden State Killer, Investigators Uploaded His DNA To Genealogy Site*, NPR (Apr. 27, 2018, 7:31 PM), https://www.npr.org/sections/thetwo-way/2018/04/27/606624218/in-hunt-for-golden-state-killer-investigators-uploaded-his-dna-to-genealogy-site.

4 *Id.*; *see also* Melody Gutierrez, *Golden State Killer Suspect's DNA Taken from Car as he Shopped at Hobby Lobby*, S.F. CHRON. (June 2, 2018, 10:51 AM), https://www.sfchronicle.com/crime/article/Golden-State-Killer-suspect-s-DNA-taken-from-12961700.php.

5 *See* Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767, 779-81 (1999).

6 *See id.*

7 *Id.* at 781-82.

8 MICHELLE MCNAMARA, I'LL BE GONE IN THE DARK: ONE WOMAN'S OBSESSIVE SEARCH FOR THE GOLDEN STATE KILLER 52-53 (Harper Perennial 2019) (2018).

9 *Id.*

10 *Id.* at 53.

11 *Id.*

12 *Id.* at 54.

13 *See generally id.*

14 *See* Guerrero, *supra* note 1.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

15 Emily Shapiro, *Inside the Timeline of Crimes by the 'Golden State Killer'*, ABCNEWS (Apr. 26, 2018, 1:34 PM), https://abcnews.go.com/US/inside-timeline-crimes-golden-state-killer/story?id=54744307.

16 MCNAMARA, *supra* note 8, at 4.

17 *See id.* at 328.

18 Joseph Serna & Benjamin Oreskes, *Why did it Take so Long to Arrest the Golden State Killer Suspect? Interagency Rivalries, Old Technology, Errors and Bad Luck*, L.A. TIMES (May 25, 2018, 4:35 PM), http://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-case-20180525-story.html#.

19 *Id.* The offender has come to be known as "The Golden State Killer," first coined by author Michelle McNamara in a 2013 Los Angeles Magazine article. *See* McNamara, *supra* note 2.

20 Wamsley, *supra* note 3.

21 *Id.*

22 *See id.*

23 MCNAMARA, *supra* note 8, at 144-45; *see also* Wamsley, *supra* note 3.

24 MCNAMARA, *supra* note 8, at 144-45, 302; *see also* Wamsley, *supra* note 3.

25 *See* MCNAMARA, *supra* note 8, at 306.

26 *See generally id.*

27 *Id.* at 283.

28 *See id.* at 286-87, 306.

29 *Id.* at 309.

30 *See* Gutierrez, *supra* note 4.

31 *See* Guerrero, *supra* note 1.

32 *See* Wamsley, *supra* note 3.

33 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

34 Erik Ortiz, *Golden State Killer Suspect's Capture Sparks DNA Site Privacy Fears*, NBCNEWS (Apr. 27, 2018, 1:49 PM), https://www.nbcnews.com/news/us-news/golden-state-killer-suspect-s-capture-sparks-dna-site-privacy-n869661.

35 *See* Wamsley, *supra* note 3.

36 *Id.*

37 *Id.*

38 *See* Ortiz, *supra* note 34.

39 *See* Gutierrez, *supra* note 4.

40 *Privacy Concerns After Public Genealogy Database used to ID "Golden State Killer" Suspect*, CBSNEWS (Apr. 27, 2018), https://www.cbsnews.com/news/privacy-concerns-after-public-genealogy-database-used-to-id-golden-state-killer-suspect/.

41 *Id.*

42 Ortiz, *supra* note 34.

43 *Id.*

44 *See* Ian Cobain, *Killer Breakthrough--the Day DNA Evidence First Nailed a Murderer*, THE GUARDIAN (June 2, 2016, 10:25 AM), https://www.theguardian.com/uk-news/2016/jun/07/killer-dna-evidence-genetic-profiling-criminal-investigation.

45 *Id.*

46 *Id.*

47 *Id.*

48 *Id.*

49 *Id.*

50 *See* Cobain, *supra* note 44.

51 *Id.*

52 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

53 *Id.*

54 *Id.*

55 *Id.*

56 *See* Cobain, *supra* note 44.

57 Some sources spell Mr. Tommie Lee Andrews' name as "Tommy." *Compare* Andrews v. State, 533 So. 2d 841 (Fla. Dist. Ct. App. 1988) ("Tommie Lee Andrews"), *with* Roger Roy, *DNA Test Gets a Chance in Orange Rape Trial*, THE ORLANDO SENTINEL, Oct. 21, 1987, at A1 ("Tommy Lee Andrews").

58 *See* Karen Cormier at al., *Evolution of DNA Evidence for Crime Solving--A Judicial and Legislative History*, 2 FORENSIC MAG., no. 4 (2005), http://tools.thermofisher.com/content/sfs/brochures/cms_042067.pdf.

59 *Id.*

60 *Id.*

61 People v. Castro, 545 N.Y.S.2d 985 (N.Y. App. Div. 1989).

62 *Id.* at 986 (first citing Frye v. United States, 293 F. 1013 (D.C. Cir. 1923) (discussing the admissibility of blood pressure monitoring to determine honesty during questioning); then citing People v. Middleton, 429 N.E.2d 100 (N.Y. 1981) (discussing the admissibility of bite mark evidence)).

63 *Castro*, 545 N.Y.S.2d at 986-87 (quoting *Middleton*, 429 N.E.2d at 103).

64 *Id.* at 987.

65 *Id.* at 999.

66 *Id.*

67 *See* Hibbert, *supra* note 5, at 774.

68 *Id.*

69 *Id.*

70 Jones v. Murray, 962 F.2d 302, 303 (4th Cir. 1992).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

71 *Id.* at 310-11.

72 *See* Hibbert, *supra* note 5, at 775.

73 *Id.* at 779.

74 *Id.* at 776.

75 *See id.* at 779.

76 *Id.*

77 FED. BUREAU OF INVESTIGATION, *Combined DNA Index System (CODIS)*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis#CODIS-and%20NDIS%C20Fact%20Sheet (last visited Oct. 18, 2019) [hereinafter FED. BUREAU OF INVESTIGATION, *CODIS*].

78 *Id.*

79 *Id.*

80 34 U.S.C. § 12592 (2019).

81 FED. BUREAU OF INVESTIGATION, *CODIS, supra* note 77.

82 *Id.*

83 *Id.*

84 FED. BUREAU OF INVESTIGATION, *Frequently Asked Questions on CODIS and NDIS*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Oct. 18, 2019) [hereinafter FED. BUREAU OF INVESTIGATION, *CODIS and NDIS FAQs*]. The FBI's Memorandum of Understanding is a mandatory agreement for participation in the NDIS, "documenting their agreement to abide by the DNA Identification Act requirements as well as record-keeping and other operational procedures governing the uploading of DNA data, expungements, CODIS users, audits, etc." *Id.*

85 U.S. CONST. amend. IV.

86 *See* Katz v. United States, 389 U.S. 347, 352-53 (1967).

87 *Id.* at 351.

88 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

89 *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)).

90 *See* *Katz*, 389 U.S. at 351.

91 *See* Oliver v. United States, 466 U.S. 170, 182-83 (1984).

92 *See* *Katz*, 389 U.S. at 357.

93 *See* Kyllo v. United States, 533 U.S. 27, 34 (2011).

94 *See* Michigan v. Chesternut, 486 U.S. 567, 573 (1988) (quoting Terry v. Ohio, 392 U.S. 1, 19 n. 16 (1968)).

95 *See id.* (quoting United States v. Mendenhall, 446 U.S. 544, 555 (1980)).

96 *See* *Katz*, 389 U.S. at 352-53.

97 United States v. Jones, 565 U.S. 400 (2012).

98 *Id.* at 404.

99 *Id.*

100 *See id.* at 404-05.

101 John P. Ludington, Annotation, *Search and Seizure: What Constitutes Abandonment of Personal Property Within Rule that Search and Seizure of Abandoned Property is not Unreasonable--modern cases*, 40 A.L.R. 4th 381 (1985).

102 United States v. Harrison, 689 F.3d 301, 307 (3d Cir. 2012).

103 *Id.*

104 *Id.*

105 *See* California v. Greenwood, 486 U.S. 35, 40 (1988).

106 *Id.* at 39-40.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

107 Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. L. REV. 857, 859 n.10 (2006).

108 State v. Athan, 158 P.3d 27, 37 (Wash. 2007).

109 *Id.*

110 Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

111 Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

112 *Id.* (quoting Riley v. California, 573 U.S. 373, 392 (2014)).

113 *Id.* (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

114 Gregory Rodriguez, *How Genealogy Became Almost as Popular as Porn*, TIME (May 30, 2014), http://time.com/133811/how-genealogy-became-almost-as-popular-as-porn/. In this article, Time Magazine points out that the most popular hobby in the United States is gardening, and the most popular category of website visited is pornography. *Id.*

115 CBSNEWS, *supra* note 40.

116 *See id.*

117 *See generally Privacy and Data Protection*, 23ANDME, https://www.23andme.com/privacy/ (last visited Oct. 18, 2019) [hereinafter *Privacy*, 23ANDME]; *see also Your Privacy*, ANCESTRY, https://www.ancestry.com/cs/legal/privacystatement (last visited Oct. 18, 2019) [hereinafter *Your Privacy*, ANCESTRY]; *see also Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last visited Jan. 21, 2020) [hereinafter *Privacy Policy*, GEDMATCH].

118 *See, e.g., Ancestry International Terms and Conditions*, ANCESTRY, https://www.ancestry.com/cs/legal/row-terms-and-conditions-en (last visited Nov. 21, 2019).

119 *E.g.*, Marcus Moretti & Michael Naughton, *Why Privacy Policies are so Inscrutable*, THE ATLANTIC (Sep. 4, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/.

120 *Privacy*, 23ANDME, *supra* note 117.

121 *Privacy Highlights*, 23ANDME, https://www.23andme.com/about/privacy/ (last updated Sept. 30, 2019) [hereinafter *Privacy Highlights*, 23ANDME].

122 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

123 *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ (last visited Oct. 18, 2019). To reach this page, a user must navigate from the 23andMe homepage, to the "Privacy and Data Protection" page through a tab, then through a link on that page to the "Privacy Statement" page, then through a link on that page to the "Transparency Report" page, then finally through a link on that page to the "Guide for Law Enforcement."

124 *Id.*

125 *Id.*

126 18 U.S.C. § 2703 (2019).

127 18 U.S.C. § 2703(c) (2019).

128 *See* 18 U.S.C. § 2703(c)(2)(A)-(F) (2019).

129 *23andMe Guide for Law Enforcement, supra* note 123.

130 18 U.S.C. § 2703(d) (2019).

131 *23andMe Guide for Law Enforcement, supra* note 123.

132 18 U.S.C. § 2703(f) (2019).

133 *23andMe Guide for Law Enforcement, supra* note 123.

134 18 U.S.C. § 2705(b) (2019).

135 *See Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement (last visited Oct. 18, 2019).

136 U.S. CONST. amend. IV.

137 *Your Privacy*, ANCESTRY, *supra* note 117.

138 *Id.*

139 *Id.*

140 *Ancestry 2018 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency (last visited Jan 22, 2020).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

141 *Compare id., with Ancestry 2017 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency-2017 (last visited Jan. 20, 2020). The 2017 report revealed that Ancestry DNA responded to thirty-one out of a total thirty-four valid law enforcement requests in 2017, all of which were related to investigations of credit card misuse or identity theft.

142 *Privacy Policy*, GEDMATCH, *supra* note 117.

143 *Id.*

144 *Id.*

145 *Id.*

146 *Id.*

147 *Id.*

148 *Privacy Policy*, GEDMATCH, *supra* note 117.

149 *Id.*

150 *Id.*

151 MICHAEL B. FIELD, ET AL., NAT'L CRIMINAL REFERENCE SERV., STUDY OF FAMILIAL DNA SEARCHING POLICIES AND PRACTICES: CASE STUDY BRIEF SERIES 3 (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251081.pdf.

152 *Id.*

153 *Id.* at 5.

154 *Id.*

155 *Id.*

156 *Id.* at 6.

157 FIELD, ET AL., *supra* note 151, at 6.

158 *Id.*

159 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

160 *Id.*

161 *Id.*

162 *Id.*

163 FIELD, ET AL., *supra* note 151, at 7-9.

164 *Id.* at 7.

165 *Id.*

166 *Id.*

167 *Id.*

168 *Id.*

169 FIELD, ET AL., *supra* note 151, at 7.

170 *Id.*

171 *Id.*

172 *Id.*

173 *Id.*

174 *Id.*

175 *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

176 *See* California v. Greenwood, 486 U.S. 35, 39-40 (1988); State v. Athan, 158 P.3d 27, 37 (Wash. 2007).

177 *Athan*, 158 P.3d at 37.

178 *Greenwood*, 486 U.S. at 39-40; United States v. Harrison, 689 F.3d 301, 307 (3d Cir. 2012).

179 *Greenwood*, 486 U.S. at 39-40.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

180 *Ancestry Guide for Law Enforcement, supra* note 135; *Privacy*, 23ANDME, *supra* note 117.

181 *See Privacy Policy*, GEDMATCH, *supra* note 117.

182 Kyllo v. United States, 533 U.S. 27, 34 (2011).

183 *Privacy Policy*, GEDMATCH, *supra* note 117.

184 FIELD, ET AL., *supra* note 151.

185 *Id.*

186 *See* MCNAMARA, *supra* note 8, at 302; *see also* Wamsley, *supra* note 3.

187 FIELD, ET AL., *supra* note 151.

188 *Id.*

189 *Id.*

190 *Id.*

191 *Id.*

192 18 U.S.C. § 2703(c) (2019).

193 United States v. Jones, 565 U.S. 400, 427 (2012).

194 FIELD, ET AL., *supra* note 151.

30 GMUCRLJ 177

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

KeyCite Yellow Flag - Negative Treatment
Distinguished by Cirwithian v. State, Del.Supr., May 6, 2021

185 A.3d 1
Supreme Court of Delaware.

David BUCKHAM, Appellant,
v.
STATE of Delaware, Appellee.

No. 538, 2016
|
Submitted: January 24, 2018
|
Decided: April 17, 2018

Synopsis

Background: Defendant was convicted in the Superior Court, No. 1509012122A & B, of first-degree assault and related charges in connection with a shooting. Defendant appealed.

Holdings: The Supreme Court, Traynor, J., held that:

[1] trial court's decision to allow State's eyewitness, who was in the middle of testifying and in the middle of recanting statement he had given to police pinning shooting on defendant, to consult with his lawyer was reversible error;

[2] search warrant, which authorized search of data on defendant's cell phone for evidence linking him to shooting, was too vague about information sought and expressly authorized search of materials there was no probable cause to search, and thus, warrant was invalid; and

[3] trial court's decision to uphold search warrant for defendant's cell phone and to admit messages from social networking website that police found on the phone was plain error.

Reversed and remanded.

West Headnotes (26)

[1] **Criminal Law** Discretion
Criminal Law Necessity and scope of proof
Criminal Law Power and duty of court
Witnesses Order, Course, and Extent of Examination

A trial judge is vested with wide discretion in regulating the conduct of the trial, including the mode and order of interrogating witnesses and presenting evidence; that includes the broad power to sequester witnesses before, during, and after their testimony. Del. R. Evid. 611(a).

[2] **Criminal Law** Power and duty of court

The heartland of witness sequestration concerns whether witnesses should be barred from hearing the testimony of other witnesses before their own, a method of ferreting out false testimony that has ancient roots, but the concept also extends to whether a witness should be barred from discussing his testimony with others once questioning has commenced; the concern, of course, is that permitting mid-testimony consultations may lead to improper attempts to influence the testimony in light of the testimony already given.

[3] **Criminal Law** Power and duty of court

Whether and how a witness should be sequestered is a matter committed to the trial judge's discretion.

[4] **Criminal Law** Power and duty of court

A criminal defendant has no constitutional right to any particular type of witness sequestration.

[5] **Criminal Law** Power and duty of court

A request for a “heartland” sequestration order, an order barring witnesses from hearing the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

testimony of other witnesses, is not granted as of statutory right in Delaware, as it is in some jurisdictions. Del. R. Evid. 615.

[6] **Criminal Law** Power and duty of court

Criminal Law Consultation between accused or counsel and witnesses

The decision of whether to grant a request to sequester a witness rests comfortably in the trial judge's authority to control the mode of witness interrogation; the same is true for a decision to grant a recess and allow a conference between a lawyer and a testifying witness. Del. R. Evid. 615.

[7] **Criminal Law** Consultation between accused or counsel and witnesses

A trial judge must exercise his or her discretion in determining whether to grant a recess and allow a conference between a lawyer and a testifying witness in service of the trial's truth-seeking function.

1 Cases that cite this headnote

[8] **Criminal Law** Consultation between accused or counsel and witnesses

Witnesses Order, Course, and Extent of Examination

Witnesses Counsel for witness

Trial judges are bound to use their power to control how witnesses are interrogated to make the interrogation and presentation effective for the ascertainment of truth, and allowing a witness to consult with counsel in the midst of questioning is fraught with the risk of interfering with the truth-seeking process.

[9] **Criminal Law** Consultation between accused or counsel and witnesses

It is antithetical to the process of truth-seeking that any witness be permitted to consult with counsel during cross-examination to be coached on what to say, or not say, or how-to-say-it, or how to control or put a better face on testimonial damage already done.

[10] **Criminal Law** Consultation between accused or counsel and witnesses

The truth-seeking function of a trial will most often be best served by requiring that the witness undergo direct questioning and cross-examination without interruption for counseling.

[11] **Criminal Law** Consultation between accused or counsel and witnesses

Because of the tantalizing potential for misconduct they pose, mid-testimony conferences with counsel are an extremely dangerous practice; no trial judge should allow one without carefully considering whether there is a genuine need for it—one that rises above a bare desire to coach a struggling witness—and, even if there is, whether the risk of coaching is simply too great to allow it.

[12] **Criminal Law** Consultation between accused or counsel and witnesses

Criminal Law Reception of evidence

Trial court's decision to allow State's eyewitness, who was in the middle of testifying and in the middle of recanting statement he had given to police pinning shooting on defendant, to consult with his lawyer was reversible error in trial for assault and related charges in connection with shooting; testimony of only other eyewitness was problematic as his account of events varied since the night of the shooting, no physical evidence linked defendant to the shooting, and after conference, eyewitness told third version of events that he later disavowed on cross-examination.

[13] **Criminal Law** Prejudice to rights of party as ground of review

Not all errors call for reversal; but to deem an error harmless, and safely disregard it, the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Supreme Court must have a fair assurance that the judgment was not substantially swayed by the error. Del. Super. Ct. Crim. R. 52(a).

1 Cases that cite this headnote

[14] **Criminal Law** Remarks and Conduct of Judge

Criminal Law Reception of evidence

No party, not even a criminal defendant, has a constitutional right to any particular type of witness sequestration, so even if a trial court abuses its discretion by allowing a witness to consult with a lawyer in the middle of testimony, that error is not of constitutional magnitude and is not subject to the more rigorous form of harmless error review that applies to trial errors that infringe upon constitutional rights. Del. Super. Ct. Crim. R. 52(a).

[15] **Criminal Law** Prejudice to rights of party as ground of review

Determining whether an error is harmless is necessarily a case-specific inquiry; one that requires the Supreme Court to scrutinize the record to evaluate both the importance of the error and the strength of the other evidence presented at trial. Del. Super. Ct. Crim. R. 52(a).

1 Cases that cite this headnote

[16] **Criminal Law** Searches and seizures

Because the Supreme Court pays great deference to the issuing magistrate's determination that a search warrant was supported by probable cause, the Supreme Court's duty is simply to ensure that the magistrate had a substantial basis for concluding that probable caused existed and that the magistrate's determination did not reflect an improper analysis of the totality of the circumstances. U.S. Const. Amend. 4; Del. Const. art. 1, § 6.

2 Cases that cite this headnote

[17] **Criminal Law** Review De Novo

The Supreme Court reviews questions challenging a search warrant's particularity and breadth de novo. U.S. Const. Amend. 4; Del. Const. art. 1, § 6.

[18] **Criminal Law** In Preliminary Proceedings

Where a defendant did not raise a challenge to a search warrant's particularity and breadth in the Superior Court, the Supreme Court will take notice of an error only if it is plain. U.S. Const. Amend. 4; Del. Const. art. 1, § 6.

1 Cases that cite this headnote

[19] **Criminal Law** Necessity of Objections in General

Under the plain error standard of review, the error complained of must be so clearly prejudicial to substantial rights as to jeopardize the fairness and integrity of the trial process.

1 Cases that cite this headnote

[20] **Searches and Seizures** Necessity for writing; oral presentation or supplementation

For a search warrant to issue, there must be more than just probable cause that a crime has been committed; there must also be, within the four corners of the affidavit, facts adequate for a judicial officer to form a reasonable belief that the property to be seized will be found in a particular place. U.S. Const. Amend. 4; Del. Const. art. 1, § 6.

5 Cases that cite this headnote

[21] **Searches and Seizures** Objects or information sought

Search warrant, which authorized search of data on attempted murder suspect's cell phone for evidence linking him to shooting, was too vague about information sought and expressly authorized search of materials there was no probable cause to search, and thus, warrant was invalid; although trial court found that affidavit supporting warrant created probable cause to search phone for GPS data to

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

ascertain where suspect had been during six weeks prior to his arrest, warrant did not limit the search of cell phone to any relevant time frame, and warrant authorized police to search incoming and outgoing calls, missed calls, contact history, images, photographs, text messages, and contents of messages on social media website. U.S. Const. Amend. 4; Del. Const. art. 1, § 6; 11 Del. Code § 2306.

24 Cases that cite this headnote

[22] **Searches and Seizures** Particularity or generality and overbreadth in general

A warrant must describe the items to be searched for and seized with as much particularity as the circumstances reasonably allow and be no broader than the probable cause on which it is based. U.S. Const. Amend. 4; Del. Const. art. 1, § 6.

2 Cases that cite this headnote

[23] **Criminal Law** Necessity of Objections in General

Plain errors must be apparent on the face of the record, basic, serious, and fundamental in their character, and clearly deprive an accused of a substantial right, or clearly show manifest injustice.

[24] **Criminal Law** Necessity of Objections in General

In plain error review, the Supreme Court judges whether an error is apparent from the vantage point of the appellate court in reviewing the trial record, not whether it was apparent to the trial court in light of then-existing law.

[25] **Criminal Law** Necessity of Objections in General

To be plain error, the error must be more than just apparent from the record; it must also be so clearly prejudicial to substantial rights as to jeopardize the fairness and integrity of the trial process, which means that it must have affected the outcome of the trial.

[26] **Criminal Law** Wrongfully obtained evidence

Searches and Seizures Particular concrete applications

Trial court's decision to uphold search warrant for defendant's cell phone and to admit messages from social networking website that police found on the phone was plain error in trial for assault and related charges in connection with shooting; mismatch between scope of warrant and probable cause finding that trial court cited to support the warrant was readily apparent from the record, both of State's witnesses told various versions of events, and prosecutor told jury that social networking messages on cell phone would be important to their decision. U.S. Const. Amend. 4; Del. Const. art. 1, § 6.

11 Cases that cite this headnote

***4** Court Below: Superior Court of the State of Delaware, Cr. ID No. 1509012122A & B, Upon appeal from the Superior Court. **REVERSED** and **REMANDED**.

Attorneys and Law Firms

Christina L. Ruggiero, Esquire (argued), Eugene J. Maurer, Jr., Esquire, Eugene J. Maurer, Jr., P.A., Wilmington, Delaware, Counsel for Appellant.

Abby Adams, Esquire (argued), Department of Justice, Georgetown, Delaware, Counsel for Appellee.

Before STRINE, Chief Justice; VALIHURA, VAUGHN, SEITZ, and TRAYNOR, Justices.

Opinion

TRAYNOR, Justice:

David Buckham was convicted at trial of assault in the first degree and related charges in connection with a shooting. His appeal presents two questions of criminal procedure. First, we consider the propriety of the trial court's decision to call a recess at the State's request so that one of the State's

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

witnesses, who was in the middle of testifying—and in the middle of recanting a statement he had given to investigators before trial—could consult with his lawyer. Buckham—who was forbidden by the trial court from cross-examining the witness about what transpired during the consultation—contends it was reversible error to allow it and a violation of his confrontation rights to bar him from cross-examining the witness about it.

Second, we consider whether it was plain error for the trial court to uphold a warrant that authorized a search of "[a]ny and all store[d] data" on Buckham's cell phone for any evidence of any kind that might link him to the shooting. The trial court sustained the warrant despite recognizing that the only nexus the warrant application established between his phone and the shooting was that the phone might have contained GPS data that might have been useful to investigators. The search instead turned up some arguably incriminating Facebook messages, and Buckham contends that they should have been suppressed. He did not raise this precise contention below, but he contends that the mismatch between the scope of the warrant and the probable cause the trial court found to support it was so apparent, and that the warrant was so lacking in particularity, that upholding the warrant was plain error.

We agree that the trial court's decision to allow the State's witness a mid-testimony consultation with counsel was reversible error and that the decision to uphold the warrant—and admit the Facebook messages—was plain error. We therefore reverse Buckham's convictions and remand for a new trial.

I

A

During the early morning hours of August 3, 2015, two Wilmington police officers ***5** responded to a shooting. They found Gerald Walker—apparently shot in his upper abdomen—lying in a fetal position in the entranceway of a residence. Walker was in pain, but lucid, and he told the officers that he had been shot by the occupants of a dark-colored SUV. He said that three or four shots had come from the front passenger side of the vehicle, but he was unable to see the occupants because the vehicle's windows were heavily tinted. The police did not locate any witnesses or recover any shell casings or other physical evidence from the scene.

With no identification of the perpetrators and no physical evidence, the investigation languished into September. Then, halfway through the month, a 911 caller reported that a person who had previously shot him had just driven past his house. One of the officers who responded was one of the two who had responded to the August 3 shooting, and when he arrived on the scene, he discovered that the 911 caller was none other than Gerald Walker. Walker reported that he and his fiancé were sitting on the steps of her home when the same vehicle from the August 3 shooting drove by. He identified the driver as David Buckham and the passenger as Imean Waters and said that as the two drove by, one or both of the them said, "We're on your top"—meaning that they were still after him. [1] Walker also claimed that Waters waved a gun at him to drive the point home.

The officer also had a brief conversation with Walker about the August 3 shooting. Despite telling the officers on the night of the shooting that he had not been able to get a look at the occupants of the vehicle, Walker now told the officer definitively that Buckham was the assailant. According to the officer's recollection of the conversation, Walker also told him that Buckham had exited the vehicle and fired the shots from there, not while concealed behind the vehicle's tinted windows.

Later that day, a detective interviewed Walker, and Walker again blamed the shooting on Buckham. He told the detective that Waters was driving and that when Waters said "hit him," Buckham started shooting. [2] But while he was steadfast that Buckham was the shooter, he admitted that he did not see the shots being fired or "even see the gun"—he "just heard the shot." [3]

Based on what Walker had told them, law enforcement secured arrest warrants for Waters and Buckham. Waters was arrested that same day, and he too was interviewed by the police. When asked about the shooting on August 3, he admitted that he and Buckham had driven past the site of the shooting, but he initially claimed that he had dropped Buckham off on the side of the road and heard gunshots only after driving away. But after being pressed on his story, Waters told the police that Buckham shot Walker from the passenger seat of his vehicle.

Based on the information provided by Walker and Waters, police secured a warrant for Buckham's arrest. They were unable to locate him, and it was not until approximately six

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

weeks later that he was arrested in a library in New Jersey by federal law enforcement officers. His cell phone was seized incident to his arrest, and it was turned over to the Wilmington police.

The gun used in the shooting has never been recovered. The inability of the police to find the gun or to ascertain where ***6** Buckham had been residing during the six weeks they had been searching for him prompted them to seek a search warrant for his cell phone. They apparently thought that they may be able to find GPS location data on the phone, which could reveal where Buckham had been residing and, in turn, might lead to the discovery of the gun.

The warrant they obtained for Buckham's phone authorized them to search not just for GPS location data, but for "[a]ny and all store[d] data contained within the internal memory of the cellular phones [sic]." It is unclear from the record whether the police found any GPS data and, if they did, whether they actually used it to search for the gun. What is clear is that they found and read private messages Buckham had exchanged with various people through the Facebook application on his phone, some of which were later introduced at trial.

B

Buckham was charged with a host of offenses, the most serious of which was attempted murder in the first degree. Not surprisingly, at center stage at his trial were Walker and Waters, the only percipient witnesses (other than, allegedly, Buckham) to the shooting. Neither wished to be there.

Walker appeared at trial only after being arrested and held on a material-witness warrant. When he was called to the stand, his testimony diverged yet again from the previous accounts he had given to the police. Contrary to his claim that Buckham had shot at him from outside the vehicle, Walker testified that Buckham "started shooting out of the window."[4] The prosecutor sought clarification—asking him, "what window?"—but Walkers reiterated that Buckham shot from through the "passenger side window."[5] And despite telling the detective that he had not seen the weapon that had been used to shoot him or who fired it, Walker testified that he had seen "a little black gun" in Buckham's hand just before the shooting started, and he testified, unequivocally, that Buckham was the shooter.[6] He also disclosed, for the first time, that a "senior citizen" named "Mr. Mel" was sitting outside with him when Waters and Buckham pulled up in the SUV and presumably witnessed the entire encounter. As if these inconsistencies did not provide sufficient fodder to question Walker's credibility, he announced—in open court—that defense counsel's questions were "aggravating" him, that he was "just going to keep answering questions with, 'I don't know' " because he was tired of answering them, and, at one point, that he intended to "plead the Fifth to every question from now on" (which, after the jury was excused, prompted a warning of contempt from the trial judge).[7]

The prosecution then called Waters, whose testimony was more problematic. Before Buckham's trial, Waters had agreed to plead guilty to conspiracy in the second degree (in connection with the allegedly menacing drive-by that occurred in mid-September) in exchange for testifying at Buckham's trial. But despite having admitted on the day of his arrest that Buckham shot Walker from the passenger seat ***7** of his vehicle, Waters disavowed even having seen Walker that day:

> Q: So, with respect to the August 3rd, 2015, shooting, what do you remember about that day?
>
> A: The only thing I remember was me and Buckham riding around. I didn't see no gun, or nothing.
>
> ....
>
> Q: Do you remember seeing [Walker]—
>
> A: No.[8]

After a brief sidebar conference, the prosecutor attempted to clarify Waters' testimony:

> Q: .... So, bringing you back to when you stated that you and Mr. Buckham were driving around on August 3rd, 2015.
>
> A: Yes.
>
> Q: And I asked you did you see [Walker] that day.
>
> A: Yes. I hadn't seen him.
>
> Q: So, is it your testimony today that you did not see [Walker] on August 3rd, 2015?
>
> A: No, I did not.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> Q: And, Mr. Waters, on August 3rd, 2015, did you hear gunshots that day?
>
> A: No. [9]

That prompted the prosecutor to request another sidebar conference at which she told the court, "Mr. Waters is facing significant issues, not only by violating the cooperation agreement, but also by potentially perjuring himself ... [and] he may want to speak to his counsel at this point." [10] Over Buckham's counsel's objection, the trial judge agreed. Buckham's counsel asked whether he would be permitted to cross-examine Waters about the substance of the conversation, but the trial judge answered in the negative:

> Well, if you are asking whether or not during the break that he [spoke] with counsel, I think I would let you ask that question.
>
> Obviously, exploring with him what counsel maybe told him would be a violation of the attorney/client privilege and I wouldn't allow you to pursue that. But, I would allow you to say, When you took the break did you have an opportunity to speak with [your lawyer?] [11]

After the consultation took place, the trial judge reiterated that he would not allow Buckham's counsel "to explore the contents of the discussion because of the privileged situation of that conversation." [12]

Not surprisingly, Waters' testimony took on a different tenor when he returned from speaking with his lawyer. When asked again whether he remembered anything about August 3, the day of the shooting, this time he responded, "Not really." [13] And when asked if he remembered the day Walker was shot, he acknowledged only that he "heard about it." [14] The prosecutor then asked him to confirm that he had told the police on the day of his arrest that he had been present at the shooting, but he denied having any recollection of that either, telling the prosecutor, "I was under the influence. I don't remember." [15] The State then terminated its direct examination so that it could lay the foundation for ***8** admitting the statement Waters gave to police on the day of his arrest in lieu of any further live testimony.

Buckham did not testify. He was ultimately acquitted of attempted murder, but found guilty of the lesser-included offense of first-degree assault and a number of other lesser charges. At a bench trial that followed, he was convicted of possession-of-a-firearm-by-a-person-prohibited and possession-of-ammunition-by-a-person-prohibited charges as a result of the jury's verdict. He was sentenced to twenty-six years of incarceration, suspended after sixteen years.

II

Buckham contends that the trial judge should not have allowed Waters to confer with his lawyer during his direct examination and made matters worse by restricting Buckham's cross-examination after the consultation took place. He contends that the former was an abuse of discretion and that the latter infringed his right of confrontation, both of which, he says, require reversal.

A

[1] **[2]** It is well settled that the trial judge is vested with wide discretion in regulating the conduct of the trial, [16] including "the mode and order of interrogating witnesses and presenting evidence." [17] That includes the "broad power to sequester witnesses before, during, and after their testimony." [18] The "heartland" of witness sequestration concerns whether witnesses should be barred from hearing the testimony of other witnesses before their own [19]—a method of ferreting out false testimony that has "ancient" roots [20]—but the concept also extends to whether a witness should be barred from discussing his testimony with others once questioning has commenced. [21] The concern, of course, is that permitting mid-testimony consultations may lead to "improper attempts to influence the testimony in light of the testimony already given." [22]

[3] **[4]** **[5]** **[6]** Whether and how a witness should be sequestered is a matter committed to the trial judge's discretion. Even "[a] criminal defendant," like Buckham, "has no constitutional right" to any particular type of witness sequestration, [23] and ***9** "the failure to sequester prosecution witnesses does not necessarily violate any constitutional right of the defendant to cross-examine those witnesses, or to a fair trial generally." [24] In Delaware, even a request for a "heartland" sequestration order—an order barring witnesses from hearing the testimony of other

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

witnesses—is not granted as of statutory right, as it is in some jurisdictions.[25] The decision instead rests comfortably in the trial judge's authority to control the mode of witness interrogation. The same is true for a "decision to grant a recess and allow a conference between a lawyer and a testifying witness."[26] The scenarios where a mid-testimony consultation might be requested are too varied for there to be a "hard and fast rule governing every contingency."[27]

[7] **[8]** **[9]** But a trial judge must exercise this discretion in service of the trial's truth-seeking function. Trial judges are bound to use their power to control how witnesses are interrogated to "make the interrogation and presentation effective for the ascertainment of truth,"[28] and allowing a witness to consult with counsel in the midst of questioning is fraught with the risk of interfering with the truth-seeking process. As we recognized in the context of a mid-cross-examination consultation—which is not far afield of these circumstances, given how Waters' testimony was going south for the prosecution—allowing a witness who is in the middle of his testimony to consult with his counsel tends to undermine the integrity of the trial process:

> It is antithetical to the process of truth-seeking that any witness be permitted to consult with counsel during cross-examination to be "coached" on what to say, or not say, or how-to-say-it, or how to control or "put a better face on" testimonial damage already done.[29]

[10] **[11]** Put simply, "the truth-seeking function of a trial will most often be best served by requiring that the witness undergo direct questioning and cross-examination without interruption for counseling."[30] Because of the "tantalizing ***10** potential for misconduct" they pose,[31] mid-testimony conferences are "an extremely dangerous practice."[32] No trial judge should allow one without carefully considering whether there is a genuine need for it—one that rises above a bare desire to coach a struggling witness—and, even if there is, whether the risk of coaching is simply too great to allow it.[33]

B

The decision to allow this conference suffered from a number of problems. The justification for it was that Waters' testimony, which flatly contradicted the statement he had given to the police, may have put him at risk of perjury or a breach of his plea agreement and that he should have a chance to discuss those risks with his counsel before going any further. But the request for the conference did not come from Waters or even from his own lawyer, who was present in the courtroom. The request came from the prosecutor, just as Waters' testimony started going sideways.[34] There is naturally a greater risk that a mid-testimony conference will be used for coaching when the request comes in the midst of damaging testimony—and comes from the advocate whose case it is damaging.

These features set this case apart from those where courts have permitted time-outs in the middle of testimony for more benign reasons, like *United States v. Loyd*,[35] where a prosecutor—who had met a witness for the first time only thirty minutes before trial because the witness was under federal protection—quickly realized that he had not had enough time to speak with the witness to properly tailor his examination and was granted a recess to have a chance for a more thorough interview, or *Frierson v. State*,[36] where the court granted a prosecutor's request for a recess during the direct examination of a rape victim so that the prosecutor could help her regain her composure. In this case, the very purpose of the recess was to allow Waters to discuss with his lawyer the testimony already given and to consider whether he should stick by it. As the trial judge put it, he was granting the recess to "have counsel speak with him, just to make sure that they are all on the same page."[37]

Compounding these problems was the trial court's decision to seal the conversation off from cross-examination. Through many of the cases where mid-testimony ***11** consultations were sustained runs a common thread: the opposing side was permitted a full opportunity to inquire into what transpired during the consultation.[38] "Skillful cross-examination" can expose a coached witness,[39] and if a court is convinced that there is a legitimate need for a mid-testimony consultation, making the consultation fair-game for inquiry lowers the danger that it will corrupt the proceedings. Worse still, the trial court informed the parties that the consultation would be

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

off-limits for cross-examination before it took place. In many of those cases where consultations have been upheld, the trial judges warned the parties in advance that whatever transpired would be fair-game for inquiry, which can be an effective prophylaxis against coaching. But here, if the temptation to coach Waters was brewing, the trial court's advance ruling telegraphed that there would be no chance for Buckham's counsel to uncover it.

But not all of the circumstances cut against the trial court's decision. The fact that the lawyer the court was granting Waters a chance to confer with was his own—and not the prosecutor—reduced the risk that the recess would provide the State with an opportunity coach him on his testimony. [40] And the justification the prosecutor offered for the recess —that Waters' testimony could be exposing him to criminal prosecution—was not so unfounded as to be nothing more than a pretext to get him off the stand and into a coaching session. Waters had represented as part of his plea deal that the statement he had given to investigators prior to trial was true, so if he had remained steadfast in his repudiation of that statement as he had started to do before the prosecutor asked for a recess, he risked breaching his cooperation agreement and exposing himself to further criminal prosecution for the shooting. [41] Reversing course and standing by his earlier statement would not have been a risk-free proposition either. If the statement he had given to investigators had been false, reaffirming that statement on the stand would be perjury. The risks Waters faced were varied enough—and real enough—to give credence to the prosecutor's suggestion to let him discuss these scenarios with his lawyer before going any further.

Aside from concerns about Waters, we have recognized that a lawyer who realizes ***12** her client is about to commit perjury has an ethical obligation to try to dissuade her client, and we have suggested that if it happens while the client is on the stand, she may be justified in making a "forthright application to the court for a special ruling permitting limited consultation," and the court may be justified in granting it. [42] Waters, of course, was not the prosecutor's client, but the ethical obligation to prevent a fraud on the court applies with no less force to any other witness that a lawyer calls. [43]

Whatever the merits of allowing the conference, there is no question that it cast a "cloud over the fairness of the government's trial behavior," [44] which illustrates why granting a private, mid-testimony conference treads on treacherous ground. But we need not resolve whether that decision was an abuse of the trial court's discretion, because after initially defending the decision, the State conceded at oral argument that it was error. [45]

[12] Assuming, then, that the conference should not have occurred, we turn to whether the fact that it did occur caused Buckham harm sufficient to require reversal. The State maintains that the error was harmless and does not require a new trial. We disagree.

The State contends that the conference could not have prejudiced Buckham because Waters' testimony did not materially change after he conferred with his lawyer. But the record shows otherwise. Before the recess, Waters' testimony about the day of the shooting was unequivocal. He testified that he spent the day driving around with Buckham, did not see Walker at any time that day, and had not heard any gunshots—testimony that all favored Buckham and directly contradicted the statement Waters had given to investigators on the day of his arrest. After the recess, the first question the prosecutor asked Waters was whether he remembered the day of the shooting, and this time, he responded, "Not really." [46] A few questions later, when he was asked whether he remembered telling the police on the day of his arrest that he saw Buckham shoot Walker, Waters said—apparently for the first time—that he "was under the influence" when he gave that statement and could not remember what he said. [47]

In the State's view, even if that did amount to a change—and we think there is no question that it did—it was harmless because when Waters was cross-examined, he reverted back to the testimony he had ***13** been giving before the recess. He told Buckham's counsel that he did, in fact, remember the day of the shooting and was not present when Walker was shot. He also testified that the statement he gave to police on the day of his arrest—which, apparently, he did remember making—was a lie, told to secure himself a favorable plea deal. As the State sees it, any change in his testimony after the recess had no impact on the case because by the end of cross-examination, his testimony was back to where it started.

But this line of reasoning does not give due regard to the effect that changes in a witness's story have on the witness's credibility. Had the recess not happened, the jury would have had to weigh two competing versions of events: the statement Waters gave to police on the day of his arrest (pinning the shooting on Buckham) and Waters' claim on the stand—while under oath—that the statement had been a lie, made to shift the blame to Buckham. But the recess seems to have been

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

responsible for injecting a third version of events into Waters' testimony: his claim that he had no memory of the day of the shooting and had been under the influence on the day that he spoke with the police. Waters would later abandon that new story, but the bell had been rung; the more stories a witness tells, the less believable any of them become. Rather than being presented with a witness who had a conceivable motive and explanation for fabricating a statement that pointed the finger at Buckham, the jury now had on their hands a witness who could not seem to keep his story straight, which may have led the jury to give greater weight to the statement he gave to police than to what he was saying on the stand or to simply disregard his trial testimony altogether.

[13] **[14]** **[15]** Not all errors call for reversal.[48] But to deem an error harmless—and safely disregard it—we must have a "fair assurance ... that the judgment was not substantially swayed by the error."[49] That is necessarily a case-specific inquiry; one that requires us to "scrutinize[ ] the record" to evaluate "both the importance of the error and the strength of the other evidence presented at trial."[50]

The importance of Waters' testimony is self-evident, especially in light of the wobbly testimony from Walker that immediately preceded it. Walker was the only other eyewitness, and his account of the events had varied ever since the night of the shooting. And then there's the matter of "Mr. Mel," whose presence at the scene of the crime Walker did not disclose until trial, to the surprise of both sides. In a word, Walker's testimony was problematic.

***14** In addition, there was no physical evidence linking Buckham to the shooting. No gun or shell casings were recovered. And leaving aside the arguably incriminating Facebook messages, which we will discuss in more detail in connection with the propriety of the State's search of Buckham's phone, Buckham did not make any incriminating admissions. On this record, it would be a stretch to say that evidence of Buckham's guilt was overwhelming.

So Waters' testimony—and the statement he had given to police pinning the shooting on Buckham—were of substantial importance. If the jury were to credit that statement, that would be powerful evidence that would corroborate Walker's (latest) story. But if the jury were to credit Waters' claim—under oath—that he falsified the statement to keep himself out of jail, that would do significant damage to a case that was not particularly robust. How Waters came across on the stand was a significant moment in the trial, but just as Waters' testimony was tilting toward Buckham, the trial court granted a recess. When Waters retook the stand, he brought with him a third version of events—one of memory lapse and intoxication—which he would later disavow on cross-examination.

Whether the jury would have looked at Waters' testimony differently had he not, after speaking with his lawyer, injected that third story into the mix, and whether that would have changed the outcome, we cannot say for sure. But nor can we say "with fair assurance," on the record of this case, "that the effect ... was slight, if any at all, and had no substantial influence upon the jury."[51] For that reason, the decision to allow the mid-testimony conference was reversible error.

C

Buckham also contends that allowing Waters to confer with his lawyer during his testimony and then sealing that conversation off from inquiry violated his confrontation rights under the United States and Delaware constitutions. The trial court held that the attorney-client privilege barred Buckham's counsel from cross-examining Waters about the conversation, and that, Buckham contends, allowed the privilege to trump his constitutional right of confrontation in violation of both the Confrontation Clause of the Sixth Amendment and the corresponding protection in Article I, Section 7 of the Delaware Constitution.

Whether the attorney-client privilege must give way to the defendant's right of confrontation has generated debate[52] and remains an open question at the United States Supreme Court.[53] For a trial judge ***15** who agrees to allow a prosecution witness to speak with his lawyer in the middle of testimony, the conflict between the witness's right to invoke the privilege and the defendant's right to confront him gives rise to a difficult trilemma: allow the cross-examination to proceed (letting the defendant's right of confrontation trump the attorney-client privilege); uphold the privilege and strike the testimony the witness has already given (thereby protecting both the privilege and the right of confrontation, at the expense of the evidentiary value of the witness's testimony); or, as the trial court did here, sustain the privilege-based objection, but allow the witness's prior testimony to stand (risking a violation of the defendant's right of confrontation).[54]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Because we conclude that the decision to allow the consultation to take place was reversible error, we need not take up the questions that Buckham's argument presents or determine whether the path the trial court chose in this case violated Buckham's right of confrontation.

III

To bolster the case against Buckham, the State introduced a series of Facebook messages he sent after the warrant had issued for his arrest. In one exchange, Buckham said, "people told on me"; in another, he said, "I'm hot," and when asked whether he needed to "cool down," Buckham said, "It's too late. I'm just gonna wait on them to come."[55] There were a few more to similar effect.

The police found them after executing the search warrant they obtained for Buckham's phone. The warrant authorized them to search the phone for "[a]ny and all store[d] data contained within the internal memory of the cellular phones [sic], including but not limited to, incoming/outgoing calls, missed calls, contact history, images, photographs and SMS (text) messages" for evidence of "Attempted Murder 1st Degree."

Buckham claims that the search warrant was flawed in two respects. First, he contends that the application and affidavit upon which the warrant was based did not establish probable cause to search his phone because it did not allege a sufficient nexus between the crime he was suspected of committing and his cell phone. Second, he asserts that the warrant was so overbroad and so lacking in specificity that it constitutes an unlawful "general" warrant. Buckham raised his first argument in an unsuccessful pretrial suppression motion; he raises the second argument for the first time on appeal.

The State responds that the warrant application provided numerous facts connecting Buckham's phone to the crime, the strongest of which being that the GPS data on the phone may have been able to shed light on where Buckham had been during the six weeks he was at-large, which in turn might lead police to the gun used in the shooting. The application also mentioned that the phone was found on him when he was arrested, that police were aware that he had been posting on social media about the possibility of being arrested while he was at-large, and that ***16** criminals often use cell phones to talk about their criminal activity.

A

[16] We apply the "substantial basis" test to Buckham's contention that the affidavit did not supply probable cause to believe that evidence of the crime he was suspected of committing would be found on his phone.[56] Because we pay "great deference" to the issuing magistrate's determination that the warrant was supported by probable cause,[57] "our duty is simply to ensure that the magistrate had a substantial basis for concluding that probable caused existed"[58] and that the magistrate's determination did not "reflect[ ] an improper analysis of the totality of the circumstances."[59]

[17] **[18]** **[19]** As for Buckham's challenge to the warrant's particularity and breadth, we review those questions *de novo*.[60] But because he did not raise this challenge in the Superior Court, we will take notice of an error only if it is plain.[61] Under that standard, "the error complained of must be so clearly prejudicial to substantial rights as to jeopardize the fairness and integrity of the trial process."[62]

B

[20] The Fourth Amendment to the United States Constitution and Article I, Section 6 of the Delaware Constitution provide that warrants must be supported by a showing of probable cause. For a search warrant to issue, there must be more than just probable cause that a crime has been committed; there must also be, "within the four corners of the affidavit, ... facts adequate for a judicial officer to form a reasonable belief that ... the property to be seized will be found in a particular place."[63] The constitutional requirement that there be a nexus between the crime and the place to be searched is also enshrined in Delaware law, which requires the warrant application to not only "describe the things ... sought as particularly as may be," but also to "state that ... such things are concealed in the house, place, conveyance or person designated and ... recite the facts upon which such suspicion is founded."[64]

***17** **[21]** Buckham contends that the affidavit in this case did not provide a substantial basis for the issuing magistrate to find probable cause to believe that the phone would contain any fruits, instrumentalities, or evidence of the shooting. He stresses that there was no evidence that a cell phone was used

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

as an instrumentality of the crime or that Walker and Buckham were known to communicate by phone.

Buckham is right that many of the allegations in the warrant application are too vague and too general to connect his cell phone to the shooting. Particularly unpersuasive was the statement that "criminals often communicate through cellular phones"[65] (who doesn't in this day and age?) and the statement that Waters' girlfriend—who owns the vehicle that Waters was allegedly driving on the day of the shooting—"contacted Buckham's girlfriend via cell phone" before she spoke with the police about the incident,[66] which provides no basis at all to suspect that *Buckham's* cell phone was likely to contain evidence. Nor do we see much significance in the statement that "Buckham was making posts on social media about getting arrested" while he was at-large.[67] By that time, an arrest warrant had been issued for him; the fact that Buckham may have been using his phone to talk about his impending arrest connects his phone to the arrest warrant, not the underlying crime. Even with the deference we owe to a magistrate's probable cause finding, these sorts of generalized suspicions do not provide a substantial basis to support a probable cause finding.

The affidavit seems to have left a similar impression on the trial court. The court expressed skepticism both about its generalized allegations of a nexus between cell phones and criminal activity[68] and about the inferences that could be drawn from Buckham's social media activity.[69] But the court was moved by one inferential chain in the affidavit: that GPS data from his phone might help the police determine where he had been while he was at-large and, perhaps, lead them to the gun or other evidence of the crime. That, in the court's view, created at least some nexus between the phone and the crime:

> [T]he defendant had his—potentially had his phone at the location at which he was residing and had fled to in New Jersey, and [that] potentially would have ... been sufficient probable cause to allow them to see whether or not the phone would then provide them the location of where he was staying, which potentially would lead them to evidence concerning the crime.[70]

So despite the court's view that the affidavit did only "a minimal amount of work to try to justify the warrant" and "[s]urely" could have been better,[71] the affidavit's suggestion that a search of the phone could uncover GPS data that could lead the police to further evidence was enough to uphold the magistrate's determination that there was probable cause to search. And ***18** on that basis, the court upheld the warrant. But the court failed to address the fact that the warrant it upheld was plainly mismatched to the probable cause it cited to justify it. To be fair, neither did Buckham, but the scope of the warrant so far outruns that probable cause finding—and is so lacking in particularity relative to that probable cause finding—that it qualifies as plain error.

C

We recently had the opportunity to discuss the problem of overbroad and insufficiently particular warrants issued to search electronic devices. In *Wheeler v. State*, we recognized that a warrant—no matter its target—must both "describe the things to be searched with sufficient particularity and be no broader than the probable cause on which it is based."[72] Those requirements serve to achieve the twin objectives of the warrant requirement: ensuring that "those searches deemed necessary [are] as limited as possible" and eliminating "exploratory rummaging in a person's belongings."[73] But we also recognized that warrants issued to search electronic devices call for particular sensitivity given the "enormous potential for privacy violations" that "unconstrained searches of cell phones" pose.[74] Modern smartphones store an "unprecedented volume of private information,"[75] and a top-to-bottom search of one can "permit the government access to 'far more than the most exhaustive search of a house.' "[76]

In this case, a top-to-bottom search was precisely what the warrant authorized. The police were granted the authority to search "[a]ny and all store[d] data contained within the internal memory" of the phone for evidence of the shooting. Buckham believes that makes this warrant a "general warrant"—that scourge of executive overreach "abhorred

by the colonists" that permitted "a general, exploratory rummaging in a person's belongings" [77] for vaguely-defined categories of contraband like "smuggled goods" or "obscene materials." [78]

[22] But whether or not the warrant resembles a founding-era general warrant, Buckham is correct that it does not pass muster. As we said in *Wheeler*, a warrant must "describe the items to be searched for and seized with as much particularity as the circumstances reasonably allow" and be "no broader than the probable ***19** cause on which it is based." [79] This warrant fails both requirements.

The trial court concluded that the affidavit created probable cause to search the phone for GPS data to ascertain where Buckham had been during the six weeks prior to his arrest, [80] but the warrant did not limit the search of Buckham's cell phone to any relevant time frame and authorized the search of any data on the phone. Worse still, it authorized law enforcement to search categories of data that had nothing to do with GPS location information, like "incoming/outgoing calls, missed calls, contact history, images, photographs and SMS (text) messages." [81] So this warrant was both vague about the information sought—despite the fact that a far more particularized description could have been provided—and expressly authorized the search of materials there was no probable cause to search, like the contents of all of the Facebook messages Buckham sent. For both of those reasons, the warrant is invalid, and the search for and review of the messages violated Buckham's rights under the United States and Delaware constitutions.

D

Because Buckham did not fairly raise this issue below, our inquiry is not over. We must next determine whether allowing this warrant to stand was plain error.

[23] Plain errors must be "apparent on the face of the record[,] ... basic, serious and fundamental in their character, and ... clearly deprive an accused of a substantial right, or ... clearly show manifest injustice." [82] There is no question that the flaws in the warrant are readily apparent. Once the trial court determined that the nexus between the phone and the shooting hinged on the potential for uncovering GPS data about Buckham's location, that rendered the scope of the warrant far too broad and far too vague to be propped up by that probable cause finding.

[24] We recognize that we decided *Wheeler* only a month before the trial court ruled on Buckham's suppression motion, but we judge whether an error is apparent "from the vantage point of the appellate court in reviewing the trial record, not whether it was apparent to the trial court in light of then-existing law." [83]

[25] But to be plain error, the error must be more than just apparent from the record; it must also be "so clearly prejudicial to substantial rights as to jeopardize the fairness and integrity of the trial process." [84] This means that "it must have affected the outcome of the trial." [85] That ***20** requires us to consider the significance of the error—in this case, of admitting the Facebook messages that law enforcement read while searching Buckham's phone—in light of the record as a whole. [86]

[26] As we have observed, the prosecution's case against Buckham was not iron-clad. Walker's version of events varied from not being able to identify his mystery assailants to describing in detail a gun he claimed to have seen in Buckham's hand before the shooting started. And Waters' testimony, for its part, varied from claiming that he lied when he pointed the finger at Buckham to secure himself a plea deal, to claiming to have forgotten both the day of the shooting and his statement to police, to going back to calling it a lie. Not surprisingly, then, the prosecutor told the jury that "what [the police] found out from the cell phone that was seized from David Buckham's person" would be "so important" to their decision. [87]

The mismatch between the scope of the warrant and the probable cause finding that the trial court cited to support it is readily apparent from the record, and this error led to the admission of evidence that even the State conceded was important to the trial. We conclude under these circumstances that upholding the warrant and admitting the Facebook messages that the State uncovered was plain error. [88]

IV

We reverse Buckham's convictions and remand for a new trial. [89]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

All Citations

185 A.3d 1

Footnotes

1 App. to Opening Br. A107.

2 App. to Opening Br. A129.

3 *Id.*

4 App. A105.

5 *Id.*

6 App. A108; App. A105 ("Q: So, when you indicated Mr. Waters said "Shoot him," what happened next? A: David Buckham started shooting out the window. I started running.").

7 App. A125, A127.

8 App. A152.

9 App. A153.

10 *Id.*

11 App. A154.

12 App. A155.

13 *Id.*

14 *Id.*

15 *Id.*

16 *Czech v. State*, 945 A.2d 1088, 1095 (Del. 2008) ("It is well-settled that the trial judge is responsible for the management of the trial and is vested with broad discretion to perform that function."); *Miller v. State*, 224 A.2d 592, 595 (Del. 1966) ("[T]he trial judge has wide discretion in the conduct of the trial.").

17 D.R.E. 611(a).

18 *Geders v. United States*, 425 U.S. 80, 87, 96 S.Ct. 1330, 47 L.Ed.2d 592 (1976).

19 *United States v. Sepulveda*, 15 F.3d 1161, 1176 (1st Cir. 1993) (Selya, J.).

20 John H. Wigmore, *Sequestration of Witnesses*, 14 Harv. L. Rev. 475, 475–79 (1901).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

21 *See* *Perry v. Leeke*, 488 U.S. 272, 281, 109 S.Ct. 594, 102 L.Ed.2d 624 (1989) (recognizing that "nondiscussion orders are a corollary of the broader rule that witnesses may be sequestered to lessen the danger that their testimony will be influenced by hearing what other witnesses have to say"); *United States v. Loyd*, 743 F.2d 1555, 1564 (11th Cir. 1984) (characterizing a trial court's decision to "call[ ] a recess to allow [a] prosecutor to interview [the witness]" as a "suspension of the sequestration rule").

22 *Geders*, 425 U.S. at 87, 96 S.Ct. 1330.

23 *United States v. Edwards*, 526 F.3d 747, 758 (11th Cir. 2008); *see* *Bell v. Duckworth*, 861 F.2d 169, 170 (7th Cir. 1988) (Posner, J.) ("A refusal to exclude ('separate') witnesses until they testify is not a denial of due process. Separation or sequestration of witnesses ... is a long-established and well-recognized measure designed to increase the likelihood that testimony will be candid. But the due process clause does not incorporate every refinement of legal procedure designed to make trials fairer or more accurate—not even one hallowed by time.").

24 6 Wayne R. LaFave et al., *Criminal Procedure* § 24.4(d), at 528 (4th ed. 2015); *see* *United States v. Allen*, 542 F.2d 630, 633 (4th Cir. 1976) ("While the sequestering of witnesses is of ancient origin the practice has never been universal .... In North Carolina, for example, the invocation of 'the rule on witnesses' was unheard of until very recent years.").

25 *See* D.R.E. 615 ("At the request of a party the court may order witnesses excluded so that they cannot hear the testimony of other witnesses ...."); *cf., e.g.*, Fed. R. Evid. 615 ("At a party's request, the court must order witnesses excluded so that they cannot hear other witnesses' testimony."); Vt. R. Evid. 615 ("At the request of a party the court shall order witnesses excluded so that they cannot hear the testimony of other witnesses ....").

26 *People v. Branch*, 83 N.Y.2d 663, 612 N.Y.S.2d 365, 634 N.E.2d 966, 968 (N.Y. 1994); *see also* *Perry*, 488 U.S. at 284, 109 S.Ct. 594 (recognizing, in the context of a defendant-witness, that whether to permit a mid-testimony consultation is "a matter of discretion in individual cases"); *Loyd*, 743 F.2d at 1564 (recognizing, in the context of a prosecution witness, that "[t]he decision whether to [call a recess to] allow a prosecutor to 'work with' a witness is within the discretion of the trial court and will not be reviewed absent an abuse of that discretion").

27 *Webb v. State*, 663 A.2d 452, 460 n.9 (Del. 1995) (speaking to the propriety of a mid-cross-examination consultation between a defendant and his lawyer).

28 D.R.E. 611(a)(1).

29 *Webb*, 663 A.2d at 459.

30 *Branch*, 612 N.Y.S.2d 365, 634 N.E.2d at 967.

31 *People v. Pendleton*, 75 Ill.App.3d 580, 31 Ill.Dec. 294, 394 N.E.2d 496, 507 (1979).

32 *Duke v. United States*, 255 F.2d 721, 728 (9th Cir. 1958).

33 *See* *Geders*, 425 U.S. at 90, 96 S.Ct. 1330 ("[T]he trial judge, if he doubts that defense counsel will observe the ethical limits on guiding witnesses, may direct that the examination of the witness continue

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

without interruption until completed. If the judge considers the risk high he may arrange the sequence of testimony so that direct- and cross-examination of a witness will be completed without interruption.").

34 That neither Waters nor his counsel saw fit to request a recess distinguishes these circumstances from those where a witness (or the witness's lawyer) seeks a recess for the purpose of discussing whether to assert a privilege. *Cf*. Del. Super. Ct. Civ. R. P. 30(d)(1) (providing, in the context of civil depositions, that "[f]rom the commencement until the conclusion of a deposition, ... the attorney(s) for the deponent shall not ... consult or confer with the deponent regarding the substance of the testimony already given or anticipated to be given *except for the purpose of conferring on whether to assert a privilege against testifying* or on how to comply with a court order" (emphasis added)).

35 743 F.2d 1555 (11th Cir. 1984).

36 543 N.E.2d 669, 673 (Ind. Ct. App. 1989).

37 App. A154.

38 *See, e.g.*, *United States v. Malik*, 800 F.2d 143, 148 (7th Cir. 1986) ("The Assistant United States Attorney invited cross-examination ... of [the witness] about the conversation."); *Loyd*, 743 F.2d at 1564 ("[D]efense counsel had ample opportunity to cross-examine [the witness] about the interview by the prosecutor, yet no counsel was able to establish that [he] was coached."); *Branch*, 612 N.Y.S.2d 365, 634 N.E.2d at 968 ("[T]he court allowed the defense the opportunity to cross-examine the witness about the conference and about the change in testimony."); *Frierson*, 543 N.E.2d at 673 ("[D]efense counsel had the opportunity on cross-examination to explore any unfair coaching he suspected took place during the brief recess.").

39 *Geders*, 425 U.S. at 89–90, 96 S.Ct. 1330.

40 *Cf*. 6 John Henry Wigmore, *Evidence in Trials at Common Law* § 1841, at 472 (James H. Chadbourn rev., 1976) (proposing that trial courts should not allow private discussions between a witness and "an attorney *in the cause*" (emphasis added)).

41 By the time of Buckham's trial, Waters had already been sentenced on the charge he agreed to accept under his plea agreement, but that charge—second-degree conspiracy—related only to the mid-September drive-by, not to the August 3 shooting, and his written plea agreement made no promises that the State would spare him from liability for the shooting. So disavowing his earlier statement to investigators risked leading the State to respond to his breach of the cooperation agreement by deciding to charge him in connection with the shooting.

42 *Webb*, 663 A.2d at 460 n.9.

43 *See* Del. R. Prof. Conduct 3.3 cmt. 10 ("[A] lawyer may be surprised when the lawyer's client, or another witness called by the lawyer, offers testimony the lawyer knows to be false, either during the lawyer's direct examination or in response to cross examination by the opposing lawyer. In such situations ..., the lawyer must take reasonable remedial measures. In such situations, the advocate's proper course is to remonstrate with the client confidentially, advise the client of the lawyer's duty of candor to the tribunal and seek the client's cooperation with respect to the withdrawal or correction of the false statements or evidence.").

44 *Malik*, 800 F.2d at 149.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

45 Oral Argument at 39:13 (Jan. 24, 2018), http://livestream.com/accounts/5969852/events/8024893/videos/169188865 (Justice Traynor: "Does the State concede that it was abuse of discretion to allow the recess for the communication?" A: ".... The State would concede that it was an error for the judge to allow this to happen.... It's difficult to concede an error like that by the trial judge when it was the prosecutor who brought the issue up and created the situation, but the State would concede that it was an error.").

46 App. A155.

47 *Id.*

48 *See* Del. Super. Ct. Crim. R. P. 52(a) (providing that harmless errors—that is, "[a]ny error, defect, irregularity or variance which does not affect substantial rights"—"shall be disregarded").

49 *Ashley v. State*, 798 A.2d 1019, 1023 n.17 (Del. 2002) (per curiam) (quoting *Kotteakos v. United States*, 328 U.S. 750, 765, 66 S.Ct. 1239, 90 L.Ed. 1557 (1946)). As we have explained, no party—not even a criminal defendant—has a constitutional right to any particular type of witness sequestration, so even if a trial court abuses its discretion by allowing a witness to consult with a lawyer in the middle of testimony, that error is not of constitutional magnitude and is not subject to the more rigorous form of harmless error review that applies to trial errors that infringe upon constitutional rights. *See* *Capano v. State*, 781 A.2d 556, 597 n.54 (Del. 2001) (recognizing the distinction between constitutional and non-constitutional errors and explaining that when a trial court makes an error "of a constitutional magnitude, the conviction[ ] may be sustained [only] if the error is 'harmless beyond a reasonable doubt' ").

50 *Van Arsdall v. State*, 524 A.2d 3, 10–11 (Del. 1987).

51 *Hutchins v. State*, 153 A.2d 204, 208 (Del. 1959).

52 *See, e.g.*, *Murdoch v. Castro*, 609 F.3d 983, 993–95 (9th Cir. 2010) (en banc) (plurality opinion) ("[N]o Supreme Court case has directly addressed the potential conflict between state-law attorney-client privilege and the Confrontation Clause .... The Supreme Court might well decide that it is worthy of greater protection than the marital privilege or the confidentiality of juvenile delinquency proceedings." (citations omitted)); *id.* at 1004 (Kozinki, J., dissenting) ("Even if the attorney-client privilege were of the same dignity as the Fifth Amendment, the need for 'cross-examination and impeachment' would overcome it."); *see generally* 24 Charles Alan Wright and Kenneth W. Graham, Jr., *Federal Practice and Procedure* § 5506, at 566 (1st ed. 1986) (suggesting that "the attorney-client privilege ... may have to yield when it comes in conflict with the constitutional right of a criminal defendant," but that while [t]his possibility is acknowledged in the cases, ... it is not a frequent occurrence," and collecting cases).

53 *See* *Swidler & Berlin v. United States*, 524 U.S. 399, 408 n.3, 118 S.Ct. 2081, 141 L.Ed.2d 379 (1998) ("Petitioners, while opposing wholesale abrogation of the privilege in criminal cases, concede that exceptional circumstances implicating a criminal defendant's constitutional rights might warrant breaching the privilege. We do not, however, need to reach this issue, since such exceptional circumstances clearly are not presented here.").

54 *See* *Murdoch*, 609 F.3d at 1005 (Kozinski, J., dissenting) (discussing these alternatives).

55 App. A192, A194.

56 *See* *Sisson v. State*, 903 A.2d 288, 296 (Del. 2006).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

57 *Jensen v. State*, 482 A.2d 105, 111 (Del. 1984).

58 *Sisson*, 903 A.2d at 296.

59 *LeGrande v. State*, 947 A.2d 1103, 1108 (Del. 2008) (quoting *United States v. Leon*, 468 U.S. 897, 915, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)).

60 *See* *Wheeler v. State*, 135 A.3d 282, 295, 302 (Del. 2016) (confronting a claim that search warrants for electronic devices were "in the nature of a general warrant, unconstitutionally overbroad, and lack[ed] sufficient particularity").

61 After conceding in his opening brief and at oral argument before a three-Justice panel of this Court that he had not raised this claim below, Buckham argued to the Court *en Banc* that he had. Although his counsel made a passing reference during the suppression hearing to the concept of general warrants and to our recent decision in *Wheeler v. State*, 135 A.3d 282 (Del. 2016), which addressed the problem of overbroad and insufficiently particular electronic-device warrants, his motion did not mention this issue, and the trial court did not rule on it. We are unpersuaded by Buckham's belated effort to secure a more favorable standard of review.

62 *Wainwright v. State*, 504 A.2d 1096, 1100 (Del. 1986).

63 *Sisson*, 903 A.2d at 296.

64 11 *Del. C.* § 2306.

65 App. A34.

66 App. A33.

67 App. A34.

68 *See* App. A76–77 ("[I]f all I had was I know about cell phones, and cell phones can do this, I [would] have real concerns about that being an adequate warrant.").

69 *See* App. A76 (commenting that while the affidavit alleged that Buckham had done "some posting," "I think the defense has done a good job of persuading me that perhaps that's not as significant as I initially thought it was").

70 *Id.*

71 App. A77–78.

72 *Wheeler v. State*, 135 A.3d 282, 299 (Del. 2016).

73 *Id.* at 298 (alteration in original) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971)).

74 *Id.* at 299 (citing *Riley v. California*, —— U.S. ——, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014)); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important."); 2 Wayne R. LaFave, *Search and Seizure* § 4.6(a),

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

at 774 (5th ed. 2012 & Supp. 2017) ("The greatest care in [drafting a warrant's] description is required when the consequences of seizure of innocent articles by mistake is most substantial, as ... where the place to be searched is a cell phone ....").

75 *Id.*

76 *Id.* (quoting *Riley*, 134 S.Ct. at 2491).

77 *Id.* at 296 (quoting *Coolidge*, 403 U.S. at 467, 91 S.Ct. 2022).

78 *United States v. Ninety–Two Thousand Four Hundred Twenty–Two Dollars and Fifty–Seven Cents*, 307 F.3d 137, 149 (3d Cir. 2002) (Alito, J.).

79 135 A.3d at 299, 305.

80 We express no opinion on the correctness of that conclusion or, more generally, the notion that a warrant to search a cell phone for GPS data can issue upon a showing that law enforcement cannot account for a suspect's whereabouts prior to an arrest and believe that the GPS data may lead them to another place to search for evidence. We conclude simply that the warrant was plainly too broad and too lacking in particulars to be supported by the trial court's probable-cause determination.

81 App. A31. We are aware that modern smartphones can tag photographs with GPS-based location information, but that would at most justify an examination of the metadata of any photographs retrieved from the phone to see whether it contained location information.

82 *Wainwright*, 504 A.2d at 1100.

83 *Capano*, 781 A.2d at 663.

84 *Williams v. State*, 796 A.2d 1281, 1284 (Del. 2002).

85 *Morgan v. State*, 962 A.2d 248, 254 (Del. 2008).

86 *See* *Wainwright*, 504 A.2d at 1100–01.

87 App. A77–78.

88 *See* *Henry v. State*, 373 A.2d 575, 576 n.1 (Del. 1977) ("We regard the failure to comply with the [night-time warrant] statute as plain error ....").

89 Before this Court, Buckham also argued that the trial court abused its discretion in denying his request for a mistrial after the lead detective mentioned his nickname, which the parties and the trial court agreed before trial was not to be used because of its possible prejudicial effect. We need not reach the substance of Buckham's argument on this issue because of our decision to reverse and remand, but we assume that on retrial the improper mention of Buckham's nickname will not recur.

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

KeyCite Yellow Flag - Negative Treatment
Not Followed on State Law Grounds State v. Wright, Iowa, June 18, 2021

108 S.Ct. 1625
Supreme Court of the United States

CALIFORNIA, Petitioner
v.
Billy GREENWOOD and Dyanne Van Houten.

No. 86–684.
|
Argued Jan. 11, 1988.
|
Decided May 16, 1988.

Synopsis
State appealed from order of the Superior Court which dismissed drug charges against defendants. The California Court of Appeal, 182 Cal.App.3d 729, 227 Cal.Rptr. 539, affirmed, and certiorari was granted. The Supreme Court, Justice White, held that defendants did not have reasonable expectation of privacy protected by the Fourth Amendment in garbage which they placed in opaque bags outside their house for collection by trash collector.

Reversed and remanded.

Justice Brennan dissented and filed an opinion in which Justice Marshall joined.

Justice Kennedy did not participate.

Procedural Posture(s): On Appeal.

West Headnotes (8)

[1] **Searches and Seizures** Abandoned, surrendered, or disclaimed items

Fourth Amendment does not prohibit the warrantless search or seizure of garbage left for collection outside the curtilage of a home. U.S.C.A. Const.Amend. 4.

174 Cases that cite this headnote

[2] **Searches and Seizures** Abandoned, surrendered, or disclaimed items

Warrantless search and seizure of garbage bags left at curb outside of house would violate Fourth Amendment only if there were manifestation of a subjective expectation of privacy in the garbage which society would accept as objectively reasonable. U.S.C.A. Const.Amend. 4.

557 Cases that cite this headnote

[3] **Searches and Seizures** Expectation of privacy

Expectation of privacy does not give rise to Fourth Amendment protection unless society is prepared to accept that expectation as subjectively reasonable. U.S.C.A. Const.Amend. 4.

169 Cases that cite this headnote

[4] **Searches and Seizures** Abandoned, surrendered, or disclaimed items

Residents of house sufficiently exposed their garbage to the public to defeat their claim to Fourth Amendment protection by placing the garbage in opaque bags at the curbside for pickup by a trash collector; residents of the house could have no reasonable expectation or privacy in the inculpatory items which they discarded. U.S.C.A. Const.Amend. 4.

465 Cases that cite this headnote

[5] **Criminal Law** Judicial Notice

It is common knowledge that plastic garbage bags left on or at the site of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public.

79 Cases that cite this headnote

[6] **Searches and Seizures** Abandoned, surrendered, or disclaimed items

Fact that state Supreme Court had announced a right to privacy in garbage left outside the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

home for collection did not make expectation of privacy in the garbage reasonable so as to entitle it to Fourth Amendment protection. U.S.C.A. Const.Amend. 4.

501 Cases that cite this headnote

[7] **States** Particular provisions

Individual states may construe their own Constitutions as imposing more stringent constraints on police conduct than does the Federal Constitution. U.S.C.A. Const.Amend. 4.

44 Cases that cite this headnote

[8] **Constitutional Law** Improperly obtained evidence; suppression

Criminal Law Searches, seizures, and arrests

California constitutional amendment which eliminates the exclusionary rule for evidence seized in violation of state, but not federal, law does not violate the due process clause. U.S.C.A. Const.Amend. 14; West's Ann.Cal. Const. Art. 1, § 28(d).

24 Cases that cite this headnote

****1626 *35** *Syllabus* *

Acting on information indicating that respondent Greenwood might be engaged in narcotics trafficking, police twice obtained from his regular trash collector garbage bags left on the curb in front of his house. On the basis of items in the bags which were indicative of narcotics use, the police obtained warrants to search the house, discovered controlled substances during the searches, and arrested respondents on felony narcotics charges. Finding that probable cause to search the house would not have existed without the evidence obtained from the trash searches, the State Superior Court dismissed the charges under *People v. Krivda, 5 Cal.3d 357, 96 Cal.Rptr. 62, 486 P.2d 1262,* which held that warrantless trash searches violate the Fourth Amendment and the California Constitution. Although noting a post-*Krivda* state constitutional amendment eliminating the exclusionary rule for evidence seized in violation of state, but not federal, law, the State Court of Appeal affirmed on the ground that *Krivda* was based on federal, as well as state, law.

Held:

1. The Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home. Pp. 1628–1631.

(a) Since respondents voluntarily left their trash for collection in an area particularly suited for public inspection, their claimed expectation of privacy in the inculpatory items they discarded was not objectively reasonable. It is common knowledge that plastic garbage bags left along a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through it or permitted others, such as the police, to do so. The police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public. Pp. 1628–1630.

(b) Greenwood's alternative argument that his expectation of privacy in his garbage should be deemed reasonable as a matter of federal constitutional law because the warrantless search and seizure of his garbage was impermissible as a matter of California law under *Krivda,* ***36** which he contends survived the state constitutional amendment, is without merit. The reasonableness of a search for Fourth Amendment purposes does not depend upon privacy concepts embodied in the law of the particular State in which the search occurred; rather, it turns upon the understanding of society as a whole that certain areas deserve the most scrupulous protection from government invasion. There is no such understanding with respect to garbage left for collection at the side of a public street. Pp. 1629–1630.

2. Also without merit is Greenwood's contention that the California constitutional amendment violates the Due Process Clause of the Fourteenth Amendment. Just as this Court's Fourth Amendment exclusionary rule decisions have not required ****1627** suppression where the benefits of deterring minor police misconduct were overbalanced by the societal costs of exclusion, California was not foreclosed by the Due Process Clause from concluding that the benefits of excluding relevant evidence of criminal activity do not outweigh the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

costs when the police conduct at issue does not violate federal law. P. 1631.

182 Cal.App.3d 729, 227 Cal.Rptr. 539 (1986), reversed and remanded.

WHITE, J., delivered the opinion of the Court, in which REHNQUIST, C.J., and BLACKMUN, STEVENS, O'CONNOR, and SCALIA, JJ., joined. BRENNAN, J., filed a dissenting opinion, in which MARSHALL, J., joined, *post,* p. ——. KENNEDY, J., took no part in the consideration or decision of the case.

Attorneys and Law Firms

Michael J. Pear argued the cause for petitioner. With him on the briefs were *Cecil Hicks* and *Michael R. Capizzi.*

Michael Ian Garey, by appointment of the Court, 484 U.S. 808, argued the cause for respondents and filed a brief for respondent Greenwood. *Richard L. Schwartzberg* filed a brief for respondent Van Houten.*

* Briefs of *amici curiae* urging reversal were filed for the State of California et al. by *John K. Van de Kamp,* Attorney General of California, *Steve White,* Chief Assistant Attorney General, *John H. Sugiyama,* Senior Assistant Attorney General, *Ronald E. Niver* and *Laurence K. Sullivan,* Supervising Deputy Attorneys General, and by the Attorneys General for their respective States as follows: *Robert Butterworth* of Florida, *Warren Price III* of Hawaii, *Linley E. Pearson* of Indiana, *David L. Armstrong* of Kentucky, *Hubert H. Humphrey III* of Minnesota, *LeRoy S. Zimmerman* of Pennsylvania, *Travis Medlock* of South Carolina, *W.J. Michael Cody* of Tennessee, *Kenneth O. Eikenberry* of Washington, *Donald J. Hanaway* of Wisconsin, and *Joseph B. Meyer* of Wyoming; and for Americans for Effective Law Enforcement, Inc., et al. by *Fred E. Inbau, Wayne W. Schmidt, James P. Manak, David Crump, Courtney A. Evans, Daniel B. Hales,* and *Jack E. Yelverton.*

Opinion

***37** Justice WHITE delivered the opinion of the Court.

[1] The issue here is whether the Fourth Amendment prohibits the warrantless search and seizure of garbage left for collection outside the curtilage of a home. We conclude, in accordance with the vast majority of lower courts that have addressed the issue, that it does not.

I

In early 1984, Investigator Jenny Stracner of the Laguna Beach Police Department received information indicating that respondent Greenwood might be engaged in narcotics trafficking. Stracner learned that a criminal suspect had informed a federal drug enforcement agent in February 1984 that a truck filled with illegal drugs was en route to the Laguna Beach address at which Greenwood resided. In addition, a neighbor complained of heavy vehicular traffic late at night in front of Greenwood's single-family home. The neighbor reported that the vehicles remained at Greenwood's house for only a few minutes.

Stracner sought to investigate this information by conducting a surveillance of Greenwood's home. She observed several vehicles make brief stops at the house during the late-night and early morning hours, and she followed a truck from the house to a residence that had previously been under investigation as a narcotics-trafficking location.

On April 6, 1984, Stracner asked the neighborhood's regular trash collector to pick up the plastic garbage bags that Greenwood had left on the curb in front of his house and to turn the bags over to her without mixing their contents with garbage from other houses. The trash collector cleaned his truck bin of other refuse, collected the garbage bags from the street in front of Greenwood's house, and turned the bags over to Stracner. The officer searched through the rubbish ***38** and found items indicative of narcotics use. She recited the information that she had gleaned from the trash search in an affidavit in support of a warrant to search Greenwood's home.

Police officers encountered both respondents at the house later that day when they arrived to execute the warrant. The police discovered quantities of cocaine and hashish during their search of the house. Respondents were arrested on felony narcotics charges. They subsequently posted bail.

The police continued to receive reports of many late-night visitors to the Greenwood house. On May 4, Investigator Robert Rahaeuser obtained Greenwood's garbage from the regular trash collector in the same manner as had Stracner. The garbage again contained evidence of narcotics use.

Rahaeuser secured another search warrant for Greenwood's home based on the information from the second trash

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

search. The police found more narcotics and evidence of narcotics trafficking when they **1628 executed the warrant. Greenwood was again arrested.

The Superior Court dismissed the charges against respondents on the authority of *People v. Krivda,* 5 Cal.3d 357, 96 Cal.Rptr. 62, 486 P.2d 1262 (1971), which held that warrantless trash searches violate the Fourth Amendment and the California Constitution. The court found that the police would not have had probable cause to search the Greenwood home without the evidence obtained from the trash searches.

The Court of Appeal affirmed. 182 Cal.App.3d 729, 227 Cal.Rptr. 539 (1986). The court noted at the outset that the fruits of warrantless trash searches could no longer be suppressed if *Krivda* were based only on the California Constitution, because since 1982 the State has barred the suppression of evidence seized in violation of California law but not federal law. See Cal. Const., Art. I, § 28(d); *In re Lance W.,* 37 Cal.3d 873, 210 Cal.Rptr. 631, 694 P.2d 744 (1985). But *Krivda,* a decision binding on the Court of Appeal, also held that the fruits of warrantless trash searches were to be excluded under federal *39 law. Hence, the Superior Court was correct in dismissing the charges against respondents. 182 Cal.App.3d, at 735, 227 Cal.Rptr. at 542. [1]

The California Supreme Court denied the State's petition for review of the Court of Appeal's decision. We granted certiorari, 483 U.S. 1019, 107 S.Ct. 3260, 97 L.Ed.2d 760 and now reverse.

II

[2] The warrantless search and seizure of the garbage bags left at the curb outside the Greenwood house would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable. *O'Connor v. Ortega,* 480 U.S. 709, 715, 107 S.Ct. 1492, 1496, 94 L.Ed.2d 714 (1987); *California v. Ciraolo,* 476 U.S. 207, 211, 106 S.Ct. 1809, 1811, 90 L.Ed.2d 210 (1986); *Oliver v. United States,* 466 U.S. 170, 177, 104 S.Ct. 1735, 1740, 80 L.Ed.2d 214 (1984); *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 516, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). Respondents do not disagree with this standard.

They assert, however, that they had, and exhibited, an expectation of privacy with respect to the trash that was searched by the police: The trash, which was placed on the street for collection at a fixed time, was contained in opaque plastic bags, which the garbage collector was expected to pick up, mingle with the trash of others, and deposit at the garbage dump. The trash was only temporarily on the street, and there was little likelihood that it would be inspected by anyone.

[3] It may well be that respondents did not expect that the contents of their garbage bags would become known to the police or other members of the public. An expectation of privacy does not give rise to Fourth Amendment protection, *40 however, unless society is prepared to accept that expectation as objectively reasonable.

[4] [5] Here, we conclude that respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection. It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, [2] children, scavengers, **1629 [3] snoops, [4] and other members of the public. See *Krivda, supra,* 5 Cal.3d, at 367, 96 Cal.Rptr., at 69, 486 P.2d, at 1269. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so. Accordingly, having deposited their garbage "in an area particularly suited for *41 public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it," *United States v. Reicherter,* 647 F.2d 397, 399 (CA3 1981), respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded.

Furthermore, as we have held, the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public. Hence, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz v. United States, supra,* 389 U.S. at 351, 88 S.Ct., at 511. We held in *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), for example, that the police did not violate the Fourth

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Amendment by causing a pen register to be installed at the telephone company's offices to record the telephone numbers dialed by a criminal suspect. An individual has no legitimate expectation of privacy in the numbers dialed on his telephone, we reasoned, because he voluntarily conveys those numbers to the telephone company when he uses the telephone. Again, we observed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.,* at 743–744, 99 S.Ct., at 2582.

Similarly, we held in *California v. Ciraolo, supra,* that the police were not required by the Fourth Amendment to obtain a warrant before conducting surveillance of the respondent's fenced backyard from a private plane flying at an altitude of 1,000 feet. We concluded that the respondent's expectation that his yard was protected from such surveillance was unreasonable because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed." *Id.,* 476 U.S., at 213–214, 106 S.Ct., at 1813.

Our conclusion that society would not accept as reasonable respondents' claim to an expectation of privacy in trash left for collection in an area accessible to the public is reinforced by the unanimous rejection of similar claims by the Federal Courts of Appeals. See *United States v. Dela Espriella,* ***42** 781 F.2d 1432, 1437 (CA9 1986); *United States v. O'Bryant,* 775 F.2d 1528, 1533–1534 (CA11 1985); *United States v. Michaels,* 726 F.2d 1307, 1312–1313 (CA8), cert. denied, 469 U.S. 820, 105 S.Ct. 92, 83 L.Ed.2d 38 (1984); *United States v. Kramer,* 711 F.2d 789, 791–794 (CA7), cert. denied, 464 U.S. 962, 104 S.Ct. 397, 78 L.Ed.2d 339 (1983); *United States v. Terry,* 702 F.2d 299, 308–309 (CA2), cert. denied ****1630** *sub nom. Williams v. United States,* 461 U.S. 931, 103 S.Ct. 2095, 77 L.Ed.2d 304 (1983); *United States v. Reicherter, supra,* at 399; *United States v. Vahalik,* 606 F.2d 99, 100–101 (CA5 1979) (*per curiam*), cert. denied, 444 U.S. 1081, 100 S.Ct. 1034, 62 L.Ed.2d 765 (1980); *United States v. Crowell,* 586 F.2d 1020, 1025 (CA4 1978), cert. denied, 440 U.S. 959, 99 S.Ct. 1500, 59 L.Ed.2d 772 (1979); *Magda v. Benson,* 536 F.2d 111, 112–113 (CA6 1976) (*per curiam*); *United States v. Mustone,* 469 F.2d 970, 972–974 (CA1 1972). In *United States v. Thornton,* 241 U.S.App.D.C. 46, 56, and n. 11, 746 F.2d 39, 49, and n. 11 (1984), the court observed that "the overwhelming weight of authority rejects the proposition that a reasonable expectation of privacy exists with respect to trash discarded outside the home and the curtilege [*sic*] thereof." In addition, of those state appellate courts that have considered the issue, the vast majority have held that the police may conduct warrantless searches and seizures of garbage discarded in public areas. See *Commonwealth v. Chappee,* 397 Mass. 508, 512–513, 492 N.E.2d 719, 721–722 (1986); *Cooks v. State,* 699 P.2d 653, 656 (Okla.Crim.), cert. denied, 474 U.S. 935, 106 S.Ct. 268, 88 L.Ed.2d 275 (1985); *State v. Stevens,* 123 Wis.2d 303, 314–317, 367 N.W.2d 788, 794–797, cert. denied, 474 U.S. 852, 106 S.Ct. 151, 88 L.Ed.2d 125 (1985); *State v. Ronngren,* 361 N.W.2d 224, 228–230 (N.D.1985); *State v. Brown,* 20 Ohio App.3d 36, 37–38, 484 N.E.2d 215, 217–218 (1984); *State v. Oquist,* 327 N.W.2d 587 (Minn.1982); *People v. Whotte,* 113 Mich.App. 12, 317 N.W.2d 266 (1982); *Commonwealth v. Minton,* 288 Pa.Super. 381, 391, 432 A.2d 212, 217 (1981); *State v. Schultz,* 388 So.2d 1326 (Fla.App.1980); *People v. Huddleston,* 38 Ill.App.3d 277, 347 N.E.2d 76 (1976); *Willis v. State,* 518 S.W.2d 247, 249 (Tex.Crim.App.1975); *Smith v. State,* 510 P.2d 793 (Alaska), cert. denied, ***43** 414 U.S. 1086, 94 S.Ct. 603, 38 L.Ed.2d 489 (1973); *State v. Fassler,* 108 Ariz. 586, 592–593, 503 P.2d 807, 813–814 (1972); *Croker v. State,* 477 P.2d 122, 125–126 (Wyo.1970); *State v. Purvis,* 249 Ore. 404, 411, 438 P.2d 1002, 1005 (1968). But see *State v. Tanaka,* 67 Haw. 658, 701 P.2d 1274 (1985); *People v. Krivda,* 5 Cal.3d 357, 96 Cal.Rptr. 62, 486 P.2d 1262 (1971). [5]

III

[6] We reject respondent Greenwood's alternative argument for affirmance: that his expectation of privacy in his garbage should be deemed reasonable as a matter of federal constitutional law because the warrantless search and seizure of his garbage was impermissible as a matter of California law. He urges that the state-law right of Californians to privacy in their garbage, announced by the California Supreme Court in *Krivda, supra,* survived the subsequent

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

state constitutional amendment eliminating the suppression remedy as a means of enforcing that right. See *In re Lance W.,* 37 Cal.3d, at 886–887, 210 Cal.Rptr., at 639–640, 694 P.2d, at 752–753. Hence, he argues that the Fourth Amendment should itself vindicate that right.

[7] Individual States may surely construe their own constitutions as imposing more stringent constraints on police conduct than does the Federal Constitution. We have never intimated, however, that whether or not a search is reasonable within the meaning of the Fourth Amendment depends on the law of the particular State in which the search occurs. We have emphasized instead that the Fourth Amendment analysis must turn on such factors as "our *societal* understanding that certain areas deserve the most scrupulous protection from government invasion." *Oliver v. United States,* 466 U.S., at 178, 104 S.Ct., at 1741 (emphasis added). See also *Rakas v. Illinois,* 439 U.S. 128, 143–144, n. 12, 99 S.Ct. 421, 430–431, n. 12, 58 L.Ed.2d 387 (1978). We have already concluded that society as a whole possesses no such un ****1631** derstanding ***44** with regard to garbage left for collection at the side of a public street. Respondent's argument is no less than a suggestion that concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment. We do not accept this submission.

IV

[8] Greenwood finally urges as an additional ground for affirmance that the California constitutional amendment eliminating the exclusionary rule for evidence seized in violation of state but not federal law violates the Due Process Clause of the Fourteenth Amendment. In his view, having recognized a state-law right to be free from warrantless searches of garbage, California may not under the Due Process Clause deprive its citizens of what he describes as "the only effective deterrent" to violations of this right. Greenwood concedes that no direct support for his position can be found in the decisions of this Court. He relies instead on cases holding that individuals are entitled to certain procedural protections before they can be deprived of a liberty or property interest created by state law. See *Hewitt v. Helms,* 459 U.S. 460, 103 S.Ct. 864, 74 L.Ed.2d 675 (1983); *Vitek v. Jones,* 445 U.S. 480, 100 S.Ct. 1254, 63 L.Ed.2d 552 (1980).

We see no merit in Greenwood's position. California could amend its Constitution to negate the holding in *Krivda* that state law forbids warrantless searches of trash. We are convinced that the State may likewise eliminate the exclusionary rule as a remedy for violations of that right. At the federal level, we have not required that evidence obtained in violation of the Fourth Amendment be suppressed in all circumstances. See, *e.g., United States v. Leon,* 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984); *United States v. Janis,* 428 U.S. 433, 96 S.Ct. 3021, 49 L.Ed.2d 1046 (1976); *United States v. Calandra,* 414 U.S. 338, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974). Rather, our decisions concerning the scope of the Fourth Amendment exclusionary rule have balanced the benefits of deterring police misconduct against the costs of excluding reliable evidence of criminal activity. See *Leon,* 468 U.S., at 908–913, 104 S.Ct., at 3412–3415. We ***45** have declined to apply the exclusionary rule indiscriminately "when law enforcement officers have acted in objective good faith or their transgressions have been minor," because "the magnitude of the benefit conferred on ... guilty defendants [in such circumstances] offends basic concepts of the criminal justice system." *Id.,* at 908, 104 S.Ct. at 3412 (citing *Stone v. Powell,* 428 U.S. 465, 490, 96 S.Ct. 3037, 3050, 49 L.Ed.2d 1067 (1976)).

The States are not foreclosed by the Due Process Clause from using a similar balancing approach to delineate the scope of their own exclusionary rules. Hence, the people of California could permissibly conclude that the benefits of excluding relevant evidence of criminal activity do not outweigh the costs when the police conduct at issue does not violate federal law.

V

The judgment of the California Court of Appeal is therefore reversed, and this case is remanded for further proceedings not inconsistent with this opinion.

It is so ordered.

Justice KENNEDY took no part in the consideration or decision of this case.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Justice BRENNAN, with whom Justice MARSHALL joins, dissenting.

Every week for two months, and at least once more a month later, the Laguna Beach police clawed through the trash that respondent Greenwood left in opaque, sealed bags on the curb outside his home. Record 113. Complete strangers minutely scrutinized their bounty, undoubtedly dredging up intimate details of Greenwood's private life and habits. The intrusions proceeded without a warrant, and no court before or since has concluded that the police acted on probable cause to believe **1632 Greenwood was engaged in any criminal activity.

Scrutiny of another's trash is contrary to commonly accepted notions of civilized behavior. I suspect, therefore, *46 that members of our society will be shocked to learn that the Court, the ultimate guarantor of liberty, deems unreasonable our expectation that the aspects of our private lives that are concealed safely in a trash bag will not become public.

I

"A container which can support a reasonable expectation of privacy may not be searched, even on probable cause, without a warrant." *United States v. Jacobsen,* 466 U.S. 109, 120, n. 17, 104 S.Ct. 1652, 1660, n. 17, 80 L.Ed.2d 85 (1984) (citations omitted). Thus, as the Court observes, if Greenwood had a reasonable expectation that the contents of the bags that he placed on the curb would remain private, the warrantless search of those bags violated the Fourth Amendment. *Ante,* at ——.

The Framers of the Fourth Amendment understood that "unreasonable searches" of "paper[s] and effects"—no less than "unreasonable searches" of "person[s] and houses"—infringe privacy. As early as 1878, this Court acknowledged that the contents of "[l]etters and sealed packages ... in the mail are as fully guarded from examination and inspection ... as if they were retained by the parties forwarding them in their own domiciles." *Ex parte Jackson,* 96 U.S. (6 Otto) 727, 733, 24 L.Ed. 877. In short, so long as a package is "closed against inspection," the Fourth Amendment protects its contents, "wherever they may be," and the police must obtain a warrant to search it just "as is required when papers are subjected to search in one's own household." *Ibid.* Accord, *United States v. Van Leeuwen,* 397 U.S. 249, 90 S.Ct. 1029, 25 L.Ed.2d 282 (1970).

With the emergence of the reasonable-expectation-of-privacy analysis, see *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 516, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring); *Smith v. Maryland,* 442 U.S. 735, 740, 99 S.Ct. 2577, 2580, 61 L.Ed.2d 220 (1979), we have reaffirmed this fundamental principle. In *Robbins v. California,* 453 U.S. 420, 101 S.Ct. 2841, 69 L.Ed.2d 744 (1981), for example, Justice Stewart, writing for a plurality of four, pronounced that "unless the container is such that its contents may be said to be in plain view, those contents are fully *47 protected by the Fourth Amendment," *id.,* at 427, 101 S.Ct., at 2846, and soundly rejected any distinction for Fourth Amendment purposes among various opaque, sealed containers:

> "[E]ven if one wished to import such a distinction into the Fourth Amendment, it is difficult if not impossible to perceive any objective criteria by which that task might be accomplished. What one person may put into a suitcase, another may put into a paper bag.... And ... no court, no constable, no citizen, can sensibly be asked to distinguish the relative 'privacy interests' in a closed suitcase, briefcase, portfolio, duffelbag, or box." *Id.,* at 426–427, 101 S.Ct., at 2846.

See also *id.,* at 428, 101 S.Ct., at 2847 (expectation of privacy attaches to any container unless it "so clearly announce[s] its contents, whether by its distinctive configuration, its transparency, or otherwise, that its contents are obvious to an observer"). With only one exception, every Justice who wrote in that case eschewed any attempt to distinguish "worthy" from "unworthy" containers. [1]

**1633 More recently, in *United States v. Ross,* 456 U.S. 798, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982), the Court, relying on the "virtually unanimous agreement *48 in *Robbins* ... that a constitutional distinction between 'worthy' and 'unworthy' containers would be improper," held that a distinction among "paper bags, locked trunks, lunch buckets, and orange crates" would be inconsistent with

> "the central purpose of the Fourth Amendment.... [A] traveler who carries a toothbrush and a few articles of

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> clothing in a paper bag or knotted scarf [may] claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.
>
> "As Justice Stewart stated in *Robbins,* the Fourth Amendment provides protection to the owner of *every container that conceals its contents from plain view.*" *Id.,* at 822–823, 102 S.Ct., at 2171–2172 (emphasis added; footnote and citation omitted).

See also *Jacobsen, supra,* 466 U.S., at 129, 104 S.Ct., at 1664 (opinion of WHITE, J.).

Accordingly, we have found a reasonable expectation of privacy in the contents of a 200–pound "double-locked footlocker," *United States v. Chadwick,* 433 U.S. 1, 11, 97 S.Ct. 2476, 2483, 53 L.Ed.2d 538 (1977); a "comparatively small, unlocked suitcase," *Arkansas v. Sanders,* 442 U.S. 753, 762, n. 9, 99 S.Ct. 2586, 2592, n. 9, 61 L.Ed.2d 235 (1979); a "totebag," *Robbins,* 453 U.S., at 422, 101 S.Ct., at 2844; and "packages wrapped in green opaque plastic," *ibid.* See also *Ross, supra,* 456 U.S., at 801, 822–823, 102 S.Ct., at 2160, 2171–2172 (suggesting that a warrant would have been required to search a " 'lunch-type' brown paper bag" and a "zippered red leather pouch" had they not been found in an automobile); *Jacobsen, supra,* 466 U.S., at 111, 114–115, 104 S.Ct. at 1655, 1656–1657 (suggesting that a warrantless search of an "ordinary cardboard box wrapped in brown paper" would have violated the Fourth Amendment had a private party not already opened it).

Our precedent, therefore, leaves no room to doubt that had respondents been carrying their personal effects in opaque, sealed plastic bags—identical to the ones they placed on the curb—their privacy would have been protected from warrantless police intrusion. So far as Fourth Amendment protection is concerned, opaque plastic bags are every bit as ***49** worthy as "packages wrapped in green opaque plastic" and "double-locked footlocker[s]." Cf. *Robbins, supra,* 453 U.S., at 441, 101 S.Ct., at 2854 (REHNQUIST, J., dissenting) (objecting to Court's discovery of reasonable expectation of privacy in contents of "two plastic garbage bags").

II

Respondents deserve no less protection just because Greenwood used the bags to discard rather than to transport his personal effects. Their contents are not inherently any less private, and Greenwood's decision to discard them, at least in the manner in which he did, does not diminish his expectation of privacy. [2]

***50** ****1634** A trash bag, like any of the above-mentioned containers, "is a common repository for one's personal effects" and, even more than many of them, is "therefore ... inevitably associated with the expectation of privacy." *Sanders, supra,* 442 U.S., at 762, 99 S.Ct., at 2592 (citing *Chadwick, supra,* 433 U.S., at 13, 97 S.Ct., at 2484). "[A]lmost every human activity ultimately manifests itself in waste products...." *Smith v. State,* 510 P.2d 793, 798 (Alaska), cert. denied, 414 U.S. 1086, 94 S.Ct. 603, 38 L.Ed.2d 489 (1973). See *California v. Rooney,* 483 U.S. 307, 320–321, n. 3, 107 S.Ct. 2852, 2859, n. 3, 97 L.Ed.2d 258 (1987) (WHITE, J., dissenting) (renowned archaeologist Emil Haury once said, "[i]f you want to know what is really going on in a community, look at its garbage") (quoted by W. Rathje, Archaeological Ethnography ... Because Sometimes It Is Better to Give Than to Receive, in Explorations in Ethnoarchaeology 49, 54 (R. Gould ed. 1978)); Weberman, The Art of Garbage Analysis: You Are What You Throw Away, 76 Esquire 113 (1971) (analyzing trash of various celebrities and drawing conclusions about their private lives). A single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it. A search of trash, like a search of the bedroom, can relate intimate details about sexual practices, health, and personal hygiene. Like rifling through desk drawers or intercepting phone calls, rummaging through trash can divulge the target's financial and professional status, political affiliations and inclinations, private thoughts, personal relationships, and romantic interests. It cannot be doubted that a sealed trash bag harbors telling evidence of the "intimate activity associated with the 'sanctity of a man's home and the privacies of life,' " which the Fourth Amendment is designed ***51** to protect. *Oliver v. United States,* 466 U.S. 170, 180, 104 S.Ct. 1735, 1742, 80 L.Ed.2d 214 (1984) (quoting *Boyd v. United States,* 116 U.S. 616, 630, 6 S.Ct. 524, 532, 29 L.Ed. 746

(1886)). See also *United States v. Dunn,* 480 U.S. 294, 300, 107 S.Ct. 1134, 1139, 94 L.Ed.2d 326 (1987).

The Court properly rejects the State's attempt to distinguish trash searches from other searches on the theory that trash is abandoned and therefore not entitled to an expectation of privacy. As the author of the Court's opinion observed last Term, a defendant's "property interest [in trash] does not settle the matter for Fourth Amendment purposes, for the reach of the Fourth Amendment is not determined by **1635 state property law." *Rooney, supra,* 483 U.S., at 320, 107 S.Ct., at 2858 (WHITE, J., dissenting). In evaluating the reasonableness of Greenwood's expectation that his sealed trash bags would not be invaded, the Court has held that we must look to "understandings that are recognized and permitted by society."[3] Most of us, I believe, would be incensed to discover a meddler—whether a neighbor, a reporter, or a detective—scrutinizing our sealed trash containers to discover some detail of our personal lives. See *State v. Schultz,* 388 So.2d 1326, 1331 (Fla.App.1980) (Anstead, J., dissenting). That was, quite naturally, the reaction to the sole incident on which the Court bases its conclusion that "snoops" and the like defeat the expectation of privacy in trash. *Ante,* at 1628, and n. 4. When a tabloid reporter examined then-Secretary of State *52 Henry Kissinger's trash and published his findings, Kissinger was "really revolted" by the intrusion and his wife suffered "grave anguish." N.Y. Times, July 9, 1975, p. A1, col. 8. The public response roundly condemning the reporter demonstrates that society not only recognized those reactions as reasonable, but shared them as well. Commentators variously characterized his conduct as "a disgusting invasion of personal privacy," Flieger, Investigative Trash, U.S. News & World Report, July 28, 1975, p. 72 (editor's page); "indefensible ... as civilized behavior," Washington Post, July 10, 1975, p. A18, col. 1 (editorial); and contrary to "the way decent people behave in relation to each other," *ibid.*

Beyond a generalized expectation of privacy, many municipalities, whether for reasons of privacy, sanitation, or both, reinforce confidence in the integrity of sealed trash containers by "prohibit[ing] anyone, except authorized employees of the Town ..., to rummage into, pick up, collect, move or otherwise interfere with articles or materials placed on ... any public street for collection." *United States v. Dzialak,* 441 F.2d 212, 215 (CA2 1971) (paraphrasing ordinance for town of Cheektowaga, New York). See also *United States v. Vahalik,* 606 F.2d 99, 100 (CA5 1979) (*per curiam*); *Magda v. Benson,* 536 F.2d 111, 112 (CA6 1976) (*per curiam*); *People v. Rooney,* 175 Cal.App.3d 634, 645, 221 Cal.Rptr. 49, 56 (1985), cert. dism'd, 483 U.S. 307, 107 S.Ct. 2852, 97 L.Ed.2d 258 (1987); *People v. Krivda,* 5 Cal.3d 357, 366, 96 Cal.Rptr. 62, 68, 486 P.2d 1262, 1268 (1971), vacated and remanded, 409 U.S. 33, 93 S.Ct. 32, 34 L.Ed.2d 45 (1972); *State v. Brown,* 20 Ohio App.3d 36, 38, n. 3, 484 N.E.2d 215, 218, n. 3 (1984). In fact, the California Constitution, as interpreted by the State's highest court, guarantees a right of privacy in trash vis-à-vis government officials. See *Krivda, supra* (recognizing right); *In re Lance W.,* 37 Cal.3d 873, 886–887, 210 Cal.Rptr. 631, 639–640, 694 P.2d 744, 752–753 (1985) (later constitutional amendment abolished exclusionary remedy but left intact the substance of the right).

*53 That is not to deny that isolated intrusions into opaque, sealed trash containers occur. When, acting on their own, "animals, children, scavengers, snoops, [or] other members of the public," *ante,* at 1628 (footnotes omitted), *actually* rummage through a bag of trash and expose its contents to plain view, "police cannot reasonably be expected to avert their eyes from evidence of criminal activity that **1636 could have been observed by any member of the public," *ante,* at 1629. That much follows from cases like *Jacobsen,* 466 U.S., at 117, 120, n. 17, 104 S.Ct., at 1658, 1660, n. 7 (emphasis added), which held that police may constitutionally inspect a package whose "integrity" a private carrier has *already* "compromised," because "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not *already* been frustrated"; and *California v. Ciraolo,* 476 U.S. 207, 213–214, 106 S.Ct. 1809, 1813, 90 L.Ed.2d 210 (1986) (emphasis added), which held that the Fourth Amendment does not prohibit police from observing what "[a]ny member of the public flying in this airspace who glanced down *could* have seen."

Had Greenwood flaunted his intimate activity by strewing his trash all over the curb for all to see, or had some nongovernmental intruder invaded his privacy and done the same, I could accept the Court's conclusion that an expectation of privacy would have been unreasonable. Similarly, had police searching the city dump run across incriminating evidence that, despite commingling with the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

trash of others, still retained its identity as Greenwood's, we would have a different case. But all that Greenwood "exposed ... to the public," *ante,* at 1628, were the exteriors of several opaque, sealed containers. Until the bags were opened by police, they hid their contents from the public's view every bit as much as did Chadwick's double-locked footlocker and Robbins' green, plastic wrapping. Faithful application of the warrant requirement does not require police to "avert their eyes from evidence of criminal activity that could have been observed by any member of the public." Rather, it only requires them ***54** to adhere to norms of privacy that members of the public plainly acknowledge.

The mere *possibility* that unwelcome meddlers *might* open and rummage through the containers does not negate the expectation of privacy in their contents any more than the possibility of a burglary negates an expectation of privacy in the home; or the possibility of a private intrusion negates an expectation of privacy in an unopened package; or the possibility that an operator will listen in on a telephone conversation negates an expectation of privacy in the words spoken on the telephone. "What a person ... seeks to preserve as private, *even in an area accessible to the public,* may be constitutionally protected." *Katz,* 389 U.S., at 351–352, 88 S.Ct., at 511. We have therefore repeatedly rejected attempts to justify a State's invasion of privacy on the ground that the privacy is not absolute. See *Chapman v. United States,* 365 U.S. 610, 616–617, 81 S.Ct. 776, 779–780, 5 L.Ed.2d 828 (1961) (search of a house invaded tenant's Fourth Amendment rights even though landlord had authority to enter house for some purposes); *Stoner v. California,* 376 U.S. 483, 487–490, 84 S.Ct. 889, 891–893, 11 L.Ed.2d 856 (1964) (implicit consent to janitorial personnel to enter motel room does not amount to consent to police search of room); *O'Connor v. Oretega,* 480 U.S. 709, 717, 107 S.Ct. 1492, 1497, 94 L.Ed.2d 714 (1987) (a government employee has a reasonable expectation of privacy in his office, even though "it is the nature of government offices that others—such as fellow employees, supervisors, consensual visitors, and the general public—may have frequent access to an individual's office"). As Justice SCALIA aptly put it, the Fourth Amendment protects "privacy ... not solitude." *O'Connor, supra,* at 730, 107 S.Ct., at 1504 (opinion concurring in judgment).

Nor is it dispositive that "respondents placed their refuse at the curb for the express purpose of conveying it to a third party, ... who might himself have sorted through respondents' trash or permitted others, such as the police, to do so." *Ante,* at 1629. In the first place, Greenwood can hardly be faulted for leaving trash on his curb when a county ordinance ***55** commanded him to do so, Orange County Code § 4–3–45(a) (1986) (must "remov[e] from the ****1637** premises at least once each week" all "solid waste created, produced or accumulated in or about [his] dwelling house"), and prohibited him from disposing of it in any other way, see Orange County Code § 3–3–85 (1988) (burning trash is unlawful). Unlike in other circumstances where privacy is compromised, Greenwood could not "avoid exposing personal belongings ... by simply leaving them at home." *O'Connor, supra,* at 725, 107 S.Ct., at 1502. More importantly, even the voluntary relinquishment of possession or control over an effect does not necessarily amount to a relinquishment of a privacy expectation in it. Were it otherwise, a letter or package would lose all Fourth Amendment protection when placed in a mailbox or other depository with the "express purpose" of entrusting it to the postal officer or a private carrier; those bailees are just as likely as trash collectors (and certainly have greater incentive) to "sor[t] through" the personal effects entrusted to them, "or permi[t] others, such as police to do so." Yet, it has been clear for at least 110 years that the possibility of such an intrusion does not justify a warrantless search by police in the first instance. See *Ex parte Jackson,* 96 U.S. (6 Otto) 727, 24 L.Ed. 877 (1878); *United States v. Van Leeuwen,* 397 U.S. 249, 90 S.Ct. 1029, 25 L.Ed.2d 282 (1970); *United States v. Jacobsen, supra* (1984). [4]

III

In holding that the warrantless search of Greenwood's trash was consistent with the Fourth Amendment, the Court paints a grim picture of our society. It depicts a society in which local authorities may command their citizens to dispose of their personal effects in the manner least protective of the ***56** "sanctity of [the] home and the privacies of life," *Boyd v. United States,* 116 U.S., at 630, 6 S.Ct. at 532, and then monitor them arbitrarily and without judicial oversight—a society that is not prepared to recognize as reasonable an individual's expectation of privacy in the most private of personal effects sealed in an opaque container and disposed of in a manner designed to commingle it imminently and inextricably with the trash of others. *Ante,* at 1628. The American society with which I am familiar "chooses to

dwell in reasonable security and freedom from surveillance," *Johnson v. United States,* 333 U.S. 10, 14, 68 S.Ct. 367, 369, 92 L.Ed. 436 (1948), and is more dedicated to individual liberty and more sensitive to intrusions on the sanctity of the home than the Court is willing to acknowledge.

I dissent.

All Citations

486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30, 56 USLW 4409

Footnotes

* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Lumber Co.,* 200 U.S. 321, 337, 26 S.Ct. 282, 287, 50 L.Ed. 499.

1 The Court of Appeal also held that respondent Van Houten had standing to seek the suppression of evidence discovered during the April 4 search of Greenwood's home. 182 Cal.App.3d, at 735, 227 Cal.Rptr., at 542–543.

2 For example, *State v. Ronngren,* 361 N.W.2d 224 (N.D.1985), involved the search of a garbage bag that a dog, acting "at the behest of no one," *id.,* at 228, had dragged from the defendants' yard into the yard of a neighbor. The neighbor deposited the bag in his own trash can, which he later permitted the police to search. The North Dakota Supreme Court held that the search of the garbage bag did not violate the defendants' Fourth Amendment rights.

3 It is not only the homeless of the Nation's cities who make use of others' refuse. For example, a nationally syndicated consumer columnist has suggested that apartment dwellers obtain cents-off coupons by "mak[ing] friends with the fellow who handles the trash" in their buildings, and has recounted the tale of "the 'Rich lady' from Westmont who once a week puts on rubber gloves and hip boots and wades into the town garbage dump looking for labels and other proofs of purchase" needed to obtain manufacturers' refunds. M. Sloane, "The Supermarket Shopper's" 1980 Guide to Coupons and Refunds 74, 161 (1980).

4 Even the refuse of prominent Americans has not been invulnerable. In 1975, for example, a reporter for a weekly tabloid seized five bags of garbage from the sidewalk outside the home of Secretary of State Henry Kissinger. Washington Post, July 9, 1975, p. A1, col. 8. A newspaper editorial criticizing this journalistic "trash-picking" observed that "[e]vidently ... 'everybody does it.' " Washington Post, July 10, 1975, p. A18, col. 1. We of course do not, as the dissent implies, "bas[e] [our] conclusion" that individuals have no reasonable expectation of privacy in their garbage on this "sole incident." *Post,* at 1634.

5 Given that the dissenters are among the tiny minority of judges whose views are contrary to ours, we are distinctly unimpressed with the dissent's prediction that "society will be shocked to learn" of today's decision. *Post,* at 1632.

1 See 453 U.S., at 436, 101 S.Ct., at 2851 (BLACKMUN, J., dissenting); *id.,* at 437, 101 S.Ct., at 2851 (REHNQUIST, J., dissenting); *id.,* at 444, 101 S.Ct., at 2855 (STEVENS, J., dissenting). But see *id.,* at 433–434, 101 S.Ct., at 2849–2850 (Powell, J., concurring in judgment) (rejecting position that all containers, even "the most trivial," like "a cigarbox or a Dixie cup," are entitled to the same Fourth Amendment protection).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Cf. *New York v. Belton,* 453 U.S. 454, 460–461, n. 4, 101 S.Ct. 2860, 2864, n. 4, 69 L.Ed.2d 768 (1981) (defining "container," for purposes of search incident to a lawful custodial arrest, as "any object capable of holding another object," including "luggage, boxes, bags, clothing, and the like").

In addition to finding that Robbins had a reasonable expectation of privacy in his duffelbag and plastic-wrapped packages, the Court also held that the automobile exception to the warrant requirement, see *Carroll v. United States,* 267 U.S. 132, 153, 45 S.Ct. 280, 285, 69 L.Ed. 543 (1925), did not apply to packages found in an automobile. The Court overruled the latter determination in *United States v. Ross,* 456 U.S. 798, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982), but reaffirmed that where, as here, the automobile exception is inapplicable, police may not conduct a warrantless search of any container that conceals its contents.

2 Both to support its position that society recognizes no reasonable privacy interest in sealed, opaque trash bags and to refute the prediction that "society will be shocked to learn" of that conclusion, *supra,* at 1632, the Court relies heavily upon a collection of lower court cases finding no Fourth Amendment bar to trash searches. But the authority that leads the Court to be "distinctly unimpressed" with our position, *ante,* at 1630, n. 5, is itself impressively undistinguished. Of 11 Federal Court of Appeals cases cited by the Court, at least 2 are factually or legally distinguishable, see *United States v. O'Bryant,* 775 F.2d 1528, 1533–1534 (CA11 1985) (police may search an apparently valuable briefcase "discarded next to an overflowing trash bin on a busy city street"); *United States v. Thornton,* 241 U.S.App.D.C. 46, 56, 746 F.2d 39, 49 (1984) (reasonable federal agents could believe in good faith that a trash search is legal), and 7 rely entirely or almost entirely on an abandonment theory that, as noted *infra,* at 1629, the Court has discredited, see *United States v. Dela Espriella,* 781 F.2d 1432, 1437 (CA9 1986) ("The question, then, becomes whether placing garbage for collection constitutes abandonment of property"); *United States v. Terry,* 702 F.2d 299, 308–309 (CA2) ("[T]he circumstances in this case clearly evidence abandonment by Williams of his trash"), cert. denied *sub nom. Williams v. United States,* 461 U.S. 931, 103 S.Ct. 2095, 77 L.Ed.2d 304 (1983); *United States v. Reicherter,* 647 F.2d 397, 399 (CA3 1981) ("[T]he placing of trash in garbage cans at a time and place for anticipated collection by public employees for hauling to a public dump signifies abandonment"); *United States v. Vahalik,* 606 F.2d 99, 100–101 (CA5 1979) (*per curiam*) ("[T]he act of placing garbage for collection is an act of abandonment which terminates any fourth amendment protection"), cert. denied, 444 U.S. 1081, 100 S.Ct. 1034, 62 L.Ed.2d 765 (1980); *United States v. Crowell,* 586 F.2d 1020, 1025 (CA4 1978) ("The act of placing [garbage] for collection is an act of abandonment and what happens to it thereafter is not within the protection of the fourth amendment"), cert. denied, 440 U.S. 959, 99 S.Ct. 1500, 59 L.Ed.2d 772 (1979); *Magda v. Benson,* 536 F.2d 111, 112 (CA6 1976) (*per curiam*) ("[F]ederal case law ... holds that garbage ... is abandoned and no longer protected by the Fourth Amendment"); *United States v. Mustone,* 469 F.2d 970, 972 (CA1 1972) (when defendant "deposited the bags on the sidewalk he abandoned them"). A reading of the Court's collection of state-court cases reveals an equally unimpressive pattern.

3 *Rakas v. Illinois,* 439 U.S. 128, 143–144, n. 12, 99 S.Ct. 421, 430–431, n. 12, 58 L.Ed.2d 387 (1978). See *ante,* at 1631 ("[T]he Fourth Amendment analysis must turn on such factors as 'our *societal* understanding that certain areas deserve the most scrupulous protection from government invasion' ") (quoting *Oliver v. United States,* 466 U.S. 170, 178, 104 S.Ct. 1735, 1741, 80 L.Ed.2d 214 (1984)); *Robbins v. California,* 453 U.S. 420, 428, 101 S.Ct. 2841, 2846, 69 L.Ed.2d 744 (1981) (plurality opinion) ("Expectations of privacy are established by general social norms"); *Dow Chemical Co. v. United States,*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

476 U.S. 227, 248, 106 S.Ct. 1819, 1832, 90 L.Ed.2d 226 (1986) (opinion of Powell, J.); Bush & Bly, Expectation of Privacy Analysis and Warrantless Trash Reconnaissance after *Katz v. United States,* 23 Ariz.L.Rev. 283, 293 (1981) ("[S]ocial custom ... serves as the most basic foundation of a great many legitimate privacy expectations") (citation omitted).

4 To be sure, statutes criminalizing interference with the mails might reinforce the expectation of privacy in mail, see, *e.g.,* 18 U.S.C. §§ 1701–1705, 1708, but the expectation of privacy in no way depends on statutory protection. In fact, none of the cases cited in the text even mention such statutes in finding Fourth Amendment protection in materials handed over to public or private carriers for delivery.

End of Document © 2022 Thomson Reuters. No claim to original U.S. Government Works.

KeyCite Yellow Flag - Negative Treatment
Declined to Extend by United States Department of Justice v. Ricco Jonas, 1st Cir.(N.H.), January 27, 2022

138 S.Ct. 2206
Supreme Court of the United States

Timothy Ivory CARPENTER, Petitioner
v.
United States.

No. 16–402.
|
Argued Nov. 29, 2017.
|
Decided June 22, 2018.

Synopsis

Background: In prosecution for multiple counts of robbery and carrying a firearm during federal crime of violence, the United States District Court for the Eastern District of Michigan, Sean F. Cox, J., 2013 WL 6385838, denied defendant's motion to suppress cell-site location information (CSLI), and denied defendant's posttrial motion for acquittal, 2013 WL 6729900, and the District Court, Sean F. Cox, J., 2014 WL 943094, denied defendant's motion for new trial. Defendant appealed. The United States Court of Appeals for the Sixth Circuit, Kethledge, Circuit Judge, 819 F.3d 880, affirmed. Certiorari was granted.

Holdings: The Supreme Court, Chief Justice Roberts, held that:

[1] an individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his physical movements as captured through CSLI;

[2] seven days of historical CSLI obtained from defendant's wireless carrier, pursuant to an order issued under the Stored Communications Act (SCA), was the product of a "search";

[3] Government's access to 127 days of historical CSLI invaded defendant's reasonable expectation of privacy; and

[4] Government must generally obtain a search warrant supported by probable cause before acquiring CSLI from a wireless carrier.

Reversed and remanded.

Justice Kennedy filed a dissenting opinion, in which Justices Thomas and Alito joined.

Justice Thomas filed a dissenting opinion.

Justice Alito filed a dissenting opinion, in which Justice Thomas joined.

Justice Gorsuch filed a dissenting opinion.

Procedural Posture(s): Appellate Review; Pre-Trial Hearing Motion; Post-Trial Hearing Motion.

West Headnotes (20)

[1] **Searches and Seizures** Fourth Amendment and reasonableness in general

The basic purpose of the Fourth Amendment is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials. U.S.C.A. Const.Amend. 4.

106 Cases that cite this headnote

[2] **Searches and Seizures** Persons, Places and Things Protected

Property rights are not the sole measure of Fourth Amendment violations; the Fourth Amendment protects people, not places. U.S.C.A. Const.Amend. 4.

90 Cases that cite this headnote

[3] **Searches and Seizures** What Constitutes Search or Seizure

Searches and Seizures Expectation of privacy

When an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

as reasonable, official intrusion into that private sphere generally qualifies as a search under the Fourth Amendment, and requires a warrant supported by probable cause. U.S.C.A. Const.Amend. 4.

114 Cases that cite this headnote

[4] **Searches and Seizures** Expectation of privacy

Although no single rubric definitively resolves which expectations of privacy are entitled to protection under the Fourth Amendment, the analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted. U.S.C.A. Const.Amend. 4.

37 Cases that cite this headnote

[5] **Searches and Seizures** Expectation of privacy

While property rights are often informative in resolving which expectations of privacy are entitled to protection under the Fourth Amendment, such an interest is not fundamental or dispositive in determining which expectations of privacy are legitimate. U.S.C.A. Const.Amend. 4.

49 Cases that cite this headnote

[6] **Searches and Seizures** Fourth Amendment and reasonableness in general

The Fourth Amendment seeks to secure the privacies of life against arbitrary power. U.S.C.A. Const.Amend. 4.

25 Cases that cite this headnote

[7] **Searches and Seizures** Fourth Amendment and reasonableness in general

A central aim of the Framers in adopting the Fourth Amendment was to place obstacles in the way of a too permeating police surveillance. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

[8] **Searches and Seizures** Use of electronic devices; tracking devices or "beepers."

In light of the immense storage capacity of modern cell phones, police officers must generally obtain a warrant before searching the contents of a phone. U.S.C.A. Const.Amend. 4.

29 Cases that cite this headnote

[9] **Searches and Seizures** Abandoned, surrendered, or disclaimed items

Under the third-party doctrine, a person has no legitimate expectation of privacy, for Fourth Amendment purposes, in information he voluntarily turns over to third parties, and that remains true even if the information is revealed on the assumption that it will be used only for a limited purpose; as a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections. U.S.C.A. Const.Amend. 4.

95 Cases that cite this headnote

[10] **Searches and Seizures** Expectation of privacy

Telecommunications Carrier's cooperation; pen registers and tracing

An individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his physical movements as captured through cell-site location information (CSLI). U.S.C.A. Const.Amend. 4.

312 Cases that cite this headnote

[11] **Searches and Seizures** Use of electronic devices; tracking devices or "beepers."

Seven days of historical cell-site location information (CSLI) obtained from suspect's wireless carrier, pursuant to an order issued by a federal magistrate judge under the Stored Communications Act (SCA), was the product of a "search" under the Fourth Amendment.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

179 Cases that cite this headnote

[12] **Searches and Seizures** Persons, Places and Things Protected

A person does not surrender all Fourth Amendment protection by venturing into the public sphere, and to the contrary, what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. U.S.C.A. Const.Amend. 4.

43 Cases that cite this headnote

[13] **Searches and Seizures** Expectation of privacy

Telecommunications Carrier's cooperation; pen registers and tracing

Government's access to 127 days of historical cell-site location information (CSLI) obtained from suspect's wireless carrier, pursuant to an order issued by a federal magistrate judge under the Stored Communications Act (SCA), invaded suspect's reasonable expectation of privacy, under the Fourth Amendment, in the whole world of his physical movements. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

187 Cases that cite this headnote

[14] **Searches and Seizures** Abandoned, surrendered, or disclaimed items

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another, but the fact of diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. U.S.C.A. Const.Amend. 4.

29 Cases that cite this headnote

[15] **Telecommunications** Carrier's cooperation; pen registers and tracing

The Government must generally obtain a search warrant supported by probable cause before acquiring cell-site location information (CSLI) from a wireless carrier. U.S.C.A. Const.Amend. 4.

405 Cases that cite this headnote

[16] **Searches and Seizures** Necessity of and preference for warrant, and exceptions in general

Although the ultimate measure of the constitutionality of a governmental search, under the Fourth Amendment, is reasonableness, warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, and thus, in the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. U.S.C.A. Const.Amend. 4.

41 Cases that cite this headnote

[17] **Telecommunications** Carrier's cooperation; pen registers and tracing

An order issued by a federal magistrate judge under the Stored Communications Act (SCA) is not a permissible mechanism for the Government to access cell-site location information (CSLI), and before compelling a wireless carrier to turn over a subscriber's CSLI, the Fourth Amendment requires the Government to get a search warrant. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

118 Cases that cite this headnote

[18] **Searches and Seizures** Emergencies and Exigent Circumstances; Opportunity to Obtain Warrant

One well-recognized exception to the search warrant requirement applies when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment. U.S.C.A. Const.Amend. 4.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

30 Cases that cite this headnote

[19] **Searches and Seizures** Emergencies and Exigent Circumstances; Opportunity to Obtain Warrant

Exigencies that support an exception to the Fourth Amendment's search warrant requirement include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence. U.S.C.A. Const.Amend. 4.

34 Cases that cite this headnote

[20] **Searches and Seizures** Expectation of privacy

The Supreme Court is obligated, as subtler and more far-reaching means of invading privacy have become available to the Government, to ensure that the progress of science does not erode Fourth Amendment protections. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

***2208** *Syllabus* *

Cell phones perform their wide and growing variety of functions by continuously connecting to a set of radio antennas called "cell sites." Each time a phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information for their own business purposes. Here, after the FBI identified the cell phone numbers of several robbery suspects, prosecutors were ***2209** granted court orders to obtain the suspects' cell phone records under the Stored Communications Act. Wireless carriers produced CSLI for petitioner Timothy Carpenter's phone, and the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days—an average of 101 data points per day. Carpenter moved to suppress the data, arguing that the Government's seizure of the records without obtaining a warrant supported by probable cause violated the Fourth Amendment. The District Court denied the motion, and prosecutors used the records at trial to show that Carpenter's phone was near four of the robbery locations at the time those robberies occurred. Carpenter was convicted. The Sixth Circuit affirmed, holding that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers.

Held :

1. The Government's acquisition of Carpenter's cell-site records was a Fourth Amendment search. Pp. 2212 - 2221.

(a) The Fourth Amendment protects not only property interests but certain expectations of privacy as well. *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576. Thus, when an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," official intrusion into that sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith v. Maryland,* 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (internal quotation marks and alterations omitted). The analysis regarding which expectations of privacy are entitled to protection is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Carroll v. United States,* 267 U.S. 132, 149, 45 S.Ct. 280, 69 L.Ed. 543. These Founding-era understandings continue to inform this Court when applying the Fourth Amendment to innovations in surveillance tools. See, *e.g.,* *Kyllo v. United States,* 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94. Pp. 2212 - 2215.

(b) The digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents but lies at the intersection of two lines of cases. One set addresses a person's expectation of privacy in his physical location and movements. See, *e.g.,* *United States v. Jones,* 565 U.S. 400, 132 S.Ct. 945, 181 L.Ed.2d 911 (five Justices concluding that privacy concerns would be raised by GPS tracking). The other addresses a person's expectation of privacy in information voluntarily turned over to third parties. See *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (no expectation of privacy in financial records held by a bank), and *Smith,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (no expectation of privacy in records of

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

dialed telephone numbers conveyed to telephone company). Pp. 2214 - 2216.

(c) Tracking a person's past movements through CSLI partakes of many of the qualities of GPS monitoring considered in *Jones*—it is detailed, encyclopedic, and effortlessly compiled. At the same time, however, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller.* Given the unique nature of cell-site records, this Court declines to extend *Smith* and *Miller* to cover them. Pp. 2216 - 2221.

(1) A majority of the Court has already recognized that individuals have a ***2210** reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which "hold for many Americans the 'privacies of life,' " *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2494–2495, 189 L.Ed.2d 430—contravenes that expectation. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones* : They give the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers. The Government contends that CSLI data is less precise than GPS information, but it thought the data accurate enough here to highlight it during closing argument in Carpenter's trial. At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in development," *Kyllo,* 533 U.S., at 36, 121 S.Ct. 2038, and the accuracy of CSLI is rapidly approaching GPS-level precision. Pp. 2217 - 2219.

(2) The Government contends that the third-party doctrine governs this case, because cell-site records, like the records in *Smith* and *Miller,* are "business records," created and maintained by wireless carriers. But there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers.

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. *Smith* and *Miller,* however, did not rely solely on the act of sharing. They also considered "the nature of the particular documents sought" and limitations on any "legitimate 'expectation of privacy' concerning their contents." *Miller,* 425 U.S., at 442, 96 S.Ct. 1619. In mechanically applying the third-party doctrine to this case the Government fails to appreciate the lack of comparable limitations on the revealing nature of CSLI.

Nor does the second rationale for the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as the term is normally understood. First, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley,* 573 U.S., at ——, 134 S.Ct., at 2484. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up. Pp. 2219 - 2220.

(d) This decision is narrow. It does not express a view on matters not before the Court; does not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras; does not address other business records that might incidentally reveal location information; and does not consider other collection techniques involving foreign affairs or national security. Pp. 2220 - 2221.

2. The Government did not obtain a warrant supported by probable cause before acquiring Carpenter's cell-site records. It acquired those records pursuant to a court order under the Stored Communications Act, which required the Government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). That showing falls well short of the probable cause required for a warrant. Consequently, an order issued under § 2703(d) is not a permissible mechanism for accessing historical cell-site ***2211** records. Not all orders compelling the production of documents will require a showing of probable cause. A warrant is required only in the rare case where the suspect has a legitimate privacy interest in records held by a third party. And even though the Government will generally need a warrant to access CSLI, case-specific exceptions—*e.g.,* exigent circumstances—may support a warrantless search. Pp. 2220 - 2223.

819 F.3d 880, reversed and remanded.

ROBERTS, C.J., delivered the opinion of the Court, in which GINSBURG, BREYER, SOTOMAYOR, and KAGAN, JJ.,

joined. KENNEDY, J., filed a dissenting opinion, in which THOMAS and ALITO, JJ., joined. THOMAS, J., filed a dissenting opinion. ALITO, J., filed a dissenting opinion, in which THOMAS, J., joined. GORSUCH, J., filed a dissenting opinion.

Attorneys and Law Firms

Nathan Freed Wessler, Ben Wizner, Brett Max Kaufman, American Civil Liberties, Union Foundation, New York, NY, David D. Cole, American Civil Liberties, Union Foundation, Washington, DC, Cecillia D. Wang, Jennifer Stisa Granick, American Civil Liberties, Union Foundation, San Francisco, CA, Harold Gurewitz, Gurewitz & Raben, PLC, Detroit, MI, Daniel S. Korobkin, Michael J. Steinberg, Kary L. Moss, American Civil Liberties, Union Fund of Michigan, Detroit, MI, Jeffrey L. Fisher, Stanford Law School, Supreme Court Litigation Clinic, Stanford, CA, for Petitioner.

Noel J. Francisco, Solicitor General, Kenneth A. Blanco, Acting Assistant Attorney General, Michael R. Dreeben, Deputy Solicitor General, Elizabeth B. Prelogar, Assistant to the Solicitor General, Jenny C. Ellickson, Attorney, Department of Justice, Washington, DC, for Respondent.

Opinion

Chief Justice ROBERTS delivered the opinion of the Court.

This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.

I

A

There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people. Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called "cell sites." Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, ***2212** wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

B

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and (ironically enough) T–Mobile stores in Detroit. One of the men confessed that, over the previous four months, the group (along with a rotating cast of getaway drivers and lookouts) had robbed nine different stores in Michigan and Ohio. The suspect identified 15 accomplices who had participated in the heists and gave the FBI some of their cell phone numbers; the FBI then reviewed his call records to identify additional numbers that he had called around the time of the robberies.

Based on that information, the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects. That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it "offers specific and

articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Federal Magistrate Judges issued two orders directing Carpenter's wireless carriers—MetroPCS and Sprint—to disclose "cell/site sector [information] for [Carpenter's] telephone[ ] at call origination and at call termination for incoming and outgoing calls" during the four-month period when the string of robberies occurred. App. to Pet. for Cert. 60a, 72a. The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was "roaming" in northeastern Ohio. Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.

Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence. See 18 U.S.C. §§ 924(c), 1951(a). Prior to trial, Carpenter moved to suppress the cell-site data provided by the wireless carriers. He argued that the Government's seizure of the records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause. The District Court denied the motion. App. to Pet. for Cert. 38a–39a.

At trial, seven of Carpenter's confederates pegged him as the leader of the operation. In addition, FBI agent Christopher Hess offered expert testimony about the cell-site data. Hess explained that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used. With this information, ***2213** Hess produced maps that placed Carpenter's phone near four of the charged robberies. In the Government's view, the location records clinched the case: They confirmed that Carpenter was "right where the ... robbery was at the exact time of the robbery." App. 131 (closing argument). Carpenter was convicted on all but one of the firearm counts and sentenced to more than 100 years in prison.

The Court of Appeals for the Sixth Circuit affirmed. 819 F.3d 880 (2016). The court held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers. Given that cell phone users voluntarily convey cell-site data to their carriers as "a means of establishing communication," the court concluded that the resulting business records are not entitled to Fourth Amendment protection. *Id.,* at 888 (quoting *Smith v. Maryland,* 442 U.S. 735, 741, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)).

We granted certiorari. 582 U.S. ——, 137 S.Ct. 2211, 198 L.Ed.2d 657 (2017).

II

A

[1] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The "basic purpose of this Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Court of City and County of San Francisco,* 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967). The Founding generation crafted the Fourth Amendment as a "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2494, 189 L.Ed.2d 430 (2014). In fact, as John Adams recalled, the patriot James Otis's 1761 speech condemning writs of assistance was "the first act of opposition to the arbitrary claims of Great Britain" and helped spark the Revolution itself. *Id.,* at —— – ——, 134 S.Ct., at 2494 (quoting 10 Works of John Adams 248 (C. Adams ed. 1856)).

[2] **[3]** For much of our history, Fourth Amendment search doctrine was "tied to common-law trespass" and focused on whether the Government "obtains information by physically intruding on a constitutionally protected area." *United States v. Jones,* 565 U.S. 400, 405, 406, n. 3, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). More recently, the Court has recognized that "property rights are not the sole measure of Fourth Amendment violations." *Soldal v. Cook County,* 506 U.S. 56, 64, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992). In *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), we established that "the Fourth

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Amendment protects people, not places," and expanded our conception of the Amendment to protect certain expectations of privacy as well. When an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith,* 442 U.S., at 740, 99 S.Ct. 2577 (internal quotation marks and alterations omitted).

[4] **[5]** **[6]** **[7]** Although no single rubric definitively resolves which expectations of privacy ***2214** are entitled to protection,[1] the analysis is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Carroll v. United States,* 267 U.S. 132, 149, 45 S.Ct. 280, 69 L.Ed. 543 (1925). On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure "the privacies of life" against "arbitrary power." *Boyd v. United States,* 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886). Second, and relatedly, that a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re,* 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948).

We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to "assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States,* 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). For that reason, we rejected in *Kyllo* a "mechanical interpretation" of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search. *Id.,* at 35, 121 S.Ct. 2038. Because any other conclusion would leave homeowners "at the mercy of advancing technology," we determined that the Government—absent a warrant—could not capitalize on such new sense-enhancing technology to explore what was happening within the home. *Ibid.*

[8] Likewise in *Riley,* the Court recognized the "immense storage capacity" of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone. 573 U.S., at ——, 134 S.Ct., at 2489. We explained that while the general rule allowing warrantless searches incident to arrest "strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to" the vast store of sensitive information on a cell phone. *Id.,* at ——, 134 S.Ct., at 2484.

B

The case before us involves the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls. This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform ***2215** our understanding of the privacy interests at stake.

The first set of cases addresses a person's expectation of privacy in his physical location and movements. In *United States v. Knotts,* 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), we considered the Government's use of a "beeper" to aid in tracking a vehicle through traffic. Police officers in that case planted a beeper in a container of chloroform before it was purchased by one of Knotts's co-conspirators. The officers (with intermittent aerial assistance) then followed the automobile carrying the container from Minneapolis to Knotts's cabin in Wisconsin, relying on the beeper's signal to help keep the vehicle in view. The Court concluded that the "augment[ed]" visual surveillance did not constitute a search because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.,* at 281, 282, 103 S.Ct. 1081. Since the movements of the vehicle and its final destination had been "voluntarily conveyed to anyone who wanted to look," Knotts could not assert a privacy interest in the information obtained. *Id.,* at 281, 103 S.Ct. 1081.

This Court in *Knotts,* however, was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance. The Court emphasized the "limited use which the government made of the signals from this particular beeper" during a discrete "automotive journey." *Id.,* at 284, 285, 103 S.Ct. 1081.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Significantly, the Court reserved the question whether "different constitutional principles may be applicable" if "twenty-four hour surveillance of any citizen of this country [were] possible." *Id.,* at 283–284, 103 S.Ct. 1081.

Three decades later, the Court considered more sophisticated surveillance of the sort envisioned in *Knotts* and found that different principles did indeed apply. In *United States v. Jones,* FBI agents installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for 28 days. The Court decided the case based on the Government's physical trespass of the vehicle. 565 U.S., at 404–405, 132 S.Ct. 945. At the same time, five Justices agreed that related privacy concerns would be raised by, for example, "surreptitiously activating a stolen vehicle detection system" in Jones's car to track Jones himself, or conducting GPS tracking of his cell phone. *Id.,* at 426, 428, 132 S.Ct. 945 (ALITO, J., concurring in judgment); *id.,* at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring). Since GPS monitoring of a vehicle tracks "every movement" a person makes in that vehicle, the concurring Justices concluded that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"—regardless whether those movements were disclosed to the public at large. *Id.,* at 430, 132 S.Ct. 945 (opinion of Alito, J.); *id.,* at 415, 132 S.Ct. 945 (opinion of Sotomayor, J.). [2]

***2216** **[9]** In a second set of decisions, the Court has drawn a line between what a person keeps to himself and what he shares with others. We have previously held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith,* 442 U.S., at 743–744, 99 S.Ct. 2577. That remains true "even if the information is revealed on the assumption that it will be used only for a limited purpose." *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections.

This third-party doctrine largely traces its roots to *Miller*. While investigating Miller for tax evasion, the Government subpoenaed his banks, seeking several months of canceled checks, deposit slips, and monthly statements. The Court rejected a Fourth Amendment challenge to the records collection. For one, Miller could "assert neither ownership nor possession" of the documents; they were "business records of the banks." *Id.,* at 440, 96 S.Ct. 1619. For another, the nature of those records confirmed Miller's limited expectation of privacy, because the checks were "not confidential communications but negotiable instruments to be used in commercial transactions," and the bank statements contained information "exposed to [bank] employees in the ordinary course of business." *Id.,* at 442, 96 S.Ct. 1619. The Court thus concluded that Miller had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government." *Id.,* at 443, 96 S.Ct. 1619.

Three years later, *Smith* applied the same principles in the context of information conveyed to a telephone company. The Court ruled that the Government's use of a pen register—a device that recorded the outgoing phone numbers dialed on a landline telephone—was not a search. Noting the pen register's "limited capabilities," the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial." 442 U.S., at 742, 99 S.Ct. 2577. Telephone subscribers know, after all, that the numbers are used by the telephone company "for a variety of legitimate business purposes," including routing calls. *Id.,* at 743, 99 S.Ct. 2577. And at any rate, the Court explained, such an expectation "is not one that society is prepared to recognize as reasonable." *Ibid.* (internal quotation marks omitted). When Smith placed a call, he "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business." *Id.,* at 744, 99 S.Ct. 2577 (internal quotation marks omitted). Once again, we held that the defendant "assumed the risk" that the company's records "would be divulged to police." *Id.,* at 745, 99 S.Ct. 2577.

III

The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site ***2217** records. After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.

[10] **[11]** We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search. [3]

A

[12] A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz,* 389 U.S., at 351–352, 88 S.Ct. 507. A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. *Jones,* 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring in judgment); *id.,* at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring). Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." *Id.,* at 429, 132 S.Ct. 945 (opinion of Alito, J.). For that reason, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.,* at 430, 132 S.Ct. 945.

[13] Allowing government access to cell-site records contravenes that expectation. Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location. Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." *Id.,* at 415, 132 S.Ct. 945 (opinion of SOTOMAYOR, J.). These location records "hold for many Americans the 'privacies of life.' " *Riley,* 573 U.S., at ——, 134 S.Ct., at 2494–2495 (quoting *Boyd,* 116 U.S., at 630, 6 S.Ct. 524). And like GPS monitoring, cell phone ***2218** tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.

In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones,* a cell phone—almost a "feature of human anatomy," *Riley,* 573 U.S., at ——, 134 S.Ct., at 2484—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. See *id.,* at ——, 134 S.Ct., at 2490 (noting that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower"); contrast *Cardwell v. Lewis,* 417 U.S. 583, 590, 94 S.Ct. 2464, 41 L.Ed.2d 325 (1974) (plurality opinion) ("A car has little capacity for escaping public scrutiny."). Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones,* police need not even know in advance whether they want to follow a particular individual, or when.

Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.

The Government and Justice KENNEDY contend, however, that the collection of CSLI should be permitted because the data is less precise than GPS information. Not to worry, they maintain, because the location records did "not on their own suffice to place [Carpenter] at the crime scene"; they placed him within a wedge-shaped sector ranging from one-eighth to four square miles. Brief for United States 24; see *post,* at 2232 - 2233. Yet the Court has already rejected the proposition that "inference insulates a search." *Kyllo,* 533 U.S., at 36, 121 S.Ct. 2038. From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial. App. 131.

At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in development." ***2219** *Kyllo,* 533 U.S., at 36, 121 S.Ct. 2038. While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters. Brief for Electronic Frontier Foundation et al. as *Amici Curiae* 12 (describing triangulation methods that estimate a device's location inside a given cell sector).

Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.

B

The Government's primary contention to the contrary is that the third-party doctrine governs this case. In its view, cell-site records are fair game because they are "business records" created and maintained by the wireless carriers. The Government (along with Justice KENNEDY) recognizes that this case features new technology, but asserts that the legal question nonetheless turns on a garden-variety request for information from a third-party witness. Brief for United States 32–34; *post,* at 2229 - 2231.

The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.

[14] The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Riley,* 573 U.S., at ——, 134 S.Ct., at 2488. *Smith* and *Miller,* after all, did not rely solely on the act of sharing. Instead, they considered "the nature of the particular documents sought" to determine whether "there is a legitimate 'expectation of privacy' concerning their contents." *Miller,* 425 U.S., at 442, 96 S.Ct. 1619. *Smith* pointed out the limited capabilities of a pen register; as explained in *Riley,* telephone call logs reveal little in the way of "identifying information." *Smith,*

442 U.S., at 742, 99 S.Ct. 2577; *Riley,* 573 U.S., at ——, 134 S.Ct., at 2493. *Miller* likewise noted that checks were "not confidential communications but negotiable instruments to be used in commercial transactions." 425 U.S., at 442, 96 S.Ct. 1619. In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.

The Court has in fact already shown special solicitude for location information in the third-party context. In *Knotts,* the Court relied on *Smith* to hold that an individual has no reasonable expectation of privacy in public movements that he "voluntarily ***2220** conveyed to anyone who wanted to look." *Knotts,* 460 U.S., at 281, 103 S.Ct. 1081; see *id.,* at 283, 103 S.Ct. 1081 (discussing *Smith*). But when confronted with more pervasive tracking, five Justices agreed that longer term GPS monitoring of even a vehicle traveling on public streets constitutes a search. *Jones,* 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring in judgment); *id.,* at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring). Justice GORSUCH wonders why "someone's location when using a phone" is sensitive, *post,* at 2262, and Justice KENNEDY assumes that a person's discrete movements "are not particularly private," *post,* at 2232. Yet this case is not about "using a phone" or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*.

Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley,* 573 U.S., at ——, 134 S.Ct., at 2484. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[ ] the risk" of turning over a comprehensive dossier of his physical movements. *Smith,* 442 U.S., at 745, 99 S.Ct. 2577.

We therefore decline to extend *Smith* and *Miller* to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.

* * *

Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future." *Northwest Airlines, Inc. v. Minnesota,* 322 U.S. 292, 300, 64 S.Ct. 950, 88 L.Ed. 1283 (1944). [4]

***2221** IV

[15] **[16]** Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records. Although the "ultimate measure of the constitutionality of a governmental search is 'reasonableness,' " our cases establish that warrantless searches are typically unreasonable where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing." *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 652–653, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995). Thus, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the

warrant requirement." *Riley,* 573 U.S., at ——, 134 S.Ct., at 2482.

[17] The Government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). That showing falls well short of the probable cause required for a warrant. The Court usually requires "some quantum of individualized suspicion" before a search or seizure may take place. *United States v. Martinez–Fuerte,* 428 U.S. 543, 560–561, 96 S.Ct. 3074, 49 L.Ed.2d 1116 (1976). Under the standard in the Stored Communications Act, however, law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation —a "gigantic" departure from the probable cause rule, as the Government explained below. App. 34. Consequently, an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant.

Justice ALITO contends that the warrant requirement simply does not apply when the Government acquires records using compulsory process. Unlike an actual search, he says, subpoenas for documents do not involve the direct taking of evidence; they are at most a "constructive search" conducted by the target of the subpoena. *Post,* at 2252 - 2253. Given this lesser intrusion on personal privacy, Justice ALITO argues that the compulsory production of records is not held to the same probable cause standard. In his view, this Court's precedents set forth a categorical rule—separate and distinct from the third-party doctrine—subjecting subpoenas to lenient scrutiny without regard to the suspect's expectation of privacy in the records. *Post,* at 2250 - 2257.

But this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy. Almost all of the examples Justice ALITO cites, see *post,* at 2253 - 2255, contemplated requests for evidence implicating diminished privacy interests or for a corporation's own books.[5] The lone exception, of course, is ***2222** *Miller,* where the Court's analysis of the third-party subpoena merged with the application of the third-party doctrine. 425 U.S., at 444, 96 S.Ct. 1619 (concluding that Miller lacked the necessary privacy interest to contest the issuance of a subpoena to his bank).

Justice ALITO overlooks the critical issue. At some point, the dissent should recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers. When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents. See *Riley,* 573 U.S., at ——, 134 S.Ct., at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered [in prior precedents].").

If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement. Under Justice ALITO's view, private letters, digital contents of a cell phone—any personal information reduced to document form, in fact—may be collected by subpoena for no reason other than "official curiosity." *United States v. Morton Salt Co.,* 338 U.S. 632, 652, 70 S.Ct. 357, 94 L.Ed. 401 (1950). Justice KENNEDY declines to adopt the radical implications of this theory, leaving open the question whether the warrant requirement applies "when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party." *Post,* at 2230 (citing *United States v. Warshak,* 631 F.3d 266, 283–288 (C.A.6 2010)). That would be a sensible exception, because it would prevent the subpoena doctrine from overcoming any reasonable expectation of privacy. If the third-party doctrine does not apply to the "modern-day equivalents of an individual's own 'papers' or 'effects,' " then the clear implication is that the documents should receive full Fourth Amendment protection. We simply think that such protection should extend as well to a detailed log of a person's movements over several years.

This is certainly not to say that all orders compelling the production of documents will require a showing of probable cause. The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party.

[18] **[19]** Further, even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual's cell-site records under certain circumstances. "One well-recognized exception applies when ' "the exigencies of the situation" make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.' " *Kentucky v. King,* 563 U.S. 452, 460, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011) (quoting ***2223** *Mincey v. Arizona,* 437 U.S. 385, 394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978)). Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence. 563 U.S., at 460, and n. 3, 131 S.Ct. 1849.

As a result, if law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of CSLI. Lower courts, for instance, have approved warrantless searches related to bomb threats, active shootings, and child abductions. Our decision today does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency.

* * *

[20] As Justice Brandeis explained in his famous dissent, the Court is obligated—as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. *Olmstead v. United States,* 277 U.S. 438, 473–474, 48 S.Ct. 564, 72 L.Ed. 944 (1928). Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, "after consulting the lessons of history," drafted the Fourth Amendment to prevent. *Di Re,* 332 U.S., at 595, 68 S.Ct. 222.

We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.

The judgment of the Court of Appeals is reversed, and the case is remanded for further proceedings consistent with this opinion.

It is so ordered.

Justice KENNEDY, with whom Justice THOMAS and Justice ALITO join, dissenting.

This case involves new technology, but the Court's stark departure from relevant Fourth Amendment precedents and principles is, in my submission, unnecessary and incorrect, requiring this respectful dissent.

The new rule the Court seems to formulate puts needed, reasonable, accepted, lawful, and congressionally authorized criminal investigations at serious risk in serious cases, often when law enforcement seeks to prevent the threat of violent crimes. And it places undue restrictions on the lawful and necessary enforcement powers exercised not only by the Federal Government, but also by law enforcement in every State and locality throughout the Nation. Adherence to this Court's longstanding precedents and analytic framework would have been the proper and prudent way to resolve this case.

The Court has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party. *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976); *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). This is true even when the records contain personal and sensitive information. So when the Government uses a subpoena to obtain, for ***2224** example, bank records, telephone records, and credit card statements from the businesses that create and keep these records, the Government does not engage in a search of the business's customers within the meaning of the Fourth Amendment.

In this case petitioner challenges the Government's right to use compulsory process to obtain a now-common kind of business record: cell-site records held by cell phone service providers. The Government acquired the records through an

investigative process enacted by Congress. Upon approval by a neutral magistrate, and based on the Government's duty to show reasonable necessity, it authorizes the disclosure of records and information that are under the control and ownership of the cell phone service provider, not its customer. Petitioner acknowledges that the Government may obtain a wide variety of business records using compulsory process, and he does not ask the Court to revisit its precedents. Yet he argues that, under those same precedents, the Government searched his records when it used court-approved compulsory process to obtain the cell-site information at issue here.

Cell-site records, however, are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process. Customers like petitioner do not own, possess, control, or use the records, and for that reason have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process.

The Court today disagrees. It holds for the first time that by using compulsory process to obtain records of a business entity, the Government has not just engaged in an impermissible action, but has conducted a search of the business's customer. The Court further concludes that the search in this case was unreasonable and the Government needed to get a warrant to obtain more than six days of cell-site records.

In concluding that the Government engaged in a search, the Court unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases. In doing so it draws an unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other. According to today's majority opinion, the Government can acquire a record of every credit card purchase and phone call a person makes over months or years without upsetting a legitimate expectation of privacy. But, in the Court's view, the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime scene. That distinction is illogical and will frustrate principled application of the Fourth Amendment in many routine yet vital law enforcement operations.

It is true that the Cyber Age has vast potential both to expand and restrict individual freedoms in dimensions not contemplated in earlier times. See *Packingham v. North Carolina,* 582 U.S. ——, ——– ——, 137 S.Ct. 1730, 1735–1736, 198 L.Ed.2d 273 (2017). For the reasons that follow, however, there is simply no basis here for concluding that the Government interfered with information that the cell phone customer, either from a legal or commonsense standpoint, should have thought the law would deem owned or controlled by him.

I

Before evaluating the question presented it is helpful to understand the nature of cell-site records, how they are commonly ***2225** used by cell phone service providers, and their proper use by law enforcement.

When a cell phone user makes a call, sends a text message or e-mail, or gains access to the Internet, the cell phone establishes a radio connection to an antenna at a nearby cell site. The typical cell site covers a more-or-less circular geographic area around the site. It has three (or sometimes six) separate antennas pointing in different directions. Each provides cell service for a different 120–degree (or 60–degree) sector of the cell site's circular coverage area. So a cell phone activated on the north side of a cell site will connect to a different antenna than a cell phone on the south side.

Cell phone service providers create records each time a cell phone connects to an antenna at a cell site. For a phone call, for example, the provider records the date, time, and duration of the call; the phone numbers making and receiving the call; and, most relevant here, the cell site used to make the call, as well as the specific antenna that made the connection. The cell-site and antenna data points, together with the date and time of connection, are known as cell-site location information, or cell-site records. By linking an individual's cell phone to a particular 120– or 60–degree sector of a cell site's coverage area at a particular time, cell-site records reveal the general location of the cell phone user.

The location information revealed by cell-site records is imprecise, because an individual cell-site sector usually covers a large geographic area. The FBI agent who offered expert testimony about the cell-site records at issue here testified that a cell site in a city reaches between a half mile and two miles in all directions. That means a 60–degree sector covers between approximately one-eighth and two square miles (and a 120–degree sector twice that area). To put that in perspective, in urban areas cell-site records often would

reveal the location of a cell phone user within an area covering between around a dozen and several hundred city blocks. In rural areas cell-site records can be up to 40 times more imprecise. By contrast, a Global Positioning System (GPS) can reveal an individual's location within around 15 feet.

Major cell phone service providers keep cell-site records for long periods of time. There is no law requiring them to do so. Instead, providers contract with their customers to collect and keep these records because they are valuable to the providers. Among other things, providers aggregate the records and sell them to third parties along with other information gleaned from cell phone usage. This data can be used, for example, to help a department store determine which of various prospective store locations is likely to get more foot traffic from middle-aged women who live in affluent zip codes. The market for cell phone data is now estimated to be in the billions of dollars. See Brief for Technology Experts as *Amici Curiae* 23.

Cell-site records also can serve an important investigative function, as the facts of this case demonstrate. Petitioner, Timothy Carpenter, along with a rotating group of accomplices, robbed at least six RadioShack and T–Mobile stores at gunpoint over a 2–year period. Five of those robberies occurred in the Detroit area, each crime at least four miles from the last. The sixth took place in Warren, Ohio, over 200 miles from Detroit.

The Government, of course, did not know all of these details in 2011 when it began investigating Carpenter. In April of that year police arrested four of Carpenter's co-conspirators. One of them confessed to committing nine robberies in Michigan and Ohio between December 2010 and March 2011. He identified 15 accomplices who had participated in at ***2226** least one of those robberies; named Carpenter as one of the accomplices; and provided Carpenter's cell phone number to the authorities. The suspect also warned that the other members of the conspiracy planned to commit more armed robberies in the immediate future.

The Government at this point faced a daunting task. Even if it could identify and apprehend the suspects, still it had to link each suspect in this changing criminal gang to specific robberies in order to bring charges and convict. And, of course, it was urgent that the Government take all necessary steps to stop the ongoing and dangerous crime spree.

Cell-site records were uniquely suited to this task. The geographic dispersion of the robberies meant that, if Carpenter's cell phone were within even a dozen to several hundred city blocks of one or more of the stores when the different robberies occurred, there would be powerful circumstantial evidence of his participation; and this would be especially so if his cell phone usually was not located in the sectors near the stores except during the robbery times.

To obtain these records, the Government applied to federal magistrate judges for disclosure orders pursuant to § 2703(d) of the Stored Communications Act. That Act authorizes a magistrate judge to issue an order requiring disclosure of cell-site records if the Government demonstrates "specific and articulable facts showing that there are reasonable grounds to believe" the records "are relevant and material to an ongoing criminal investigation."18 U.S.C. §§ 2703(d),2711(3). The full statutory provision is set out in the Appendix, *infra*.

From Carpenter's primary service provider, MetroPCS, the Government obtained records from between December 2010 and April 2011, based on its understanding that nine robberies had occurred in that timeframe. The Government also requested seven days of cell-site records from Sprint, spanning the time around the robbery in Warren, Ohio. It obtained two days of records.

These records confirmed that Carpenter's cell phone was in the general vicinity of four of the nine robberies, including the one in Ohio, at the times those robberies occurred.

II

The first Clause of the Fourth Amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." The customary beginning point in any Fourth Amendment search case is whether the Government's actions constitute a "search" of the defendant's person, house, papers, or effects, within the meaning of the constitutional provision. If so, the next question is whether that search was reasonable.

Here the only question necessary to decide is whether the Government searched anything of Carpenter's when it used compulsory process to obtain cell-site records from Carpenter's cell phone service providers. This Court's decisions in *Miller* and *Smith* dictate that the answer is no,

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

as every Court of Appeals to have considered the question has recognized. See *United States v. Thompson,* 866 F.3d 1149 (C.A.10 2017); *United States v. Graham,* 824 F.3d 421 (C.A.4 2016) (en banc); *United States v. Carpenter,* 819 F.3d 880 (C.A.6 2016); *United States v. Davis,* 785 F.3d 498 (C.A.11 2015) (en banc); *In re Application of U.S. for Historical Cell Site Data,* 724 F.3d 600 (C.A.5 2013).

A

Miller and *Smith* hold that individuals lack any protected Fourth Amendment interests ***2227** in records that are possessed, owned, and controlled only by a third party. In *Miller* federal law enforcement officers obtained four months of the defendant's banking records. 425 U.S., at 437–438, 96 S.Ct. 1619. And in *Smith* state police obtained records of the phone numbers dialed from the defendant's home phone. 442 U.S., at 737, 99 S.Ct. 2577. The Court held in both cases that the officers did not search anything belonging to the defendants within the meaning of the Fourth Amendment. The defendants could "assert neither ownership nor possession" of the records because the records were created, owned, and controlled by the companies. *Miller, supra,* at 440, 96 S.Ct. 1619; see *Smith, supra,* at 741, 99 S.Ct. 2577. And the defendants had no reasonable expectation of privacy in information they "voluntarily conveyed to the [companies] and exposed to their employees in the ordinary course of business." *Miller, supra,* at 442, 96 S.Ct. 1619; see *Smith,* 442 U.S., at 744, 99 S.Ct. 2577. Rather, the defendants "assumed the risk that the information would be divulged to police." *Id.,* at 745, 99 S.Ct. 2577.

Miller and *Smith* have been criticized as being based on too narrow a view of reasonable expectations of privacy. See, *e.g.,* Ashdown, The Fourth Amendment and the "Legitimate Expectation of Privacy," 34 Vand. L. Rev. 1289, 1313–1316 (1981). Those criticisms, however, are unwarranted. The principle established in *Miller* and *Smith* is correct for two reasons, the first relating to a defendant's attenuated interest in property owned by another, and the second relating to the safeguards inherent in the use of compulsory process.

First, *Miller* and *Smith* placed necessary limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a "requisite connection." *Minnesota v. Carter,* 525 U.S. 83, 99, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (KENNEDY, J., concurring). Fourth Amendment rights, after all, are personal. The Amendment protects "[t]he right of the people to be secure in *their* ... persons, houses, papers, and effects"—not the persons, houses, papers, and effects of others. (Emphasis added.)

The concept of reasonable expectations of privacy, first announced in *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), sought to look beyond the "arcane distinctions developed in property and tort law" in evaluating whether a person has a sufficient connection to the thing or place searched to assert Fourth Amendment interests in it. *Rakas v. Illinois,* 439 U.S. 128, 143, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). Yet "property concepts" are, nonetheless, fundamental "in determining the presence or absence of the privacy interests protected by that Amendment." *Id.,* at 143–144, n. 12, 99 S.Ct. 421. This is so for at least two reasons. First, as a matter of settled expectations from the law of property, individuals often have greater expectations of privacy in things and places that belong to them, not to others. And second, the Fourth Amendment's protections must remain tethered to the text of that Amendment, which, again, protects only a person's own "persons, houses, papers, and effects."

Katz did not abandon reliance on property-based concepts. The Court in *Katz* analogized the phone booth used in that case to a friend's apartment, a taxicab, and a hotel room. 389 U.S., at 352, 359, 88 S.Ct. 507. So when the defendant "shu[t] the door behind him" and "pa[id] the toll," *id.,* at 352, 88 S.Ct. 507, he had a temporary interest in the space and a legitimate expectation that others would not intrude, much like the interest a hotel guest has in a hotel room, ***2228** *Stoner v. California,* 376 U.S. 483, 84 S.Ct. 889, 11 L.Ed.2d 856 (1964), or an overnight guest has in a host's home, *Minnesota v. Olson,* 495 U.S. 91, 110 S.Ct. 1684, 109 L.Ed.2d 85 (1990). The Government intruded on that space when it attached a listening device to the phone booth. *Katz,* 389 U.S., at 348, 88 S.Ct. 507. (And even so, the Court made it clear that the Government's search could have been reasonable had there been judicial approval on a case-

specific basis, which, of course, did occur here. *Id.*, at 357–359, 88 S.Ct. 507.)

Miller and *Smith* set forth an important and necessary limitation on the *Katz* framework. They rest upon the commonsense principle that the absence of property law analogues can be dispositive of privacy expectations. The defendants in those cases could expect that the third-party businesses could use the records the companies collected, stored, and classified as their own for any number of business and commercial purposes. The businesses were not bailees or custodians of the records, with a duty to hold the records for the defendants' use. The defendants could make no argument that the records were their own papers or effects. See *Miller, supra,* at 440, 96 S.Ct. 1619 ("the documents subpoenaed here are not respondent's 'private papers' "); *Smith, supra,* at 741, 99 S.Ct. 2577 ("petitioner obviously cannot claim that his 'property' was invaded"). The records were the business entities' records, plain and simple. The defendants had no reason to believe the records were owned or controlled by them and so could not assert a reasonable expectation of privacy in the records.

The second principle supporting *Miller* and *Smith* is the longstanding rule that the Government may use compulsory process to compel persons to disclose documents and other evidence within their possession and control. See *United States v. Nixon,* 418 U.S. 683, 709, 94 S.Ct. 3090, 41 L.Ed.2d 1039 (1974) (it is an "ancient proposition of law" that "the public has a right to every man's evidence" (internal quotation marks and alterations omitted)). A subpoena is different from a warrant in its force and intrusive power. While a warrant allows the Government to enter and seize and make the examination itself, a subpoena simply requires the person to whom it is directed to make the disclosure. A subpoena, moreover, provides the recipient the "opportunity to present objections" before complying, which further mitigates the intrusion. *Oklahoma Press Publishing Co. v. Walling,* 327 U.S. 186, 195, 66 S.Ct. 494, 90 L.Ed. 614 (1946).

For those reasons this Court has held that a subpoena for records, although a "constructive" search subject to Fourth Amendment constraints, need not comply with the procedures applicable to warrants—even when challenged by the person to whom the records belong. *Id.,* at 202, 208, 66 S.Ct. 494. Rather, a subpoena complies with the Fourth Amendment's reasonableness requirement so long as it is " 'sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.' " *Donovan v. Lone Steer, Inc.,* 464 U.S. 408, 415, 104 S.Ct. 769, 78 L.Ed.2d 567 (1984). Persons with no meaningful interests in the records sought by a subpoena, like the defendants in *Miller* and *Smith,* have no rights to object to the records' disclosure—much less to assert that the Government must obtain a warrant to compel disclosure of the records. See *Miller,* 425 U.S., at 444–446, 96 S.Ct. 1619; *SEC v. Jerry T. O'Brien, Inc.,* 467 U.S. 735, 742–743, 104 S.Ct. 2720, 81 L.Ed.2d 615 (1984).

Based on *Miller* and *Smith* and the principles underlying those cases, it is well established that subpoenas may be used to ***2229** obtain a wide variety of records held by businesses, even when the records contain private information. See 2 W. LaFave, Search and Seizure § 4.13 (5th ed. 2012). Credit cards are a prime example. State and federal law enforcement, for instance, often subpoena credit card statements to develop probable cause to prosecute crimes ranging from drug trafficking and distribution to healthcare fraud to tax evasion. See *United States v. Phibbs,* 999 F.2d 1053 (C.A.6 1993) (drug distribution); *McCune v. DOJ,* 592 Fed.Appx. 287 (C.A.5 2014) (healthcare fraud); *United States v. Green,* 305 F.3d 422 (C.A.6 2002) (drug trafficking and tax evasion); see also 12 U.S.C. §§ 3402(4), 3407 (allowing the Government to subpoena financial records if "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry"). Subpoenas also may be used to obtain vehicle registration records, hotel records, employment records, and records of utility usage, to name just a few other examples. See 1 LaFave, *supra,* § 2.7(c).

And law enforcement officers are not alone in their reliance on subpoenas to obtain business records for legitimate investigations. Subpoenas also are used for investigatory purposes by state and federal grand juries, see *United States v. Dionisio,* 410 U.S. 1, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973), state and federal administrative agencies, see *Oklahoma Press, supra,* and state and federal legislative bodies, see *McPhaul v. United States,* 364 U.S. 372, 81 S.Ct. 138, 5 L.Ed.2d 136 (1960).

B

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Carpenter does not question these traditional investigative practices. And he does not ask the Court to reconsider *Miller* and *Smith*. Carpenter argues only that, under *Miller* and *Smith,* the Government may not use compulsory process to acquire cell-site records from cell phone service providers.

There is no merit in this argument. Cell-site records, like all the examples just discussed, are created, kept, classified, owned, and controlled by cell phone service providers, which aggregate and sell this information to third parties. As in *Miller,* Carpenter can "assert neither ownership nor possession" of the records and has no control over them. 425 U.S., at 440, 96 S.Ct. 1619.

Carpenter argues that he has Fourth Amendment interests in the cell-site records because they are in essence his personal papers by operation of 47 U.S.C. § 222. That statute imposes certain restrictions on how providers may use "customer proprietary network information"—a term that encompasses cell-site records. §§ 222(c), (h)(1)(A). The statute in general prohibits providers from disclosing personally identifiable cell-site records to private third parties. § 222(c)(1). And it allows customers to request cell-site records from the provider. § 222(c)(2).

Carpenter's argument is unpersuasive, however, for § 222 does not grant cell phone customers any meaningful interest in cell-site records. The statute's confidentiality protections may be overridden by the interests of the providers or the Government. The providers may disclose the records "to protect the[ir] rights or property" or to "initiate, render, bill, and collect for telecommunications services." §§ 222(d)(1), (2). They also may disclose the records "as required by law"—which, of course, is how they were disclosed in this case. § 222(c)(1). Nor does the statute provide customers any practical control over the records. Customers do not create the records; they have no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed. Even ***2230** their right to request access to the records is limited, for the statute "does not preclude a carrier from being reimbursed by the customers ... for the costs associated with making such disclosures." H.R.Rep. No. 104–204, pt. 1, p. 90 (1995). So in every legal and practical sense the "network information" regulated by § 222 is, under that statute, "proprietary" to the service providers, not Carpenter. The Court does not argue otherwise.

Because Carpenter lacks a requisite connection to the cell-site records, he also may not claim a reasonable expectation of privacy in them. He could expect that a third party—the cell phone service provider—could use the information it collected, stored, and classified as its own for a variety of business and commercial purposes.

All this is not to say that *Miller* and *Smith* are without limits. *Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual's own "papers" or "effects," even when those papers or effects are held by a third party. See *Ex parte Jackson,* 96 U.S. 727, 733, 24 L.Ed. 877 (1878) (letters held by mail carrier); *United States v. Warshak,* 631 F.3d 266, 283–288 (C.A.6 2010) (e-mails held by Internet service provider). As already discussed, however, this case does not involve property or a bailment of that sort. Here the Government's acquisition of cell-site records falls within the heartland of *Miller* and *Smith*.

In fact, Carpenter's Fourth Amendment objection is even weaker than those of the defendants in *Miller* and *Smith*. Here the Government did not use a mere subpoena to obtain the cell-site records. It acquired the records only after it proved to a Magistrate Judge reasonable grounds to believe that the records were relevant and material to an ongoing criminal investigation. See 18 U.S.C. § 2703(d). So even if § 222 gave Carpenter some attenuated interest in the records, the Government's conduct here would be reasonable under the standards governing subpoenas. See *Donovan,* 464 U.S., at 415, 104 S.Ct. 769.

Under *Miller* and *Smith,* then, a search of the sort that requires a warrant simply did not occur when the Government used court-approved compulsory process, based on a finding of reasonable necessity, to compel a cell phone service provider, as owner, to disclose cell-site records.

III

The Court rejects a straightforward application of *Miller* and *Smith*. It concludes instead that applying those cases to cell-site records would work a "significant extension" of the principles underlying them, *ante,* at 2219, and holds that

the acquisition of more than six days of cell-site records constitutes a search, *ante,* at 2217, n. 3.

In my respectful view the majority opinion misreads this Court's precedents, old and recent, and transforms *Miller* and *Smith* into an unprincipled and unworkable doctrine. The Court's newly conceived constitutional standard will cause confusion; will undermine traditional and important law enforcement practices; and will allow the cell phone to become a protected medium that dangerous persons will use to commit serious crimes.

A

The Court errs at the outset by attempting to sidestep *Miller* and *Smith*. The Court frames this case as following instead from *United States v. Knotts,* 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), and *United States v. Jones,* 565 U.S. 400, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). Those cases, the Court suggests, establish that ***2231** "individuals have a reasonable expectation of privacy in the whole of their physical movements." *Ante,* at 2214 - 2216, 2217.

Knotts held just the opposite: "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." 460 U.S., at 281, 103 S.Ct. 1081. True, the Court in *Knotts* also suggested that "different constitutional principles may be applicable" to "dragnet-type law enforcement practices." *Id.,* at 284, 103 S.Ct. 1081. But by dragnet practices the Court was referring to " 'twenty-four hour surveillance of any citizen of this country ... without judicial knowledge or supervision.' " *Id.,* at 283, 103 S.Ct. 1081.

Those "different constitutional principles" mentioned in *Knotts,* whatever they may be, do not apply in this case. Here the Stored Communications Act requires a neutral judicial officer to confirm in each case that the Government has "reasonable grounds to believe" the cell-site records "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). This judicial check mitigates the Court's concerns about " 'a too permeating police surveillance.' " *Ante,* at 2214 (quoting *United States v. Di Re,* 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948)). Here, even more so than in *Knotts,* "reality hardly suggests abuse." 460 U.S., at 284, 103 S.Ct. 1081.

The Court's reliance on *Jones* fares no better. In *Jones* the Government installed a GPS tracking device on the defendant's automobile. The Court held the Government searched the automobile because it "physically occupied private property [of the defendant] for the purpose of obtaining information." 565 U.S., at 404, 132 S.Ct. 945. So in *Jones* it was "not necessary to inquire about the target's expectation of privacy in his vehicle's movements." *Grady v. North Carolina,* 575 U.S. ——, ——, 135 S.Ct. 1368, 1370, 191 L.Ed.2d 459 (2015) (*per curiam*).

Despite that clear delineation of the Court's holding in *Jones,* the Court today declares that *Jones* applied the " 'different constitutional principles' " alluded to in *Knotts* to establish that an individual has an expectation of privacy in the sum of his whereabouts. *Ante,* at 2215, 2217 - 2218. For that proposition the majority relies on the two concurring opinions in *Jones,* one of which stated that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring). But *Jones* involved direct governmental surveillance of a defendant's automobile without judicial authorization—specifically, GPS surveillance accurate within 50 to 100 feet. *Id.,* at 402–403, 132 S.Ct. 945. Even assuming that the different constitutional principles mentioned in *Knotts* would apply in a case like *Jones*—a proposition the Court was careful not to announce in *Jones, supra,* at 412–413, 132 S.Ct. 945—those principles are inapplicable here. Cases like this one, where the Government uses court-approved compulsory process to obtain records owned and controlled by a third party, are governed by the two majority opinions in *Miller* and *Smith*.

B

The Court continues its analysis by misinterpreting *Miller* and *Smith,* and then it reaches the wrong outcome on these facts even under its flawed standard.

The Court appears, in my respectful view, to read *Miller* and *Smith* to establish a balancing test. For each "qualitatively different category" of information, the Court suggests, the

privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party. See ***2232** *ante,* at 2216, 2219 - 2220. When the privacy interests are weighty enough to "overcome" the third-party disclosure, the Fourth Amendment's protections apply. See *ante,* at 2220.

That is an untenable reading of *Miller* and *Smith*. As already discussed, the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy. *Miller* and *Smith* do not establish the kind of category-by-category balancing the Court today prescribes.

But suppose the Court were correct to say that *Miller* and *Smith* rest on so imprecise a foundation. Still the Court errs, in my submission, when it concludes that cell-site records implicate greater privacy interests—and thus deserve greater Fourth Amendment protection—than financial records and telephone records.

Indeed, the opposite is true. A person's movements are not particularly private. As the Court recognized in *Knotts,* when the defendant there "traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination." 460 U.S., at 281–282, 103 S.Ct. 1081. Today expectations of privacy in one's location are, if anything, even less reasonable than when the Court decided *Knotts* over 30 years ago. Millions of Americans choose to share their location on a daily basis, whether by using a variety of location-based services on their phones, or by sharing their location with friends and the public at large via social media.

And cell-site records, as already discussed, disclose a person's location only in a general area. The records at issue here, for example, revealed Carpenter's location within an area covering between around a dozen and several hundred city blocks. "Areas of this scale might encompass bridal stores and Bass Pro Shops, gay bars and straight ones, a Methodist church and the local mosque." 819 F.3d 880, 889 (C.A.6 2016). These records could not reveal where Carpenter lives and works, much less his " 'familial, political, professional, religious, and sexual associations.' " *Ante,* at 2217 (quoting *Jones, supra,* at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring)).

By contrast, financial records and telephone records do " 'revea[l] ... personal affairs, opinions, habits and associations.' " *Miller,* 425 U.S., at 451, 96 S.Ct. 1619 (Brennan, J., dissenting); see *Smith,* 442 U.S., at 751, 99 S.Ct. 2577 (Marshall, J., dissenting). What persons purchase and to whom they talk might disclose how much money they make; the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; whether they go to gay bars or straight ones; and who are their closest friends and family members. The troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records.

Still, the Court maintains, cell-site records are "unique" because they are "comprehensive" in their reach; allow for retrospective collection; are "easy, cheap, and efficient compared to traditional investigative tools"; and are not exposed to cell phone service providers in a meaningfully voluntary manner. *Ante,* at 2216 - 2218, 2220, 2223. But many other kinds of business records can be so described. Financial records are of vast scope. Banks and credit card companies keep a comprehensive account of almost every transaction an individual makes on a daily basis. "With ***2233** just the click of a button, the Government can access each [company's] deep repository of historical [financial] information at practically no expense." *Ante,* at 2218. And the decision whether to transact with banks and credit card companies is no more or less voluntary than the decision whether to use a cell phone. Today, just as when *Miller* was decided, " 'it is impossible to participate in the economic life of contemporary society without maintaining a bank account.' " 425 U.S., at 451, 96 S.Ct. 1619 (BRENNAN, J., dissenting). But this Court, nevertheless, has held that individuals do not have a reasonable expectation of privacy in financial records.

Perhaps recognizing the difficulty of drawing the constitutional line between cell-site records and financial and telephonic records, the Court posits that the accuracy of cell-site records "is rapidly approaching GPS-level precision." *Ante,* at 2219. That is certainly plausible in the era of cyber technology, yet the privacy interests associated with location information, which is often disclosed to the public at large, still would not outweigh the privacy interests implicated by financial and telephonic records.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Perhaps more important, those future developments are no basis upon which to resolve this case. In general, the Court "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *Ontario v. Quon,* 560 U.S. 746, 759, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010). That judicial caution, prudent in most cases, is imperative in this one.

Technological changes involving cell phones have complex effects on crime and law enforcement. Cell phones make crimes easier to coordinate and conceal, while also providing the Government with new investigative tools that may have the potential to upset traditional privacy expectations. See Kerr, An Equilibrium–Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev 476, 512–517 (2011). How those competing effects balance against each other, and how property norms and expectations of privacy form around new technology, often will be difficult to determine during periods of rapid technological change. In those instances, and where the governing legal standard is one of reasonableness, it is wise to defer to legislative judgments like the one embodied in § 2703(d) of the Stored Communications Act. See *Jones,* 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring). In § 2703(d) Congress weighed the privacy interests at stake and imposed a judicial check to prevent executive overreach. The Court should be wary of upsetting that legislative balance and erecting constitutional barriers that foreclose further legislative instructions. See *Quon, supra,* at 759, 130 S.Ct. 2619. The last thing the Court should do is incorporate an arbitrary and outside limit—in this case six days' worth of cell-site records—and use it as the foundation for a new constitutional framework. The Court's decision runs roughshod over the mechanism Congress put in place to govern the acquisition of cell-site records and closes off further legislative debate on these issues.

C

The Court says its decision is a "narrow one." *Ante,* at 2220. But its reinterpretation of *Miller* and *Smith* will have dramatic consequences for law enforcement, courts, and society as a whole.

Most immediately, the Court's holding that the Government must get a warrant to obtain more than six days of cell-site records limits the effectiveness of an important investigative tool for solving serious crimes. As this case demonstrates, cell-site records are uniquely suited to help ***2234** the Government develop probable cause to apprehend some of the Nation's most dangerous criminals: serial killers, rapists, arsonists, robbers, and so forth. See also, *e.g., Davis,* 785 F.3d, at 500–501 (armed robbers); Brief for Alabama et al. as *Amici Curiae* 21–22 (serial killer). These records often are indispensable at the initial stages of investigations when the Government lacks the evidence necessary to obtain a warrant. See *United States v. Pembrook,* 876 F.3d 812, 816–819 (C.A.6 2017). And the long-term nature of many serious crimes, including serial crimes and terrorism offenses, can necessitate the use of significantly more than six days of cell-site records. The Court's arbitrary 6–day cutoff has the perverse effect of nullifying Congress' reasonable framework for obtaining cell-site records in some of the most serious criminal investigations.

The Court's decision also will have ramifications that extend beyond cell-site records to other kinds of information held by third parties, yet the Court fails "to provide clear guidance to law enforcement" and courts on key issues raised by its reinterpretation of *Miller* and *Smith*. *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2491, 189 L.Ed.2d 430 (2014).

First, the Court's holding is premised on cell-site records being a "distinct category of information" from other business records. *Ante,* at 2219. But the Court does not explain what makes something a distinct category of information. Whether credit card records are distinct from bank records; whether payment records from digital wallet applications are distinct from either; whether the electronic bank records available today are distinct from the paper and microfilm records at issue in *Miller*; or whether cell-phone call records are distinct from the home-phone call records at issue in *Smith,* are just a few of the difficult questions that require answers under the Court's novel conception of *Miller* and *Smith*.

Second, the majority opinion gives courts and law enforcement officers no indication how to determine whether any particular category of information falls on the financial-records side or the cell-site-records side of its newly conceived constitutional line. The Court's multifactor analysis —considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness—puts the law on a new and unstable foundation.

Third, even if a distinct category of information is deemed to be more like cell-site records than financial records, courts and law enforcement officers will have to guess how much of that information can be requested before a warrant is required. The Court suggests that less than seven days of location information may not require a warrant. See *ante,* at 2217, n. 3; see also *ante,* at 2220 - 2221 (expressing no opinion on "real-time CSLI," tower dumps, and security-camera footage). But the Court does not explain why that is so, and nothing in its opinion even alludes to the considerations that should determine whether greater or lesser thresholds should apply to information like IP addresses or website browsing history.

Fourth, by invalidating the Government's use of court-approved compulsory process in this case, the Court calls into question the subpoena practices of federal and state grand juries, legislatures, and other investigative bodies, as Justice ALITO's opinion explains. See *post,* at 2247 - 2257 (dissenting opinion). Yet the Court fails even to mention the serious consequences this will have for the proper administration of justice.

In short, the Court's new and uncharted course will inhibit law enforcement and "keep defendants and judges guessing for years to come." ***2235** *Riley,* 573 U.S., at ——, 134 S.Ct., at 2493 (internal quotation marks omitted).

* * *

This case should be resolved by interpreting accepted property principles as the baseline for reasonable expectations of privacy. Here the Government did not search anything over which Carpenter could assert ownership or control. Instead, it issued a court-authorized subpoena to a third party to disclose information it alone owned and controlled. That should suffice to resolve this case.

Having concluded, however, that the Government searched Carpenter when it obtained cell-site records from his cell phone service providers, the proper resolution of this case should have been to remand for the Court of Appeals to determine in the first instance whether the search was reasonable. Most courts of appeals, believing themselves bound by *Miller* and *Smith,* have not grappled with this question. And the Court's reflexive imposition of the warrant requirement obscures important and difficult issues, such as the scope of Congress' power to authorize the Government to collect new forms of information using processes that deviate from traditional warrant procedures, and how the Fourth Amendment's reasonableness requirement should apply when the Government uses compulsory process instead of engaging in an actual, physical search.

These reasons all lead to this respectful dissent.

APPENDIX

"**§ 2703. Required disclosure of customer communications or records**

"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."

Justice THOMAS, dissenting.

This case should not turn on "whether" a search occurred. *Ante,* at 2223 - 2224. It should turn, instead, on *whose* property was searched. The Fourth Amendment guarantees individuals the right to be secure from unreasonable searches of "*their* persons, houses, papers, and effects." (Emphasis added.) In other words, "*each* person has the right to be secure against unreasonable searches ... in *his own* person, house, papers, and effects." *Minnesota v. Carter,* 525 U.S. 83, 92, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (Scalia, J., concurring). By obtaining the cell-site records of MetroPCS and Sprint, the Government did not search Carpenter's property. He did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them. Neither the terms of his contracts nor any provision of law makes the records his. The records belong to MetroPCS and Sprint.

The Court concludes that, although the records are not Carpenter's, the Government must get a warrant because

Carpenter had a reasonable "expectation of privacy" ***2236** in the location information that they reveal. *Ante,* at 2216 - 2217. I agree with Justice KENNEDY, Justice ALITO, Justice GORSUCH, and every Court of Appeals to consider the question that this is not the best reading of our precedents.

The more fundamental problem with the Court's opinion, however, is its use of the "reasonable expectation of privacy" test, which was first articulated by Justice Harlan in *Katz v. United States,* 389 U.S. 347, 360–361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (concurring opinion). The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence. I respectfully dissent.

I

Katz was the culmination of a series of decisions applying the Fourth Amendment to electronic eavesdropping. The first such decision was *Olmstead v. United States,* 277 U.S. 438, 48 S.Ct. 564, 72 L.Ed. 944 (1928), where federal officers had intercepted the defendants' conversations by tapping telephone lines near their homes. *Id.,* at 456–457, 48 S.Ct. 564. In an opinion by Chief Justice Taft, the Court concluded that this wiretap did not violate the Fourth Amendment. No "search" occurred, according to the Court, because the officers did not physically enter the defendants' homes. *Id.,* at 464–466, 48 S.Ct. 564. And neither the telephone lines nor the defendants' intangible conversations qualified as "persons, houses, papers, [or] effects" within the meaning of the Fourth Amendment. *Ibid.* [1] In the ensuing decades, this Court adhered to *Olmstead* and rejected Fourth Amendment challenges to various methods of electronic surveillance. See *On Lee v. United States,* 343 U.S. 747, 749–753, 72 S.Ct. 967, 96 L.Ed. 1270 (1952) (use of microphone to overhear conversations with confidential informant); *Goldman v. United States,* 316 U.S. 129, 131–132, 135–136, 62 S.Ct. 993, 86 L.Ed. 1322 (1942) (use of detectaphone to hear conversations in office next door).

In the 1960's, however, the Court began to retreat from *Olmstead*. In *Silverman v. United States,* 365 U.S. 505, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961), for example, federal officers had eavesdropped on the defendants by driving a "spike mike" several inches into the house they were occupying. *Id.,* at 506–507, 81 S.Ct. 679. This was a "search," the Court held, because the "unauthorized physical penetration into the premises" was an "actual intrusion into a constitutionally protected area." *Id.,* at 509, 512, 81 S.Ct. 679. The Court did not mention *Olmstead* 's other holding that intangible conversations are not "persons, houses, papers, [or] effects." That omission was significant. The Court confirmed two years later that "[i]t follows from [*Silverman*] that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.' " *Wong Sun v. United States,* 371 U.S. 471, 485, 83 S.Ct. 407, 9 L.Ed.2d 441 (1963); accord, ***2237** *Berger v. New York,* 388 U.S. 41, 51, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967).

In *Katz,* the Court rejected *Olmstead* 's remaining holding—that eavesdropping is not a search absent a physical intrusion into a constitutionally protected area. The federal officers in *Katz* had intercepted the defendant's conversations by attaching an electronic device to the outside of a public telephone booth. 389 U.S., at 348, 88 S.Ct. 507. The Court concluded that this was a "search" because the officers "violated the privacy upon which [the defendant] justifiably relied while using the telephone booth." *Id.,* at 353, 88 S.Ct. 507. Although the device did not physically penetrate the booth, the Court overruled *Olmstead* and held that "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion." 389 U.S., at 353, 88 S.Ct. 507. The Court did not explain what should replace *Olmstead* 's physical-intrusion requirement. It simply asserted that "the Fourth Amendment protects people, not places" and "what [a person] seeks to preserve as private ... may be constitutionally protected." 389 U.S., at 351, 88 S.Ct. 507.

Justice Harlan's concurrence in *Katz* attempted to articulate the standard that was missing from the majority opinion. While Justice Harlan agreed that " 'the Fourth Amendment protects people, not places,' " he stressed that "[t]he question ... is what protection it affords to those people," and "the answer ... requires reference to a 'place.' " *Id.,* at 361, 88 S.Ct. 507. Justice Harlan identified a "twofold requirement" to determine when the protections of the Fourth

Amendment apply: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' " *Ibid.*

Justice Harlan did not cite anything for this "expectation of privacy" test, and the parties did not discuss it in their briefs. The test appears to have been presented for the first time at oral argument by one of the defendant's lawyers. See Winn, *Katz* and the Origins of the "Reasonable Expectation of Privacy" Test, 40 McGeorge L. Rev. 1, 9–10 (2009). The lawyer, a recent law-school graduate, apparently had an "[e]piphany" while preparing for oral argument. Schneider, *Katz v. United States*: The Untold Story, 40 McGeorge L. Rev. 13, 18 (2009). He conjectured that, like the "reasonable person" test from his Torts class, the Fourth Amendment should turn on "whether a reasonable person ... could have expected his communication to be private." *Id.,* at 19. The lawyer presented his new theory to the Court at oral argument. See, *e.g.,* Tr. of Oral Arg. in *Katz v. United States,* O.T. 1967, No. 35, p. 5 (proposing a test of "whether or not, objectively speaking, the communication was intended to be private"); *id.,* at 11 ("We propose a test using a way that's not too dissimilar from the tort 'reasonable man' test"). After some questioning from the Justices, the lawyer conceded that his test should also require individuals to subjectively expect privacy. See *id.,* at 12. With that modification, Justice Harlan seemed to accept the lawyer's test almost verbatim in his concurrence.

Although the majority opinion in *Katz* had little practical significance after Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968, Justice Harlan's concurrence profoundly changed our Fourth Amendment jurisprudence. It took only one year for the full Court to adopt his two-pronged test. See *Terry v. Ohio,* 392 U.S. 1, 10, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968). And by 1979, the Court was describing Justice Harlan's test as the "lodestar" for determining whether ***2238** a "search" had occurred. *Smith v. Maryland,* 442 U.S. 735, 739, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). Over time, the Court minimized the subjective prong of Justice Harlan's test. See Kerr, *Katz* Has Only One Step: The Irrelevance of Subjective Expectations, 82 U. Chi. L. Rev. 113 (2015). That left the objective prong —the "reasonable expectation of privacy" test that the Court still applies today. See *ante,* at 2213 - 2214; *United States v. Jones,* 565 U.S. 400, 406, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012).

II

Under the *Katz* test, a "search" occurs whenever "government officers violate a person's 'reasonable expectation of privacy.' " *Jones, supra,* at 406, 132 S.Ct. 945. The most glaring problem with this test is that it has "no plausible foundation in the text of the Fourth Amendment." *Carter,* 525 U.S., at 97, 119 S.Ct. 469 (opinion of Scalia, J.). The Fourth Amendment, as relevant here, protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches." By defining "search" to mean "any violation of a reasonable expectation of privacy," the *Katz* test misconstrues virtually every one of these words.

A

The *Katz* test distorts the original meaning of "searc[h]"—the word in the Fourth Amendment that it purports to define, see *ante,* at 2213 - 2214; *Smith, supra*. Under the *Katz* test, the government conducts a search anytime it violates someone's "reasonable expectation of privacy." That is not a normal definition of the word "search."

At the founding, "search" did not mean a violation of someone's reasonable expectation of privacy. The word was probably not a term of art, as it does not appear in legal dictionaries from the era. And its ordinary meaning was the same as it is today: " '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.' " *Kyllo v. United States,* 533 U.S. 27, 32, n. 1, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (quoting N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed. 1989)); accord, 2 S. Johnson, A Dictionary of the English Language (5th ed. 1773) ("Inquiry by looking into every suspected place"); N. Bailey, An Universal Etymological English Dictionary (22d ed. 1770) ("a seeking after, a looking for, & c."); 2 J. Ash, The New and Complete Dictionary of the English Language (2d ed. 1795) ("An enquiry, an examination, the act of seeking, an enquiry by looking into every suspected place; a quest; a pursuit"); T. Sheridan, A Complete Dictionary of the English Language (6th ed. 1796) (similar). The word "search" was not associated with "reasonable expectation

of privacy" until Justice Harlan coined that phrase in 1967. The phrase "expectation(s) of privacy" does not appear in the pre-*Katz* federal or state case reporters, the papers of prominent Founders,[2] early congressional documents and debates,[3] collections of early American English texts,[4] or early American newspapers. ***2239** [5]

B

The *Katz* test strays even further from the text by focusing on the concept of "privacy." The word "privacy" does not appear in the Fourth Amendment (or anywhere else in the Constitution for that matter). Instead, the Fourth Amendment references "[t]he right of the people to be secure." It then qualifies that right by limiting it to "persons" and three specific types of property: "houses, papers, and effects." By connecting the right to be secure to these four specific objects, "[t]he text of the Fourth Amendment reflects its close connection to property." *Jones, supra,* at 405, 132 S.Ct. 945. "[P]rivacy," by contrast, "was not part of the political vocabulary of the [founding]. Instead, liberty and privacy rights were understood largely in terms of property rights." Cloud, Property Is Privacy: Locke and Brandeis in the Twenty–First Century, 55 Am. Crim. L. Rev. 37, 42 (2018).

Those who ratified the Fourth Amendment were quite familiar with the notion of security in property. Security in property was a prominent concept in English law. See, *e.g.,* 3 W. Blackstone, Commentaries on the Laws of England 288 (1768) ("[E]very man's house is looked upon by the law to be his castle"); 3 E. Coke, Institutes of Laws of England 162 (6th ed. 1680) ("[F]or a man[']s house is his Castle, & domus sua cuique est tutissimum refugium [each man's home is his safest refuge]"). The political philosophy of John Locke, moreover, "permeated the 18th-century political scene in America." *Obergefell v. Hodges,* 576 U.S. ——, ——, 135 S.Ct. 2584, 2634, 192 L.Ed.2d 609 (2015) (THOMAS, J., dissenting). For Locke, every individual had a property right "in his own person" and in anything he "removed from the common state [of] Nature" and "mixed his labour with." Second Treatise of Civil Government § 27 (1690). Because property is "very unsecure" in the state of nature, § 123, individuals form governments to obtain "a secure enjoyment of their properties." § 95. Once a government is formed, however, it cannot be given "a power to destroy that which every one designs to secure"; it cannot legitimately "endeavour to take away, and destroy the property of the people," or exercise "an absolute power over [their] lives, liberties, and estates." § 222.

The concept of security in property recognized by Locke and the English legal tradition appeared throughout the materials that inspired the Fourth Amendment. In *Entick v. Carrington,* 19 How. St. Tr. 1029 (C.P. 1765)—a heralded decision that the founding generation considered "the true and ultimate expression of constitutional law," *Boyd v. United States,* 116 U.S. 616, 626, 6 S.Ct. 524, 29 L.Ed. 746 (1886)—Lord Camden explained that "[t]he great end, for which men entered into society, was to secure their property." 19 How. St. Tr., at 1066. The American colonists echoed this reasoning in their "widespread hostility" to the Crown's writs of assistance [6]—a practice that inspired the Revolution and became "[t]he driving force behind the adoption of the [Fourth] Amendment." ***2240** *United States v. Verdugo–Urquidez,* 494 U.S. 259, 266, 110 S.Ct. 1056, 108 L.Ed.2d 222 (1990). Prominent colonists decried the writs as destroying " 'domestic security' " by permitting broad searches of homes. M. Smith, The Writs of Assistance Case 475 (1978) (quoting a 1772 Boston town meeting); see also *id.,* at 562 (complaining that " 'every householder in this province, will necessarily become *less secure* than he was before this writ' " (quoting a 1762 article in the Boston Gazette)); *id.,* at 493 (complaining that the writs were " 'expressly contrary to the common law, which ever regarded a man's *house* as his castle, or a place of perfect security' " (quoting a 1768 letter from John Dickinson)). John Otis, who argued the famous Writs of Assistance case, contended that the writs violated " 'the fundamental Principl[e] of Law' " that " '[a] Man who is quiet, is as secure in his House, as a Prince in his Castle.' " *Id.,* at 339 (quoting John Adam's notes). John Adams attended Otis' argument and later drafted Article XIV of the Massachusetts Constitution, [7] which served as a model for the Fourth Amendment. See Clancy, The Framers' Intent: John Adams, His Era, and the Fourth Amendment, 86 Ind. L.J. 979, 982 (2011); Donahue, The Original Fourth Amendment, 83 U. Chi. L. Rev. 1181, 1269 (2016) (Donahue). Adams agreed that "[p]roperty must be secured, or liberty cannot exist." Discourse on Davila, in 6 The Works of John Adams 280 (C. Adams ed. 1851).

Of course, the founding generation understood that, by securing their property, the Fourth Amendment would often protect their privacy as well. See, *e.g.,* *Boyd, supra,* at 630,

6 S.Ct. 524 (explaining that searches of houses invade "the privacies of life"); *Wilkes v. Wood,* 19 How. St. Tr. 1153, 1154 (C.P. 1763) (argument of counsel contending that seizures of papers implicate "our most private concerns"). But the Fourth Amendment's attendant protection of privacy does not justify *Katz* 's elevation of privacy as the *sine qua non* of the Amendment. See T. Clancy, The Fourth Amendment: Its History and Interpretation § 3.4.4, p. 78 (2008) ("[The *Katz* test] confuse[s] the reasons for exercising the protected right with the right itself. A purpose of exercising one's Fourth Amendment rights might be the desire for privacy, but the individual's motivation is not the right protected"); cf. *United States v. Gonzalez–Lopez,* 548 U.S. 140, 145, 126 S.Ct. 2557, 165 L.Ed.2d 409 (2006) (rejecting "a line of reasoning that 'abstracts from the right to its purposes, and then eliminates the right' "). As the majority opinion in *Katz* recognized, the Fourth Amendment "cannot be translated into a general constitutional 'right to privacy,' " as its protections "often have nothing to do with privacy at all." 389 U.S., at 350, 88 S.Ct. 507. Justice Harlan's focus on privacy in his concurrence—an opinion that was issued between *Griswold v. Connecticut,* 381 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965), and *Roe v. Wade,* 410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147 (1973)—reflects privacy's status as the organizing constitutional idea of the 1960's and 1970's. The organizing constitutional idea of the founding era, by contrast, was property.

***2241** C

In shifting the focus of the Fourth Amendment from property to privacy, the *Katz* test also reads the words "persons, houses, papers, and effects" out of the text. At its broadest formulation, the *Katz* test would find a search "*wherever* an individual may harbor a reasonable 'expectation of privacy.' " *Terry,* 392 U.S., at 9, 88 S.Ct. 1868 (emphasis added). The Court today, for example, does not ask whether cell-site location records are "persons, houses, papers, [or] effects" within the meaning of the Fourth Amendment. [8] Yet "persons, houses, papers, and effects" cannot mean "anywhere" or "anything." *Katz* 's catchphrase that "the Fourth Amendment protects people, not places," is not a serious attempt to reconcile the constitutional text. See *Carter,* 525 U.S., at 98, n. 3, 119 S.Ct. 469 (opinion of Scalia, J.). The Fourth Amendment obviously protects people; "[t]he question ... is what protection it affords to those people." *Katz,* 389 U.S., at 361, 88 S.Ct. 507 (Harlan, J., concurring). The Founders decided to protect the people from unreasonable searches and seizures of four specific things—persons, houses, papers, and effects. They identified those four categories as "the objects of privacy protection to which the *Constitution* would extend, leaving further expansion to the good judgment ... of the people through their representatives in the legislature." *Carter, supra,* at 97–98, 119 S.Ct. 469 (opinion of Scalia, J.).

This limiting language was important to the founders. Madison's first draft of the Fourth Amendment used a different phrase: "their persons, their houses, their papers, and their *other property*." 1 Annals of Cong. 452 (1789) (emphasis added). In one of the few changes made to Madison's draft, the House Committee of Eleven changed "other property" to "effects." See House Committee of Eleven Report (July 28, 1789), in N. Cogan, The Complete Bill of Rights 334 (2d ed. 2015). This change might have narrowed the Fourth Amendment by clarifying that it does not protect real property (other than houses). See *Oliver v. United States,* 466 U.S. 170, 177, and n. 7, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984); Davies, Recovering the Original Fourth Amendment, 98 Mich. L. Rev. 547, 709–714 (1999) (Davies). Or the change might have broadened the Fourth Amendment by clarifying that it protects commercial goods, not just personal possessions. See Donahue 1301. Or it might have done both. Whatever its ultimate effect, the change reveals that the Founders understood the phrase "persons, houses, papers, and effects" to be an important measure of the Fourth Amendment's overall scope. See Davies 710. The *Katz* test, however, displaces and renders that phrase entirely "superfluous." *Jones,* 565 U.S., at 405, 132 S.Ct. 945.

D

"[P]ersons, houses, papers, and effects" are not the only words that the *Katz* test reads out of the Fourth Amendment. The Fourth Amendment specifies that the people have a right to be secure from unreasonable searches of "their" persons, houses, papers, and effects. Although phrased in the plural, "[t]he obvious meaning of ['their'] is that *each* person has the right to be secure against unreasonable searches ***2242** and seizures in *his own* person, house, papers, and effects." *Carter, supra,* at 92, 119 S.Ct. 469 (opinion of Scalia,

J.); see also *District of Columbia v. Heller,* 554 U.S. 570, 579, 128 S.Ct. 2783, 171 L.Ed.2d 637 (2008) (explaining that the Constitution uses the plural phrase "the people" to "refer to individual rights, not 'collective' rights"). Stated differently, the word "their" means, at the very least, that individuals do not have Fourth Amendment rights in *someone else's* property. See *Carter, supra,* at 92–94, 119 S.Ct. 469 (opinion of Scalia, J.). Yet, under the *Katz* test, individuals can have a reasonable expectation of privacy in another person's property. See, *e.g.,* *Carter,* 525 U.S., at 89, 119 S.Ct. 469 (majority opinion) ("[A] person may have a legitimate expectation of privacy in the house of someone else"). Until today, our precedents have not acknowledged that individuals can claim a reasonable expectation of privacy in someone else's business records. See *ante,* at 2224 (KENNEDY, J., dissenting). But the Court erases that line in this case, at least for cell-site location records. In doing so, it confirms that the *Katz* test does not necessarily require an individual to prove that the government searched *his* person, house, paper, or effect.

Carpenter attempts to argue that the cell-site records are, in fact, his "papers," see Brief for Petitioner 32–35; Reply Brief 14–15, but his arguments are unpersuasive, see *ante,* at 2229 - 2230 (opinion of KENNEDY, J.); *post,* at 2257 - 2259 (ALITO, J., dissenting). Carpenter stipulated below that the cell-site records are the business records of Sprint and MetroPCS. See App. 51. He cites no property law in his briefs to this Court, and he does not explain how he has a property right in the companies' records under the law of any jurisdiction at any point in American history. If someone stole these records from Sprint or MetroPCS, Carpenter does not argue that he could recover in a traditional tort action. Nor do his contracts with Sprint and MetroPCS make the records his, even though such provisions could exist in the marketplace. Cf., *e.g.,* Google Terms of Service, https://policies.google.com/terms ("Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours").

Instead of property, tort, or contract law, Carpenter relies on the federal Telecommunications Act of 1996 to demonstrate that the cell site records are his papers. The Telecommunications Act generally bars cell-phone companies from disclosing customers' cell site location information to the public. See 47 U.S.C. § 222(c). This is sufficient to make the records his, Carpenter argues, because the Fourth Amendment merely requires him to identify a source of "positive law" that "protects against access by the public without consent." Brief for Petitioner 32–33 (citing Baude & Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1825–1826 (2016); emphasis deleted).

Carpenter is mistaken. To come within the text of the Fourth Amendment, Carpenter must prove that the cell-site records are *his* ; positive law is potentially relevant only insofar as it answers that question. The text of the Fourth Amendment cannot plausibly be read to mean "any violation of positive law" any more than it can plausibly be read to mean "any violation of a reasonable expectation of privacy."

Thus, the Telecommunications Act is insufficient because it does not give Carpenter a property right in the cell-site records. Section 222, titled "Privacy of customer ***2243** information," protects customers' privacy by preventing cell-phone companies from disclosing sensitive information about them. The statute creates a "duty to protect the confidentiality" of information relating to customers, § 222(a), and creates "[p]rivacy requirements" that limit the disclosure of that information, § 222(c)(1). Nothing in the text pre-empts state property law or gives customers a property interest in the companies' business records (assuming Congress even has that authority). [9] Although § 222 "protects the interests of individuals against wrongful uses or disclosures of personal data, the rationale for these legal protections has not historically been grounded on a perception that people have property rights in personal data as such." Samuelson, Privacy as Intellectual Property? 52 Stan. L. Rev. 1125, 1130–1131 (2000) (footnote omitted). Any property rights remain with the companies.

E

The *Katz* test comes closer to the text of the Fourth Amendment when it asks whether an expectation of privacy is "reasonable," but it ultimately distorts that term as well. The Fourth Amendment forbids "unreasonable searches." In other words, reasonableness determines the legality of a search, not "whether a search ... within the meaning of the Constitution has *occurred*." *Carter,* 525 U.S., at 97, 119 S.Ct. 469 (opinion of Scalia, J.) (internal quotation marks omitted).

Moreover, the *Katz* test invokes the concept of reasonableness in a way that would be foreign to the ratifiers of the Fourth Amendment. Originally, the word "unreasonable" in the Fourth Amendment likely meant "against reason"—as in "against the reason of the common law." See Donahue 1270–1275; Davies 686–693; *California v. Acevedo,* 500 U.S. 565, 583, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991) (Scalia, J., concurring in judgment). At the founding, searches and seizures were regulated by a robust body of common-law rules. See generally W. Cuddihy, The Fourth Amendment: Origins and Original Meaning 602–1791 (2009); *e.g., Wilson v. Arkansas,* 514 U.S. 927, 931–936, 115 S.Ct. 1914, 131 L.Ed.2d 976 (1995) (discussing the common-law knock-and-announce rule). The search-and-seizure practices that the Founders feared most—such as general warrants—were already illegal under the common law, and jurists such as Lord Coke described violations of the common law as "against reason." See Donahue 1270–1271, and n. 513. Locke, Blackstone, Adams, and other influential figures shortened the phrase "against reason" to "unreasonable." See *id.,* at 1270–1275. Thus, by prohibiting "unreasonable" searches and seizures in the Fourth Amendment, the Founders ensured that the newly created Congress could not use legislation to abolish the established common-law rules of search and seizure. See T. Cooley, Constitutional Limitations *303 (2d ed. 1871); 3 J. Story, Commentaries on the ***2244** Constitution of the United States § 1895, p. 748 (1833).

Although the Court today maintains that its decision is based on "Founding-era understandings," *ante,* at 2214, the Founders would be puzzled by the Court's conclusion as well as its reasoning. The Court holds that the Government unreasonably searched Carpenter by subpoenaing the cell-site records of Sprint and MetroPCS without a warrant. But the Founders would not recognize the Court's "warrant requirement." *Ante,* at 2222. The common law required warrants for some types of searches and seizures, but not for many others. The relevant rule depended on context. See *Acevedo, supra,* at 583–584, 111 S.Ct. 1982 (opinion of Scalia, J.); Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 763–770 (1994); Davies 738–739. In cases like this one, a subpoena for third-party documents was not a "search" to begin with, and the common law did not limit the government's authority to subpoena third parties. See *post,* at 2247 - 2253 (ALITO, J., dissenting). Suffice it to say, the Founders would be confused by this Court's transformation of their common-law protection of property into a "warrant requirement" and a vague inquiry into "reasonable expectations of privacy."

III

That the *Katz* test departs so far from the text of the Fourth Amendment is reason enough to reject it. But the *Katz* test also has proved unworkable in practice. Jurists and commentators tasked with deciphering our jurisprudence have described the *Katz* regime as "an unpredictable jumble," "a mass of contradictions and obscurities," "all over the map," "riddled with inconsistency and incoherence," "a series of inconsistent and bizarre results that [the Court] has left entirely undefended," "unstable," "chameleon-like," " 'notoriously unhelpful,' " "a conclusion rather than a starting point for analysis," "distressingly unmanageable," "a dismal failure," "flawed to the core," "unadorned fiat," and "inspired by the kind of logic that produced Rube Goldberg's bizarre contraptions." [10] Even Justice Harlan, four years after penning his concurrence in *Katz,* confessed that the test encouraged "the substitution of words for analysis." *United States v. White,* 401 U.S. 745, 786, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971) (dissenting opinion).

***2245** After 50 years, it is still unclear what question the *Katz* test is even asking. This Court has steadfastly declined to elaborate the relevant considerations or identify any meaningful constraints. See, *e.g., ante,* at 2213 - 2214 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *O'Connor v. Ortega,* 480 U.S. 709, 715, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987) (plurality opinion) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable"); *Oliver,* 466 U.S., at 177, 104 S.Ct. 1735 ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion").

Justice Harlan's original formulation of the *Katz* test appears to ask a descriptive question: Whether a given expectation of privacy is "one that society is prepared to recognize as 'reasonable.' " 389 U.S., at 361, 88 S.Ct. 507. As written, the *Katz* test turns on society's actual, current views about the reasonableness of various expectations of privacy.

But this descriptive understanding presents several problems. For starters, it is easily circumvented. If, for example, "the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry," individuals could not realistically expect privacy in their homes. *Smith,* 442 U.S., at 740, n. 5, 99 S.Ct. 2577; see also Chemerinsky, Rediscovering Brandeis's Right to Privacy, 45 Brandeis L.J. 643, 650 (2007) ("[Under *Katz,* t]he government seemingly can deny privacy just by letting people know in advance not to expect any"). A purely descriptive understanding of the *Katz* test also risks "circular[ity]." *Kyllo,* 533 U.S., at 34, 121 S.Ct. 2038. While this Court is supposed to base its decisions on society's expectations of privacy, society's expectations of privacy are, in turn, shaped by this Court's decisions. See Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 S.Ct. Rev. 173, 188 ("[W]hether [a person] will or will not have [a reasonable] expectation [of privacy] will depend on what the legal rule is").

To address this circularity problem, the Court has insisted that expectations of privacy must come from outside its Fourth Amendment precedents, "either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Rakas v. Illinois,* 439 U.S. 128, 144, n. 12, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). But the Court's supposed reliance on "real or personal property law" rings hollow. The whole point of *Katz* was to " 'discredi[t]' " the relationship between the Fourth Amendment and property law, 389 U.S., at 353, 88 S.Ct. 507, and this Court has repeatedly downplayed the importance of property law under the *Katz* test, see, *e.g., United States v. Salvucci,* 448 U.S. 83, 91, 100 S.Ct. 2547, 65 L.Ed.2d 619 (1980) ("[P]roperty rights are neither the beginning nor the end of this Court's inquiry [under *Katz*]"); *Rawlings v. Kentucky,* 448 U.S. 98, 105, 100 S.Ct. 2556, 65 L.Ed.2d 633 (1980) ("[This Court has] emphatically rejected the notion that 'arcane' concepts of property law ought to control the ability to claim the protections of the Fourth Amendment"). Today, for example, the Court makes no mention of property law, except to reject its relevance. See *ante,* at 2214, and n. 1.

As for "understandings that are recognized or permitted in society," this Court has never answered even the most basic questions about what this means. See Kerr, ***2246** Four Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 504–505 (2007). For example, our precedents do not explain who is included in "society," how we know what they "recogniz[e] or permi[t]," and how much of society must agree before something constitutes an "understanding."

Here, for example, society might prefer a balanced regime that prohibits the Government from obtaining cell-site location information unless it can persuade a neutral magistrate that the information bears on an ongoing criminal investigation. That is precisely the regime Congress created under the Stored Communications Act and Telecommunications Act. See 47 U.S.C. § 222(c)(1); 18 U.S.C. §§ 2703(c)(1)(B), (d). With no sense of irony, the Court invalidates this regime today—the one that society actually created "in the form of its elected representatives in Congress." 819 F.3d 880, 890 (2016).

Truth be told, this Court does not treat the *Katz* test as a descriptive inquiry. Although the *Katz* test is phrased in descriptive terms about society's views, this Court treats it like a normative question—whether a particular practice *should* be considered a search under the Fourth Amendment. Justice Harlan thought this was the best way to understand his test. See *White,* 401 U.S., at 786, 91 S.Ct. 1122 (dissenting opinion) (explaining that courts must assess the "desirability" of privacy expectations and ask whether courts "should" recognize them by "balanc[ing]" the "impact on the individual's sense of security ... against the utility of the conduct as a technique of law enforcement"). And a normative understanding is the only way to make sense of this Court's precedents, which bear the hallmarks of subjective policymaking instead of neutral legal decisionmaking. "[T]he only thing the past three decades have established about the *Katz* test" is that society's expectations of privacy "bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable." *Carter,* 525 U.S., at 97, 119 S.Ct. 469 (opinion of Scalia, J.). Yet, "[t]hough we know ourselves to be eminently reasonable, self-awareness of eminent reasonableness is not really a substitute for democratic election." *Sosa v. Alvarez–Machain,* 542 U.S. 692, 750, 124 S.Ct. 2739, 159 L.Ed.2d 718 (2004) (Scalia, J., concurring in part and concurring in judgment).

* * *

In several recent decisions, this Court has declined to apply the *Katz* test because it threatened to narrow the original scope

of the Fourth Amendment. See *Grady v. North Carolina,* 575 U.S. ——, ——, 135 S.Ct. 1368, 1370, 191 L.Ed.2d 459 (2015) (*per curiam*); *Florida v. Jardines,* 569 U.S. 1, 5, 133 S.Ct. 1409, 185 L.Ed.2d 495 (2013); *Jones,* 565 U.S., at 406–407, 132 S.Ct. 945. But as today's decision demonstrates, *Katz* can also be invoked to expand the Fourth Amendment beyond its original scope. This Court should not tolerate errors in either direction. "The People, through ratification, have already weighed the policy tradeoffs that constitutional rights entail." *Luis v. United States,* 578 U.S. ——, ——, 136 S.Ct. 1083, 1101, 194 L.Ed.2d 256 (2016) (THOMAS, J., concurring in judgment). Whether the rights they ratified are too broad or too narrow by modern lights, this Court has no authority to unilaterally alter the document they approved.

Because the *Katz* test is a failed experiment, this Court is dutybound to reconsider it. Until it does, I agree with my dissenting colleagues' reading of our precedents. Accordingly, I respectfully dissent.

Justice ALITO, with whom Justice THOMAS joins, dissenting.

I share the Court's concern about the effect of new technology on personal privacy, ***2247** but I fear that today's decision will do far more harm than good. The Court's reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely.

First, the Court ignores the basic distinction between an actual search (dispatching law enforcement officers to enter private premises and root through private papers and effects) and an order merely requiring a party to look through its own records and produce specified documents. The former, which intrudes on personal privacy far more deeply, requires probable cause; the latter does not. Treating an order to produce like an actual search, as today's decision does, is revolutionary. It violates both the original understanding of the Fourth Amendment and more than a century of Supreme Court precedent. Unless it is somehow restricted to the particular situation in the present case, the Court's move will cause upheaval. Must every grand jury subpoena *duces tecum* be supported by probable cause? If so, investigations of terrorism, political corruption, white-collar crime, and many other offenses will be stymied. And what about subpoenas and other document-production orders issued by administrative agencies? See, *e.g.,* 15 U.S.C. § 57b–1(c) (Federal Trade Commission); §§ 77s(c), 78u(a)-(b) (Securities and Exchange Commission); 29 U.S.C. § 657(b) (Occupational Safety and Health Administration); 29 C.F.R. § 1601.16(a)(2) (2017) (Equal Employment Opportunity Commission).

Second, the Court allows a defendant to object to the search of a third party's property. This also is revolutionary. The Fourth Amendment protects "[t]he right of the people to be secure in *their* persons, houses, papers, and effects" (emphasis added), not the persons, houses, papers, and effects of others. Until today, we have been careful to heed this fundamental feature of the Amendment's text. This was true when the Fourth Amendment was tied to property law, and it remained true after *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), broadened the Amendment's reach.

By departing dramatically from these fundamental principles, the Court destabilizes long-established Fourth Amendment doctrine. We will be making repairs—or picking up the pieces —for a long time to come.

I

Today the majority holds that a court order requiring the production of cell-site records may be issued only after the Government demonstrates probable cause. See *ante,* at 2220 - 2221. That is a serious and consequential mistake. The Court's holding is based on the premise that the order issued in this case was an actual "search" within the meaning of the Fourth Amendment, but that premise is inconsistent with the original meaning of the Fourth Amendment and with more than a century of precedent.

A

The order in this case was the functional equivalent of a subpoena for documents, and there is no evidence that these writs were regarded as "searches" at the time of the founding. Subpoenas *duces tecum* and other forms of compulsory document production were well known to the founding generation. Blackstone dated the first writ of subpoena to the reign of King Richard II in the late 14th century, and by the end of the 15th century, the use of such writs had "become

the daily practice of the [Chancery] court." 3 W. Blackstone, ***2248** Commentaries on the Laws of England 53 (G. Tucker ed. 1803) (Blackstone). Over the next 200 years, subpoenas would grow in prominence and power in tandem with the Court of Chancery, and by the end of Charles II's reign in 1685, two important innovations had occurred.

First, the Court of Chancery developed a new species of subpoena. Until this point, subpoenas had been used largely to compel attendance and oral testimony from witnesses; these subpoenas correspond to today's subpoenas *ad testificandum*. But the Court of Chancery also improvised a new version of the writ that tacked onto a regular subpoena an order compelling the witness to bring certain items with him. By issuing these so-called subpoenas *duces tecum,* the Court of Chancery could compel the production of papers, books, and other forms of physical evidence, whether from the parties to the case or from third parties. Such subpoenas were sufficiently commonplace by 1623 that a leading treatise on the practice of law could refer in passing to the fee for a "*Sub poena of Ducas tecum* " (seven shillings and two pence) without needing to elaborate further. T. Powell, The Attourneys Academy 79 (1623). Subpoenas *duces tecum* would swell in use over the next century as the rules for their application became ever more developed and definite. See, *e.g.,* 1 G. Jacob, The Compleat Chancery–Practiser 290 (1730) ("The *Subpoena duces tecum* is awarded when the Defendant has confessed by his Answer that he hath such Writings in his Hands as are prayed by the Bill to be discovered or brought into Court").

Second, although this new species of subpoena had its origins in the Court of Chancery, it soon made an appearance in the work of the common-law courts as well. One court later reported that "[t]he Courts of Common law ... employed the same or similar means ... from the time of Charles the Second at least." *Amey v. Long,* 9 East. 473, 484, 103 Eng. Rep. 653, 658 (K.B. 1808).

By the time Blackstone published his Commentaries on the Laws of England in the 1760's, the use of subpoenas *duces tecum* had bled over substantially from the courts of equity to the common-law courts. Admittedly, the transition was still incomplete: In the context of jury trials, for example, Blackstone complained about "the want of a compulsive power for the production of books and papers belonging to the parties." Blackstone 381; see also, *e.g., Entick v. Carrington,* 19 State Trials 1029, 1073 (K.B. 1765) ("I wish some cases had been shewn, where the law forceth evidence out of the owner's custody by process. [But] where the adversary has by force or fraud got possession of your own proper evidence, there is no way to get it back but by action"). But Blackstone found some comfort in the fact that at least those documents "[i]n the hands of third persons ... can generally be obtained by rule of court, or by adding a clause of requisition to the writ of *subpoena,* which is then called a *subpoena duces tecum*." Blackstone 381; see also, *e.g., Leeds v. Cook,* 4 Esp. 256, 257, 170 Eng. Rep. 711 (N.P. 1803) (third-party subpoena *duces tecum*); *Rex v. Babb,* 3 T.R. 579, 580, 100 Eng. Rep. 743, 744 (K.B. 1790) (third-party document production). One of the primary questions outstanding, then, was whether common-law courts would remedy the "defect[s]" identified by the Commentaries, and allow parties to use subpoenas *duces tecum* not only with respect to third parties but also with respect to each other. Blackstone 381.

That question soon found an affirmative answer on both sides of the Atlantic. In the United States, the First Congress established the federal court system in the ***2249** Judiciary Act of 1789. As part of that Act, Congress authorized "all the said courts of the United States ... in the trial of actions at law, on motion and due notice thereof being given, to require the parties to produce books or writings in their possession or power, which contain evidence pertinent to the issue, in cases and under circumstances where they might be compelled to produce the same by the ordinary rules of proceeding in chancery." § 15, 1 Stat. 82. From that point forward, federal courts in the United States could compel the production of documents regardless of whether those documents were held by parties to the case or by third parties.

In Great Britain, too, it was soon definitively established that common-law courts, like their counterparts in equity, could subpoena documents held either by parties to the case or by third parties. After proceeding in fits and starts, the King's Bench eventually held in *Amey v. Long* that the "writ of subpoena duces tecum [is] a writ of compulsory obligation and effect in the law." 9 East., at 486, 103 Eng. Rep., at 658. Writing for a unanimous court, Lord Chief Justice Ellenborough explained that "[t]he right to resort to means competent to compel the production of written, as well as oral, testimony seems essential to the very existence and constitution of a Court of Common Law." *Id.,* at 484, 103 Eng. Rep., at 658. Without the power to issue subpoenas *duces tecum,* the Lord Chief Justice observed, common-law courts "could not possibly proceed with due effect." *Ibid.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

The prevalence of subpoenas *duces tecum* at the time of the founding was not limited to the civil context. In criminal cases, courts and prosecutors were also using the writ to compel the production of necessary documents. In *Rex v. Dixon,* 3 Burr. 1687, 97 Eng. Rep. 1047 (K.B. 1765), for example, the King's Bench considered the propriety of a subpoena *duces tecum* served on an attorney named Samuel Dixon. Dixon had been called "to give evidence before the grand jury of the county of Northampton" and specifically "to produce three vouchers ... in order to found a prosecution by way of indictment against [his client] Peach ... for forgery." *Id.,* at 1687, 97 Eng. Rep., at 1047–1048. Although the court ultimately held that Dixon had not needed to produce the vouchers on account of attorney-client privilege, none of the justices expressed the slightest doubt about the general propriety of subpoenas *duces tecum* in the criminal context. See *id.,* at 1688, 97 Eng. Rep., at 1048. As Lord Chief Justice Ellenborough later explained, "[i]n that case no objection was taken to the writ, but to the special circumstances under which the party possessed the papers; so that the Court may be considered as recognizing the general obligation to obey writs of that description in other cases." *Amey, supra,* at 485, 103 Eng. Rep., at 658; see also 4 J. Chitty, Practical Treatise on the Criminal Law 185 (1816) (template for criminal subpoena *duces tecum*).

As *Dixon* shows, subpoenas *duces tecum* were routine in part because of their close association with grand juries. Early American colonists imported the grand jury, like so many other common-law traditions, and they quickly flourished. See *United States v. Calandra,* 414 U.S. 338, 342–343, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974). Grand juries were empaneled by the federal courts almost as soon as the latter were established, and both they and their state counterparts actively exercised their wide-ranging common-law authority. See R. Younger, The People's Panel 47–55 (1963). Indeed, "the Founders thought the grand jury so essential ... that they provided in the Fifth Amendment that federal prosecution for serious crimes can only be instituted by 'a presentment or ***2250** indictment of a Grand Jury.' " *Calandra, supra,* at 343, 94 S.Ct. 613.

Given the popularity and prevalence of grand juries at the time, the Founders must have been intimately familiar with the tools they used—including compulsory process—to accomplish their work. As a matter of tradition, grand juries were "accorded wide latitude to inquire into violations of criminal law," including the power to "compel the production of evidence or the testimony of witnesses as [they] conside[r] appropriate." *Ibid.* Long before national independence was achieved, grand juries were already using their broad inquisitorial powers not only to present and indict criminal suspects but also to inspect public buildings, to levy taxes, to supervise the administration of the laws, to advance municipal reforms such as street repair and bridge maintenance, and in some cases even to propose legislation. Younger, *supra,* at 5–26. Of course, such work depended entirely on grand juries' ability to access any relevant documents.

Grand juries continued to exercise these broad inquisitorial powers up through the time of the founding. See *Blair v. United States,* 250 U.S. 273, 280, 39 S.Ct. 468, 63 L.Ed. 979 (1919) ("At the foundation of our Federal Government the inquisitorial function of the grand jury and the compulsion of witnesses were recognized as incidents of the judicial power"). In a series of lectures delivered in the early 1790's, Justice James Wilson crowed that grand juries were "the peculiar boast of the common law" thanks in part to their wide-ranging authority: "All the operations of government, and of its ministers and officers, are within the compass of their view and research." 2 J. Wilson, The Works of James Wilson 534, 537 (R. McCloskey ed. 1967). That reflected the broader insight that "[t]he grand jury's investigative power must be broad if its public responsibility is adequately to be discharged." *Calandra, supra,* at 344, 94 S.Ct. 613.

Compulsory process was also familiar to the founding generation in part because it reflected "the ancient proposition of law" that " ' "the public ... has a right to every man's evidence." ' " *United States v. Nixon,* 418 U.S. 683, 709, 94 S.Ct. 3090, 41 L.Ed.2d 1039 (1974); see also *ante,* at 2228 (KENNEDY, J., dissenting). As early as 1612, "Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.' " *Blair, supra,* at 279–280, 39 S.Ct. 468. That duty could be "onerous at times," yet the Founders considered it "necessary to the administration of justice according to the forms and modes established in our system of government." *Id.,* at 281, 39 S.Ct. 468; see also *Calandra, supra,* at 345, 94 S.Ct. 613.

B

Talk of kings and common-law writs may seem out of place in a case about cell-site records and the protections afforded by the Fourth Amendment in the modern age. But this history matters, not least because it tells us what was on the minds of those who ratified the Fourth Amendment and how they understood its scope. That history makes it abundantly clear that the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all.

The Fourth Amendment does not regulate all methods by which the Government obtains documents. Rather, it prohibits only those "searches and seizures" of "persons, houses, papers, and effects" that are "unreasonable." Consistent with that language, "at least until the latter half of the 20th century" "our Fourth Amendment jurisprudence was tied to common-law trespass." ***2251** *United States v. Jones,* 565 U.S. 400, 405, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). So by its terms, the Fourth Amendment does not apply to the compulsory production of documents, a practice that involves neither any physical intrusion into private space nor any taking of property by agents of the state. Even Justice Brandeis—a stalwart proponent of construing the Fourth Amendment liberally—acknowledged that "under any ordinary construction of language," "there is no 'search' or 'seizure' when a defendant is required to produce a document in the orderly process of a court's procedure." *Olmstead v. United States,* 277 U.S. 438, 476, 48 S.Ct. 564, 72 L.Ed. 944 (1928) (dissenting opinion). [1]

Nor is there any reason to believe that the Founders intended the Fourth Amendment to regulate courts' use of compulsory process. American colonists rebelled against the Crown's physical invasions of their persons and their property, not against its acquisition of information by any and all means. As Justice Black once put it, "[t]he Fourth Amendment was aimed directly at the abhorred practice of breaking in, ransacking and searching homes and other buildings and seizing people's personal belongings without warrants issued by magistrates." *Katz,* 389 U.S., at 367, 88 S.Ct. 507 (dissenting opinion). More recently, we have acknowledged that "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2494, 189 L.Ed.2d 430 (2014).

General warrants and writs of assistance were noxious not because they allowed the Government to acquire evidence in criminal investigations, but because of the *means* by which they permitted the Government to acquire that evidence. Then, as today, searches could be quite invasive. Searches generally begin with officers "mak[ing] nonconsensual entries into areas not open to the public." *Donovan v. Lone Steer, Inc.,* 464 U.S. 408, 414, 104 S.Ct. 769, 78 L.Ed.2d 567 (1984). Once there, officers are necessarily in a position to observe private spaces generally shielded from the public and discernible only with the owner's consent. Private area after private area becomes exposed to the officers' eyes as they rummage through the owner's property in their hunt for the object or objects of the search. If they are searching for documents, officers may additionally have to rifle through many other papers—potentially filled with the most intimate details of a person's thoughts and life—before they find the specific information ***2252** they are seeking. See *Andresen v. Maryland,* 427 U.S. 463, 482, n. 11, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976). If anything sufficiently incriminating comes into view, officers seize it. *Horton v. California,* 496 U.S. 128, 136–137, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990). Physical destruction always lurks as an underlying possibility; "officers executing search warrants on occasion must damage property in order to perform their duty." *Dalia v. United States,* 441 U.S. 238, 258, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979); see, *e.g.,* *United States v. Ramirez,* 523 U.S. 65, 71–72, 118 S.Ct. 992, 140 L.Ed.2d 191 (1998) (breaking garage window); *United States v. Ross,* 456 U.S. 798, 817–818, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982) (ripping open car upholstery); *Brown v. Battle Creek Police Dept.,* 844 F.3d 556, 572 (C.A.6 2016) (shooting and killing two pet dogs); *Lawmaster v. Ward,* 125 F.3d 1341, 1350, n. 3 (C.A.10 1997) (breaking locks).

Compliance with a subpoena *duces tecum* requires none of that. A subpoena *duces tecum* permits a subpoenaed individual to conduct the search for the relevant documents himself, without law enforcement officers entering his home or rooting through his papers and effects. As a result, subpoenas avoid the many incidental invasions of privacy that

necessarily accompany any actual search. And it was *those* invasions of privacy—which, although incidental, could often be extremely intrusive and damaging—that led to the adoption of the Fourth Amendment.

Neither this Court nor any of the parties have offered the slightest bit of historical evidence to support the idea that the Fourth Amendment originally applied to subpoenas *duces tecum* and other forms of compulsory process. That is telling, for as I have explained, these forms of compulsory process were a feature of criminal (and civil) procedure well known to the Founders. The Founders would thus have understood that holding the compulsory production of documents to the same standard as actual searches and seizures would cripple the work of courts in civil and criminal cases alike. It would be remarkable to think that, despite that knowledge, the Founders would have gone ahead and sought to impose such a requirement. It would be even more incredible to believe that the Founders would have imposed that requirement through the inapt vehicle of an amendment directed at different concerns. But it would blink reality entirely to argue that this entire process happened without anyone saying *the least thing about it*—not during the drafting of the Bill of Rights, not during any of the subsequent ratification debates, and not for most of the century that followed. If the Founders thought the Fourth Amendment applied to the compulsory production of documents, one would imagine that there would be *some* founding-era evidence of the Fourth Amendment being applied to the compulsory production of documents. Cf. *Free Enterprise Fund v. Public Company Accounting Oversight Bd.,* 561 U.S. 477, 505, 130 S.Ct. 3138, 177 L.Ed.2d 706 (2010); *Printz v. United States,* 521 U.S. 898, 905, 117 S.Ct. 2365, 138 L.Ed.2d 914 (1997). Yet none has been brought to our attention.

C

Of course, our jurisprudence has not stood still since 1791. We now evaluate subpoenas *duces tecum* and other forms of compulsory document production under the Fourth Amendment, although we employ a reasonableness standard that is less demanding than the requirements for a warrant. But the road to that doctrinal destination was anything but smooth, and our initial missteps—and the subsequent struggle to extricate ourselves from their consequences—should provide an object ***2253** lesson for today's majority about the dangers of holding compulsory process to the same standard as actual searches and seizures.

For almost a century after the Fourth Amendment was enacted, this Court said and did nothing to indicate that it might regulate the compulsory production of documents. But that changed temporarily when the Court decided *Boyd v. United States,* 116 U.S. 616, 6 S.Ct. 524, 29 L.Ed. 746 (1886), the first—and, until today, the only—case in which this Court has ever held the compulsory production of documents to the same standard as actual searches and seizures.

The *Boyd* Court held that a court order compelling a company to produce potentially incriminating business records violated both the Fourth and the Fifth Amendments. The Court acknowledged that "certain aggravating incidents of actual search and seizure, such as forcible entry into a man's house and searching amongst his papers, are wanting" when the Government relies on compulsory process. *Id.,* at 622, 6 S.Ct. 524. But it nevertheless asserted that the Fourth Amendment ought to "be liberally construed," *id.,* at 635, 6 S.Ct. 524, and further reasoned that compulsory process "effects the sole object and purpose of search and seizure" by "forcing from a party evidence against himself," *id.,* at 622, 6 S.Ct. 524. "In this regard," the Court concluded, "the Fourth and Fifth Amendments run almost into each other." *Id.,* at 630, 6 S.Ct. 524. Having equated compulsory process with actual searches and seizures and having melded the Fourth Amendment with the Fifth, the Court then found the order at issue unconstitutional because it compelled the production of property to which the Government did not have superior title. See *id.,* at 622–630, 6 S.Ct. 524.

In a concurrence joined by Chief Justice Waite, Justice Miller agreed that the order violated the Fifth Amendment, *id.,* at 639, 6 S.Ct. 524, but he strongly protested the majority's invocation of the Fourth Amendment. He explained: "[T]here is no reason why this court should assume that the action of the court below, in requiring a party to produce certain papers ..., authorizes an unreasonable search or seizure of the house, papers, or effects of that party. There is in fact no search and no seizure." *Ibid.* "If the mere service of a notice to produce a paper ... is a search," Justice Miller concluded, "then a change has taken place in the meaning of words, which has not come within my reading, and which I think was

unknown at the time the Constitution was made." *Id.,* at 641, 6 S.Ct. 524.

Although *Boyd* was replete with stirring rhetoric, its reasoning was confused from start to finish in a way that ultimately made the decision unworkable. See 3 W. LaFave, J. Israel, N. King, & O. Kerr, Criminal Procedure § 8.7(a) (4th ed. 2015). Over the next 50 years, the Court would gradually roll back *Boyd* 's erroneous conflation of compulsory process with actual searches and seizures.

That effort took its first significant stride in *Hale v. Henkel,* 201 U.S. 43, 26 S.Ct. 370, 50 L.Ed. 652 (1906), where the Court found it "quite clear" and "conclusive" that "the search and seizure clause of the Fourth Amendment was not intended to interfere with the power of courts to compel, through a *subpoena duces tecum,* the production, upon a trial in court, of documentary evidence." *Id.,* at 73, 26 S.Ct. 370. Without that writ, the Court recognized, "it would be 'utterly impossible to carry on the administration of justice.' " *Ibid.*

Hale, however, did not entirely liberate subpoenas *duces tecum* from Fourth ***2254** Amendment constraints. While refusing to treat such subpoenas as the equivalent of actual searches, *Hale* concluded that they must not be unreasonable. And it held that the subpoena *duces tecum* at issue was "far too sweeping in its terms to be regarded as reasonable." *Id.,* at 76, 26 S.Ct. 370. The *Hale* Court thus left two critical questions unanswered: Under the Fourth Amendment, what makes the compulsory production of documents "reasonable," and how does that standard differ from the one that governs actual searches and seizures?

The Court answered both of those questions definitively in *Oklahoma Press Publishing Co. v. Walling,* 327 U.S. 186, 66 S.Ct. 494, 90 L.Ed. 614 (1946), where we held that the Fourth Amendment regulates the compelled production of documents, but less stringently than it does full-blown searches and seizures. *Oklahoma Press* began by admitting that the Court's opinions on the subject had "perhaps too often ... been generative of heat rather than light," "mov[ing] with variant direction" and sometimes having "highly contrasting" "emphasis and tone." *Id.,* at 202, 66 S.Ct. 494. "The primary source of misconception concerning the Fourth Amendment's function" in this context, the Court explained, "lies perhaps in the identification of cases involving so-called 'figurative' or 'constructive' search with cases of actual search and seizure." *Ibid.* But the Court held that "the basic distinction" between the compulsory production of documents on the one hand, and actual searches and seizures on the other, meant that two different standards had to be applied. *Id.,* at 204, 66 S.Ct. 494.

Having reversed *Boyd* 's conflation of the compelled production of documents with actual searches and seizures, the Court then set forth the relevant Fourth Amendment standard for the former. When it comes to "the production of corporate or other business records," the Court held that the Fourth Amendment "at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant." *Oklahoma Press, supra,* at 208, 66 S.Ct. 494. Notably, the Court held that a showing of probable cause was not necessary so long as "the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry." *Id.,* at 209, 66 S.Ct. 494.

Since *Oklahoma Press,* we have consistently hewed to that standard. See, *e.g., Lone Steer, Inc.,* 464 U.S., at 414–415, 104 S.Ct. 769; *United States v. Miller,* 425 U.S. 435, 445–446, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976); *California Bankers Assn. v. Shultz,* 416 U.S. 21, 67, 94 S.Ct. 1494, 39 L.Ed.2d 812 (1974); *United States v. Dionisio,* 410 U.S. 1, 11–12, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973); *See v. Seattle,* 387 U.S. 541, 544, 87 S.Ct. 1737, 18 L.Ed.2d 943 (1967); *United States v. Powell,* 379 U.S. 48, 57–58, 85 S.Ct. 248, 13 L.Ed.2d 112 (1964); *McPhaul v. United States,* 364 U.S. 372, 382–383, 81 S.Ct. 138, 5 L.Ed.2d 136 (1960); *United States v. Morton Salt Co.,* 338 U.S. 632, 652–653, 70 S.Ct. 357, 94 L.Ed. 401 (1950); cf. *McLane Co. v. EEOC,* 581 U.S. ——, ——, 137 S.Ct. 1159, 1169–1170, 197 L.Ed.2d 500 (2017). By applying *Oklahoma Press* and thereby respecting "the traditional distinction between a search warrant and a subpoena," *Miller, supra,* at 446, 96 S.Ct. 1619, this Court has reinforced "the basic compromise" between "the public interest" in every man's evidence and the private interest "of men to be free from officious meddling." *Oklahoma Press, supra,* at 213, 66 S.Ct. 494.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

***2255** D

Today, however, the majority inexplicably ignores the settled rule of *Oklahoma Press* in favor of a resurrected version of *Boyd*. That is mystifying. This should have been an easy case regardless of whether the Court looked to the original understanding of the Fourth Amendment or to our modern doctrine.

As a matter of original understanding, the Fourth Amendment does not regulate the compelled production of documents at all. Here the Government received the relevant cell-site records pursuant to a court order compelling Carpenter's cell service provider to turn them over. That process is thus immune from challenge under the original understanding of the Fourth Amendment.

As a matter of modern doctrine, this case is equally straightforward. As Justice KENNEDY explains, no search or seizure of Carpenter or his property occurred in this case. *Ante,* at 2226 - 2235; see also Part II, *infra*. But even if the majority were right that the Government "searched" Carpenter, it would at most be a "figurative or constructive search" governed by the *Oklahoma Press* standard, not an "actual search" controlled by the Fourth Amendment's warrant requirement.

And there is no doubt that the Government met the *Oklahoma Press* standard here. Under *Oklahoma Press,* a court order must " 'be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.' " *Lone Steer, Inc., supra,* at 415, 104 S.Ct. 769. Here, the type of order obtained by the Government almost necessarily satisfies that standard. The Stored Communications Act allows a court to issue the relevant type of order "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that ... the records ... sough[t] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). And the court "may quash or modify such order" if the provider objects that the "records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." *Ibid.* No such objection was made in this case, and Carpenter does not suggest that the orders contravened the *Oklahoma Press* standard in any other way.

That is what makes the majority's opinion so puzzling. It decides that a "search" of Carpenter occurred within the meaning of the Fourth Amendment, but then it leaps straight to imposing requirements that—until this point—have governed only *actual* searches and seizures. See *ante,* at 2220 - 2221. Lost in its race to the finish is any real recognition of the century's worth of precedent it jeopardizes. For the majority, this case is apparently no different from one in which Government agents raided Carpenter's home and removed records associated with his cell phone.

Against centuries of precedent and practice, all that the Court can muster is the observation that "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." *Ante,* at 2221. Frankly, I cannot imagine a concession more damning to the Court's argument than that. As the Court well knows, the reason that we have never seen such a case is because—until today—defendants categorically had no "reasonable expectation of privacy" and no property interest in records belonging to third parties. See Part II, *infra*. By implying otherwise, the Court tries the nice trick of seeking shelter under the cover of precedents that it simultaneously perforates.

***2256** Not only that, but even if the Fourth Amendment permitted someone to object to the subpoena of a third party's records, the Court cannot explain why that individual should be entitled to *greater* Fourth Amendment protection than the party actually being subpoenaed. When parties are subpoenaed to turn over their records, after all, they will at most receive the protection afforded by *Oklahoma Press* even though they will own and have a reasonable expectation of privacy in the records at issue. Under the Court's decision, however, the Fourth Amendment will extend greater protections to someone else who is not being subpoenaed and does not own the records. That outcome makes no sense, and the Court does not even attempt to defend it.

We have set forth the relevant Fourth Amendment standard for subpoenaing business records many times over. Out of those dozens of cases, the majority cannot find even one that so much as suggests an exception to the *Oklahoma Press* standard for sufficiently personal information. Instead, we have always "described the constitutional requirements" for compulsory process as being " 'settled' " and as applying categorically to all " 'subpoenas [of] corporate books or

records.' " *Lone Steer, Inc.,* 464 U.S., at 415, 104 S.Ct. 769 (internal quotation marks omitted). That standard, we have held, is "*the most* " protection the Fourth Amendment gives "to the production of corporate records and papers." *Oklahoma Press,* 327 U.S., at 208, 66 S.Ct. 494 (emphasis added). [2]

Although the majority announces its holding in the context of the Stored Communications Act, nothing stops its logic from sweeping much further. The Court has offered no meaningful limiting principle, and none is apparent. Cf. Tr. of Oral Arg. 31 (Carpenter's counsel admitting that "a grand jury subpoena ... would be held to the same standard as any other subpoena or subpoena-like request for [cell-site] records").

Holding that subpoenas must meet the same standard as conventional searches will seriously damage, if not destroy, their utility. Even more so than at the founding, today the Government regularly uses subpoenas *duces tecum* and other forms of compulsory process to carry out its essential functions. See, *e.g., Dionisio,* 410 U.S., at 11–12, 93 S.Ct. 764 (grand jury subpoenas); *McPhaul,* 364 U.S., at 382–383, 81 S.Ct. 138 (legislative subpoenas); *Oklahoma Press, supra,* at 208–209, 66 S.Ct. 494 (administrative subpoenas). Grand juries, for example, have long "compel[led] the production of evidence" in order to determine "*whether* there is probable cause to believe a crime has been committed." *Calandra,* 414 U.S., at 343, 94 S.Ct. 613 (emphasis added). Almost by definition, then, grand juries will be unable at first to demonstrate "the probable cause required for a warrant." *Ante,* at 2221 (majority opinion); see also *Oklahoma Press, supra,* at 213, 66 S.Ct. 494. If they are required to do so, the effects are as predictable as they are alarming: Many investigations will sputter out at the start, and a host of criminals will be able to evade law enforcement's reach.

"To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence." *Nixon,* 418 U.S., at 709, 94 S.Ct. 3090. For over a hundred years, we have understood that holding ***2257** subpoenas to the same standard as actual searches and seizures "would stop much if not all of investigation in the public interest at the threshold of inquiry." *Oklahoma Press, supra,* at 213, 66 S.Ct. 494. Today a skeptical majority decides to put that understanding to the test.

II

Compounding its initial error, the Court also holds that a defendant has the right under the Fourth Amendment to object to the search of a third party's property. This holding flouts the clear text of the Fourth Amendment, and it cannot be defended under either a property-based interpretation of that Amendment or our decisions applying the reasonable-expectations-of-privacy test adopted in *Katz,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576. By allowing Carpenter to object to the search of a third party's property, the Court threatens to revolutionize a second and independent line of Fourth Amendment doctrine.

A

It bears repeating that the Fourth Amendment guarantees "[t]he right of the people to be secure in *their* persons, houses, papers, and effects." (Emphasis added.) The Fourth Amendment does not confer rights with respect to the persons, houses, papers, and effects of others. Its language makes clear that "Fourth Amendment rights are personal," *Rakas v. Illinois,* 439 U.S. 128, 140, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978), and as a result, this Court has long insisted that they "may not be asserted vicariously," *id.,* at 133, 99 S.Ct. 421. It follows that a "person who is aggrieved ... only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed." *Id.,* at 134, 99 S.Ct. 421.

In this case, as Justice KENNEDY cogently explains, the cell-site records obtained by the Government belong to Carpenter's cell service providers, not to Carpenter. See *ante,* at 2229 - 2230. Carpenter did not create the cell-site records. Nor did he have possession of them; at all relevant times, they were kept by the providers. Once Carpenter subscribed to his provider's service, he had no right to prevent the company from creating or keeping the information in its records. Carpenter also had no right to demand that the providers destroy the records, no right to prevent the providers from destroying the records, and, indeed, no right to modify the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

records in any way whatsoever (or to prevent the providers from modifying the records). Carpenter, in short, has no meaningful control over the cell-site records, which are created, maintained, altered, used, and eventually destroyed by his cell service providers.

Carpenter responds by pointing to a provision of the Telecommunications Act that requires a provider to disclose cell-site records when a customer so requests. See 47 U.S.C. § 222(c)(2). But a statutory disclosure requirement is hardly sufficient to give someone an ownership interest in the documents that must be copied and disclosed. Many statutes confer a right to obtain copies of documents without creating any property right. [3]

***2258** Carpenter's argument is particularly hard to swallow because nothing in the Telecommunications Act precludes cell service providers from charging customers a fee for accessing cell-site records. See *ante,* at 2229 - 2230 (KENNEDY, J., dissenting). It would be very strange if the owner of records were required to pay in order to inspect his own property.

Nor does the Telecommunications Act give Carpenter a property right in the cell-site records simply because they are subject to confidentiality restrictions. See 47 U.S.C. § 222(c)(1) (without a customer's permission, a cell service provider may generally "use, disclose, or permit access to individually identifiable [cell-site records]" only with respect to "its provision" of telecommunications services). Many federal statutes impose similar restrictions on private entities' use or dissemination of information in their own records without conferring a property right on third parties. [4]

***2259** It would be especially strange to hold that the Telecommunication Act's confidentiality provision confers a property right when the Act creates an express exception for any disclosure of records that is "required by law." 47 U.S.C. § 222(c)(1). So not only does Carpenter lack " 'the most essential and beneficial' " of the " 'constituent elements' " of property, *Dickman v. Commissioner,* 465 U.S. 330, 336, 104 S.Ct. 1086, 79 L.Ed.2d 343 (1984)—*i.e.,* the right to use the property to the exclusion of others—but he cannot even exclude the party he would most like to keep out, namely, the Government. [5]

For all these reasons, there is no plausible ground for maintaining that the information at issue here represents Carpenter's "papers" or "effects." [6]

B

In the days when this Court followed an exclusively property-based approach to the Fourth Amendment, the distinction between an individual's Fourth Amendment rights and those of a third party was clear cut. We first asked whether the object of the search—say, a house, papers, or effects—belonged to the defendant, and, if it did, whether the Government had committed a "trespass" in acquiring the evidence at issue. *Jones,* 565 U.S., at 411, n. 8, 132 S.Ct. 945.

When the Court held in *Katz* that "property rights are not the sole measure of Fourth Amendment violations," *Soldal v. Cook County,* 506 U.S. 56, 64, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992), the sharp boundary between personal and third-party rights was tested. Under *Katz,* a party may invoke the Fourth Amendment whenever law enforcement officers violate the party's "justifiable" or "reasonable" expectation of privacy. See 389 U.S., at 353, 88 S.Ct. 507; see also *id.,* at 361, 88 S.Ct. 507 (Harlan, J., concurring) (applying the Fourth Amendment where "a person [has] exhibited an actual (subjective) expectation of privacy" and where that "expectation [is] one that society is prepared to recognize as 'reasonable' "). Thus freed from ***2260** the limitations imposed by property law, parties began to argue that they had a reasonable expectation of privacy in items owned by others. After all, if a trusted third party took care not to disclose information about the person in question, that person might well have a reasonable expectation that the information would not be revealed.

Efforts to claim Fourth Amendment protection against searches of the papers and effects of others came to a head in *Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71, where the defendant sought the suppression of two banks' microfilm copies of his checks, deposit slips, and other records. The defendant did not claim that he owned these documents, but he nonetheless argued that "analysis of ownership, property rights and possessory interests in the determination of Fourth Amendment rights ha[d] been severely impeached" by *Katz* and other recent cases. See Brief for Respondent in *United States v. Miller,* O.T.1975, No. 74–1179, p. 6. Turning to

Katz, he then argued that he had a reasonable expectation of privacy in the banks' records regarding his accounts. Brief for Respondent in No. 74–1179, at 6; see also *Miller, supra,* at 442–443, 96 S.Ct. 1619.

Acceptance of this argument would have flown in the face of the Fourth Amendment's text, and the Court rejected that development. Because Miller gave up "dominion and control" of the relevant information to his bank, *Rakas,* 439 U.S., at 149, 99 S.Ct. 421, the Court ruled that he lost any protected Fourth Amendment interest in that information. See *Miller, supra,* at 442–443, 96 S.Ct. 1619. Later, in *Smith v. Maryland,* 442 U.S. 735, 745, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), the Court reached a similar conclusion regarding a telephone company's records of a customer's calls. As Justice KENNEDY concludes, *Miller* and *Smith* are thus best understood as placing "necessary limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a 'requisite connection.' " *Ante,* at 2227.

The same is true here, where Carpenter indisputably lacks any meaningful property-based connection to the cell-site records owned by his provider. Because the records are not Carpenter's in any sense, Carpenter may not seek to use the Fourth Amendment to exclude them.

By holding otherwise, the Court effectively allows Carpenter to object to the "search" of a third party's property, not recognizing the revolutionary nature of this change. The Court seems to think that *Miller* and *Smith* invented a new "doctrine"—"the third-party doctrine"—and the Court refuses to "extend" this product of the 1970's to a new age of digital communications. *Ante,* at 2216 - 2217, 2220. But the Court fundamentally misunderstands the role of *Miller* and *Smith*. Those decisions did not forge a new doctrine; instead, they rejected an argument that would have disregarded the clear text of the Fourth Amendment and a formidable body of precedent.

In the end, the Court never explains how its decision can be squared with the fact that the Fourth Amendment protects only "[t]he right of the people to be secure in *their* persons, houses, papers, and effects." (Emphasis added.)

* * *

Although the majority professes a desire not to " 'embarrass the future,' " *ante,* at 2220, we can guess where today's decision will lead.

One possibility is that the broad principles that the Court seems to embrace will be applied across the board. All subpoenas *duces tecum* and all other orders compelling ***2261** the production of documents will require a demonstration of probable cause, and individuals will be able to claim a protected Fourth Amendment interest in any sensitive personal information about them that is collected and owned by third parties. Those would be revolutionary developments indeed.

The other possibility is that this Court will face the embarrassment of explaining in case after case that the principles on which today's decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered. If we take this latter course, we will inevitably end up "mak[ing] a crazy quilt of the Fourth Amendment." *Smith, supra,* at 745, 99 S.Ct. 2577.

All of this is unnecessary. In the Stored Communications Act, Congress addressed the specific problem at issue in this case. The Act restricts the misuse of cell-site records by cell service providers, something that the Fourth Amendment cannot do. The Act also goes beyond current Fourth Amendment case law in restricting access by law enforcement. It permits law enforcement officers to acquire cell-site records only if they meet a heightened standard and obtain a court order. If the American people now think that the Act is inadequate or needs updating, they can turn to their elected representatives to adopt more protective provisions. Because the collection and storage of cell-site records affects nearly every American, it is unlikely that the question whether the current law requires strengthening will escape Congress's notice.

Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope. The Fourth Amendment restricts the conduct of the Federal Government and the States; it does not apply to private actors. But today, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans. If today's decision encourages the public to think that this Court can protect them from this looming threat to

their privacy, the decision will mislead as well as disrupt. And if holding a provision of the Stored Communications Act to be unconstitutional dissuades Congress from further legislation in this field, the goal of protecting privacy will be greatly disserved.

The desire to make a statement about privacy in the digital age does not justify the consequences that today's decision is likely to produce.

Justice GORSUCH, dissenting.

In the late 1960s this Court suggested for the first time that a search triggering the Fourth Amendment occurs when the government violates an "expectation of privacy" that "society is prepared to recognize as 'reasonable.' " *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). Then, in a pair of decisions in the 1970s applying the *Katz* test, the Court held that a "reasonable expectation of privacy" *doesn't* attach to information shared with "third parties." See *Smith v. Maryland,* 442 U.S. 735, 743–744, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). By these steps, the Court came to conclude, the Constitution does nothing to limit investigators from searching records you've entrusted to your bank, accountant, and maybe even your doctor.

***2262** What's left of the Fourth Amendment? Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, *for* us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.

What to do? It seems to me we could respond in at least three ways. The first is to ignore the problem, maintain *Smith* and *Miller,* and live with the consequences. If the confluence of these decisions and modern technology means our Fourth Amendment rights are reduced to nearly nothing, so be it. The second choice is to set *Smith* and *Miller* aside and try again using the *Katz* "reasonable expectation of privacy" jurisprudence that produced them. The third is to look for answers elsewhere.

*

Start with the first option. *Smith* held that the government's use of a pen register to record the numbers people dial on their phones doesn't infringe a reasonable expectation of privacy because that information is freely disclosed to the third party phone company. 442 U.S., at 743–744, 99 S.Ct. 2577. *Miller* held that a bank account holder enjoys no reasonable expectation of privacy in the bank's records of his account activity. That's true, the Court reasoned, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 425 U.S., at 443, 96 S.Ct. 1619. Today the Court suggests that *Smith* and *Miller* distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to "extend" those decisions to particular classes of information, depending on their sensitivity. See *ante,* at 2216 - 2221. But as the Sixth Circuit recognized and Justice KENNEDY explains, no balancing test of this kind can be found in *Smith* and *Miller*. See *ante,* at 2231 - 2232 (dissenting opinion). Those cases announced a categorical rule: Once you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have had in it. And even if *Smith* and *Miller* did permit courts to conduct a balancing contest of the kind the Court now suggests, it's still hard to see how that would help the petitioner in this case. Why is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know and the Court does not say.

The problem isn't with the Sixth Circuit's application of *Smith* and *Miller* but with the cases themselves. Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can —at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely. In the years since its adoption, countless scholars, too, have come to conclude that the "third-party doctrine is not only wrong, but horribly wrong." Kerr, The Case for the Third–Party Doctrine, 107 Mich. L. Rev. 561, 563, n. 5, 564 (2009) (collecting criticisms but defending the

doctrine (footnotes omitted)). The reasons are obvious. "As an empirical statement about subjective ***2263** expectations of privacy," the doctrine is "quite dubious." Baude & Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1872 (2016). People often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private. Meanwhile, if the third party doctrine is supposed to represent a normative assessment of when a person should expect privacy, the notion that the answer might be "never" seems a pretty unattractive societal prescription. *Ibid.*

What, then, is the explanation for our third party doctrine? The truth is, the Court has never offered a persuasive justification. The Court has said that by conveying information to a third party you " 'assum[e] the risk' " it will be revealed to the police and therefore lack a reasonable expectation of privacy in it. *Smith, supra,* at 744, 99 S.Ct. 2577. But assumption of risk doctrine developed in tort law. It generally applies when "by contract or otherwise [one] expressly agrees to accept a risk of harm" or impliedly does so by "manifest[ing] his willingness to accept" that risk and thereby "take[s] his chances as to harm which may result from it." Restatement (Second) of Torts §§ 496B, 496C(1), and Comment *b* (1965); see also 1 D. Dobbs, P. Hayden, & E. Bublick, Law of Torts §§ 235–236, pp. 841–850 (2d ed. 2017). That rationale has little play in this context. Suppose I entrust a friend with a letter and he promises to keep it secret until he delivers it to an intended recipient. In what sense have I agreed to bear the risk that he will turn around, break his promise, and spill its contents to someone else? More confusing still, what have I done to "manifest my willingness to accept" the risk that the government will pry the document from my friend and read it *without* his consent?

One possible answer concerns knowledge. I know that my friend *might* break his promise, or that the government *might* have some reason to search the papers in his possession. But knowing about a risk doesn't mean you assume responsibility for it. Whenever you walk down the sidewalk you know a car may negligently or recklessly veer off and hit you, but that hardly means you accept the consequences and absolve the driver of any damage he may do to you. Epstein, Privacy and the Third Hand: Lessons From the Common Law of Reasonable Expectations, 24 Berkeley Tech. L.J. 1199, 1204 (2009); see W. Keeton, D. Dobbs, R. Keeton, & D. Owen, Prosser & Keeton on Law of Torts 490 (5th ed.1984).

Some have suggested the third party doctrine is better understood to rest on consent than assumption of risk. "So long as a person knows that they are disclosing information to a third party," the argument goes, "their choice to do so is voluntary and the consent valid." Kerr, *supra,* at 588. I confess I still don't see it. Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government.* Perhaps there are exceptions, like when the third party is an undercover government agent. See Murphy, The Case Against the Case Against the Third–Party Doctrine: A Response to Epstein and Kerr, 24 Berkeley Tech. L.J. 1239, 1252 (2009); cf. *Hoffa v. United States,* 385 U.S. 293, 87 S.Ct. 408, 17 L.Ed.2d 374 (1966). But otherwise this conception of consent appears to be just assumption of risk relabeled—you've "consented" to whatever risks are foreseeable.

Another justification sometimes offered for third party doctrine is clarity. You (and the police) know exactly how much protection you have in information confided ***2264** to others: none. As rules go, "the king always wins" is admirably clear. But the opposite rule would be clear too: Third party disclosures *never* diminish Fourth Amendment protection (call it "the king always loses"). So clarity alone cannot justify the third party doctrine.

In the end, what do *Smith* and *Miller* add up to? A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants. The Sixth Circuit had to follow that rule and faithfully did just that, but it's not clear why we should.

*

There's a second option. What if we dropped *Smith* and *Miller* 's third party doctrine and retreated to the root *Katz* question whether there is a "reasonable expectation of privacy" in data held by third parties? Rather than solve the problem with the third party doctrine, I worry this option only risks returning us to its source: After all, it was *Katz* that produced *Smith* and *Miller* in the first place.

Katz's problems start with the text and original understanding of the Fourth Amendment, as Justice THOMAS thoughtfully explains today. *Ante,* at 2237 - 2244 (dissenting opinion). The Amendment's protections do not depend on the breach of some abstract "expectation of privacy" whose contours are left to the judicial imagination. Much more concretely,

it protects your "person," and your "houses, papers, and effects." Nor does your right to bring a Fourth Amendment claim depend on whether a judge happens to agree that your subjective expectation to privacy is a "reasonable" one. Under its plain terms, the Amendment grants you the right to invoke its guarantees whenever one of your protected things (your person, your house, your papers, or your effects) is unreasonably searched or seized. Period.

History too holds problems for *Katz*. Little like it can be found in the law that led to the adoption of the Fourth Amendment or in this Court's jurisprudence until the late 1960s. The Fourth Amendment came about in response to a trio of 18th century cases "well known to the men who wrote and ratified the Bill of Rights, [and] famous throughout the colonial population." Stuntz, The Substantive Origins of Criminal Procedure, 105 Yale L.J. 393, 397 (1995). The first two were English cases invalidating the Crown's use of general warrants to enter homes and search papers. *Entick v. Carrington,* 19 How. St. Tr. 1029 (K.B. 1765); *Wilkes v. Wood,* 19 How. St. Tr. 1153 (K.B. 1763); see W. Cuddihy, The Fourth Amendment: Origins and Original Meaning 439–487 (2009); *Boyd v. United States,* 116 U.S. 616, 625–630, 6 S.Ct. 524, 29 L.Ed. 746 (1886). The third was American: the Boston Writs of Assistance Case, which sparked colonial outrage at the use of writs permitting government agents to enter houses and business, breaking open doors and chests along the way, to conduct searches and seizures—and to force third parties to help them. Stuntz, *supra,* at 404–409; M. Smith, The Writs of Assistance Case (1978). No doubt the colonial outrage engendered by these cases rested in part on the government's intrusion upon privacy. But the framers chose not to protect privacy in some ethereal way dependent on judicial intuitions. They chose instead to protect privacy in particular places and things—"persons, houses, papers, and effects"—and against particular threats—"unreasonable" governmental "searches and seizures." See *Entick, supra,* at 1066 ("Papers are the owner's goods and chattels; they are his dearest property; and so far from enduring a seizure, that they will hardly bear an inspection"); see also *ante,* at 2235 - 2246 (THOMAS, J., dissenting).

***2265** Even taken on its own terms, *Katz* has never been sufficiently justified. In fact, we still don't even know what its "reasonable expectation of privacy" test *is*. Is it supposed to pose an empirical question (what privacy expectations do people *actually* have) or a normative one (what expectations *should* they have)? Either way brings problems. If the test is supposed to be an empirical one, it's unclear why judges rather than legislators should conduct it. Legislators are responsive to their constituents and have institutional resources designed to help them discern and enact majoritarian preferences. Politically insulated judges come armed with only the attorneys' briefs, a few law clerks, and their own idiosyncratic experiences. They are hardly the representative group you'd expect (or want) to be making empirical judgments for hundreds of millions of people. Unsurprisingly, too, judicial judgments often fail to reflect public views. See Slobogin & Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society," 42 Duke L.J. 727, 732, 740–742 (1993). Consider just one example. Our cases insist that the seriousness of the offense being investigated does *not* reduce Fourth Amendment protection. *Mincey v. Arizona,* 437 U.S. 385, 393–394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978). Yet scholars suggest that most people *are* more tolerant of police intrusions when they investigate more serious crimes. See Blumenthal, Adya, & Mogle, The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy," 11 U. Pa. J. Const. L. 331, 352–353 (2009). And I very much doubt that this Court would be willing to adjust its *Katz* cases to reflect these findings even if it believed them.

Maybe, then, the *Katz* test should be conceived as a normative question. But if that's the case, why (again) do judges, rather than legislators, get to determine whether society *should be* prepared to recognize an expectation of privacy as legitimate? Deciding what privacy interests *should be* recognized often calls for a pure policy choice, many times between incommensurable goods—between the value of privacy in a particular setting and society's interest in combating crime. Answering questions like that calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts. See The Federalist No. 78, p. 465 (C. Rossiter ed. 1961) (A. Hamilton). When judges abandon legal judgment for political will we not only risk decisions where "reasonable expectations of privacy" come to bear "an uncanny resemblance to those expectations of privacy" shared by Members of this Court. *Minnesota v. Carter,* 525 U.S. 83, 97, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (Scalia, J., concurring). We also risk undermining public confidence in the courts themselves.

My concerns about *Katz* come with a caveat. *Sometimes,* I accept, judges may be able to discern and describe existing societal norms. See, *e.g., Florida v. Jardines,* 569 U.S.

1, 8, 133 S.Ct. 1409, 185 L.Ed.2d 495 (2013) (inferring a license to enter on private property from the " 'habits of the country' " (quoting *McKee v. Gratz,* 260 U.S. 127, 136, 43 S.Ct. 16, 67 L.Ed. 167 (1922))); Sachs, Finding Law, 107 Cal. L. Rev. (forthcoming 2019), online at https://ssrn.com/abstract=3064443 (as last visited June 19, 2018). That is particularly true when the judge looks to positive law rather than intuition for guidance on social norms. See *Byrd v. United States,* 584 U.S. ——, —— – ——, 138 S.Ct. 1518, 1527, —— L.Ed.2d —— (2018) ("general property-based concept[s] guid[e] the resolution of this case"). So there may be *some* occasions where *Katz* is capable of principled application— ***2266** though it may simply wind up approximating the more traditional option I will discuss in a moment. Sometimes it may also be possible to apply *Katz* by analogizing from precedent when the line between an existing case and a new fact pattern is short and direct. But so far this Court has declined to tie itself to any significant restraints like these. See *ante,* at 2214, n. 1 ("[W]hile property rights are often informative, our cases by no means suggest that such an interest is 'fundamental' or 'dispositive' in determining which expectations of privacy are legitimate").

As a result, *Katz* has yielded an often unpredictable—and sometimes unbelievable—jurisprudence. *Smith* and *Miller* are only two examples; there are many others. Take *Florida v. Riley,* 488 U.S. 445, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989), which says that a police helicopter hovering 400 feet above a person's property invades no reasonable expectation of privacy. Try that one out on your neighbors. Or *California v. Greenwood,* 486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988), which holds that a person has no reasonable expectation of privacy in the garbage he puts out for collection. In that case, the Court said that the homeowners forfeited their privacy interests because "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public." *Id.,* at 40, 108 S.Ct. 1625 (footnotes omitted). But the habits of raccoons don't prove much about the habits of the country. I doubt, too, that most people spotting a neighbor rummaging through their garbage would think they lacked reasonable grounds to confront the rummager. Making the decision all the stranger, California state law expressly *protected* a homeowner's property rights in discarded trash. *Id.,* at 43, 108 S.Ct. 1625. Yet rather than defer to that as evidence of the people's habits and reasonable expectations of privacy, the Court substituted its own curious judgment.

Resorting to *Katz* in data privacy cases threatens more of the same. Just consider. The Court today says that judges should use *Katz* 's reasonable expectation of privacy test to decide what Fourth Amendment rights people have in cell-site location information, explaining that "no single rubric definitively resolves which expectations of privacy are entitled to protection." *Ante,* at 2213 - 2214. But then it offers a twist. Lower courts should be sure to add two special principles to their *Katz* calculus: the need to avoid "arbitrary power" and the importance of "plac[ing] obstacles in the way of a too permeating police surveillance." *Ante,* at 2214 (internal quotation marks omitted). While surely laudable, these principles don't offer lower courts much guidance. The Court does not tell us, for example, how far to carry either principle or how to weigh them against the legitimate needs of law enforcement. At what point does access to electronic data amount to "arbitrary" authority? When does police surveillance become "too permeating"? And what sort of "obstacles" should judges "place" in law enforcement's path when it does? We simply do not know.

The Court's application of these principles supplies little more direction. The Court declines to say whether there is any sufficiently limited period of time "for which the Government may obtain an individual's historical [location information] free from Fourth Amendment scrutiny." *Ante,* at 2217, n. 3; see *ante,* at 2216 - 2219. But then it tells us that access to seven days' worth of information *does* trigger Fourth Amendment scrutiny—even though here the carrier "produced only two days of records." *Ante,* at 2217, n. 3. Why is the relevant fact the seven days of ***2267** information the government *asked for* instead of the two days of information the government *actually saw* ? Why seven days instead of ten or three or one? And in what possible sense did the government "search" five days' worth of location information it was never even sent? We do not know.

Later still, the Court adds that it can't say whether the Fourth Amendment is triggered when the government collects "real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)." *Ante,* at 2220. But what distinguishes historical data from real-time data, or seven days of a single person's data from a download of *everyone* 's data over some indefinite period of time? Why isn't a tower dump the *paradigmatic* example of "too permeating

police surveillance" and a dangerous tool of "arbitrary" authority—the touchstones of the majority's modified *Katz* analysis? On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not? Here again we are left to guess. At the same time, though, the Court offers some firm assurances. It tells us its decision does *not* "call into question conventional surveillance techniques and tools, such as security cameras." *Ibid.* That, however, just raises more questions for lower courts to sort out about what techniques qualify as "conventional" and why those techniques would be okay *even if* they lead to "permeating police surveillance" or "arbitrary police power."

Nor is this the end of it. After finding a reasonable expectation of privacy, the Court says there's still more work to do. Courts must determine whether to "extend" *Smith* and *Miller* to the circumstances before them. *Ante,* at 2216, 2219 - 2220. So apparently *Smith* and *Miller* aren't quite left for dead; they just no longer have the clear reach they once did. How do we measure their new reach? The Court says courts now must conduct a *second Katz*-like balancing inquiry, asking whether the fact of disclosure to a third party outweighs privacy interests in the "category of information" so disclosed. *Ante,* at 2218, 2219 - 2220. But how are lower courts supposed to weigh these radically different interests? Or assign values to different categories of information? All we know is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller* 's shorn grasp, while a lifetime of bank or phone records does not. As to any other kind of information, lower courts will have to stay tuned.

In the end, our lower court colleagues are left with two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition. In the Court's defense, though, we have arrived at this strange place not because the Court has misunderstood *Katz*. Far from it. We have arrived here because this is where *Katz* inevitably leads.

*

There is another way. From the founding until the 1960s, the right to assert a Fourth Amendment claim didn't depend on your ability to appeal to a judge's personal sensibilities about the "reasonableness" of your expectations or privacy. It was tied to the law. *Jardines,* 569 U.S., at 11, 133 S.Ct. 1409; *United States v. Jones,* 565 U.S. 400, 405, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." True to those words and their original understanding, the traditional approach ***2268** asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment. Though now often lost in *Katz* 's shadow, this traditional understanding persists. *Katz* only "supplements, rather than displaces the traditional property-based understanding of the Fourth Amendment." *Byrd,* 584 U.S., at ——, 138 S.Ct., at 1526 (internal quotation marks omitted); *Jardines, supra,* at 11, 133 S.Ct. 1409 (same); *Soldal v. Cook County,* 506 U.S. 56, 64, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992) (*Katz* did not "snuf[f] out the previously recognized protection for property under the Fourth Amendment").

Beyond its provenance in the text and original understanding of the Amendment, this traditional approach comes with other advantages. Judges are supposed to decide cases based on "democratically legitimate sources of law"—like positive law or analogies to items protected by the enacted Constitution—rather than "their own biases or personal policy preferences." Pettys, Judicial Discretion in Constitutional Cases, 26 J.L. & Pol. 123, 127 (2011). A Fourth Amendment model based on positive legal rights "carves out significant room for legislative participation in the Fourth Amendment context," too, by asking judges to consult what the people's representatives have to say about their rights. Baude & Stern, 129 Harv. L. Rev., at 1852. Nor is this approach hobbled by *Smith* and *Miller,* for those cases are just *limitations* on *Katz,* addressing only the question whether individuals have a reasonable expectation of privacy in materials they share with third parties. Under this more traditional approach, Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties.

Given the prominence *Katz* has claimed in our doctrine, American courts are pretty rusty at applying the traditional approach to the Fourth Amendment. We know that if a house, paper, or effect is yours, you have a Fourth Amendment interest in its protection. But what kind of legal interest is sufficient to make something *yours* ? And what source of law determines that? Current positive law? The common law at 1791, extended by analogy to modern times? Both?

See *Byrd, supra,* at —— – ——, 138 S.Ct., at 1531 (THOMAS, J., concurring); cf. Re, The Positive Law Floor, 129 Harv. L. Rev. Forum 313 (2016). Much work is needed to revitalize this area and answer these questions. I do not begin to claim all the answers today, but (unlike with *Katz*) at least I have a pretty good idea what the questions *are*. And it seems to me a few things can be said.

First, the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them. Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a *bailment*. A bailment is the "delivery of personal property by one person (the *bailor*) to another (the *bailee*) who holds the property for a certain purpose." Black's Law Dictionary 169 (10th ed. 2014); J. Story, Commentaries on the Law of Bailments § 2, p. 2 (1832) ("a bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust"). A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the "implication[s] from their ***2269** conduct" if they don't. 8 C.J. S., Bailments § 36, pp. 468–469 (2017). A bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion. *Id.,* § 43, at 481; see *Goad v. Harris,* 207 Ala. 357, 92 So. 546 (1922); *Knight v. Seney,* 290 Ill. 11, 17, 124 N.E. 813, 815–816 (1919); *Baxter v. Woodward,* 191 Mich. 379, 385, 158 N.W. 137, 139 (1916). This approach is quite different from *Smith* and *Miller* 's (counter)-intuitive approach to reasonable expectations of privacy; where those cases extinguish Fourth Amendment interests once records are given to a third party, property law may preserve them.

Our Fourth Amendment jurisprudence already reflects this truth. In *Ex parte Jackson,* 96 U.S. 727, 24 L.Ed. 877 (1878), this Court held that sealed letters placed in the mail are "as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." *Id.,* at 733. The reason, drawn from the Fourth Amendment's text, was that "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to *their papers,* thus closed against inspection, *wherever they may be*." *Ibid.* (emphasis added). It did not matter that letters were bailed to a third party (the government, no less). The sender enjoyed the same Fourth Amendment protection as he does "when papers are subjected to search in one's own household." *Ibid.*

These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents. Whatever may be left of *Smith* and *Miller,* few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest. See *ante,* at 2230 (KENNEDY, J., dissenting) (noting that enhanced Fourth Amendment protection may apply when the "modern-day equivalents of an individual's own 'papers' or 'effects' ... are held by a third party" through "bailment"); *ante,* at 2259, n. 6 (ALITO, J., dissenting) (reserving the question whether Fourth Amendment protection may apply in the case of "bailment" or when "someone has entrusted papers he or she owns ... to the safekeeping of another"); *United States v. Warshak,* 631 F.3d 266, 285–286 (C.A.6 2010) (relying on an analogy to *Jackson* to extend Fourth Amendment protection to e-mail held by a third party service provider).

Second, I doubt that complete ownership or exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right. Where houses are concerned, for example, individuals can enjoy Fourth Amendment protection without fee simple title. Both the text of the Amendment and the common law rule support that conclusion. "People call a house 'their' home when legal title is in the bank, when they rent it, and even when they merely occupy it rent free." *Carter,* 525 U.S., at 95–96, 119 S.Ct. 469 (Scalia, J., concurring). That rule derives from the common law. *Oystead v. Shed,* 13 Mass. 520, 523 (1816) (explaining, citing "[t]he very learned judges, *Foster, Hale,* and *Coke,*" that the law "would be as much disturbed by a forcible entry to arrest a boarder or a servant, who had acquired, by contract, express or implied, a right to enter the house at all times, and to remain in it as long as they please, as if the object were to arrest the master of the house or his children"). That is why tenants and resident family members—though they have no legal title—have standing to complain ***2270** about searches of the houses in which they live. *Chapman v. United States,* 365 U.S. 610, 616–

617, 81 S.Ct. 776, 5 L.Ed.2d 828 (1961), *Bumper v. North Carolina,* 391 U.S. 543, 548, n. 11, 88 S.Ct. 1788, 20 L.Ed.2d 797 (1968).

Another point seems equally true: just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it. Not infrequently one person comes into possession of someone else's property without the owner's consent. Think of the finder of lost goods or the policeman who impounds a car. The law recognizes that the goods and the car still belong to their true owners, for "where a person comes into lawful possession of the personal property of another, even though there is no formal agreement between the property's owner and its possessor, the possessor will become a constructive bailee when justice so requires." *Christensen v. Hoover,* 643 P.2d 525, 529 (Colo.1982) (en banc); Laidlaw, Principles of Bailment, 16 Cornell L.Q. 286 (1931). At least some of this Court's decisions have already suggested that use of technology is functionally compelled by the demands of modern life, and in that way the fact that we store data with third parties may amount to a sort of involuntary bailment too. See *ante,* at 2217 - 2218 (majority opinion); *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2484, 189 L.Ed.2d 430 (2014).

Third, positive law may help provide detailed guidance on evolving technologies without resort to judicial intuition. State (or sometimes federal) law often creates rights in both tangible and intangible things. See *Ruckelshaus v. Monsanto Co.,* 467 U.S. 986, 1001, 104 S.Ct. 2862, 81 L.Ed.2d 815 (1984). In the context of the Takings Clause we often ask whether those state-created rights are sufficient to make something someone's property for constitutional purposes. See *id.,* at 1001–1003, 104 S.Ct. 2862; *Louisville Joint Stock Land Bank v. Radford,* 295 U.S. 555, 590–595, 55 S.Ct. 854, 79 L.Ed. 1593 (1935). A similar inquiry may be appropriate for the Fourth Amendment. Both the States and federal government are actively legislating in the area of third party data storage and the rights users enjoy. See, *e.g.,* Stored Communications Act, 18 U.S.C. § 2701 *et seq.*; Tex. Prop.Code Ann. § 111.004(12) (West 2017) (defining "[p]roperty" to include "property held in any digital or electronic medium"). State courts are busy expounding common law property principles in this area as well. *E.g., Ajemian v. Yahoo!, Inc.,* 478 Mass. 169, 170, 84 N.E.3d 766, 768 (2017) (e-mail account is a "form of property often referred to as a 'digital asset' "); *Eysoldt v. ProScan Imaging,* 194 Ohio App.3d 630, 638, 2011–Ohio–2359, 957 N.E.2d 780, 786 (2011) (permitting action for conversion of web account as intangible property). If state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations.

Fourth, while positive law may help establish a person's Fourth Amendment interest there may be some circumstances where positive law cannot be used to defeat it. *Ex parte Jackson* reflects that understanding. There this Court said that "[n]o law of Congress" could authorize letter carriers "to invade the secrecy of letters." 96 U.S., at 733. So the post office couldn't impose a regulation dictating that those mailing letters surrender all legal interests in them once they're deposited in a mailbox. If that is right, *Jackson* suggests the existence of a constitutional floor below which Fourth Amendment rights may not descend. Legislatures cannot ***2271** pass laws declaring your house or papers to be your property except to the extent the police wish to search them without cause. As the Court has previously explained, "we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' " *Jones,* 565 U.S., at 406, 132 S.Ct. 945 (quoting *Kyllo v. United States,* 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001)). Nor does this mean protecting only the specific rights known at the founding; it means protecting their modern analogues too. So, for example, while thermal imaging was unknown in 1791, this Court has recognized that using that technology to look inside a home constitutes a Fourth Amendment "search" of that "home" no less than a physical inspection might. *Id.,* at 40, 121 S.Ct. 2038.

Fifth, this constitutional floor may, in some instances, bar efforts to circumvent the Fourth Amendment's protection through the use of subpoenas. No one thinks the government can evade *Jackson* 's prohibition on opening sealed letters without a warrant simply by issuing a subpoena to a postmaster for "all letters sent by John Smith" or, worse, "all letters sent by John Smith concerning a particular transaction." So the question courts will confront will be this: What other kinds of records are sufficiently similar to letters in the mail that the same rule should apply?

It may be that, as an original matter, a subpoena requiring the recipient to produce records wasn't thought of as a "search or seizure" by the government implicating the Fourth Amendment, see *ante,* at 2247 - 2253 (opinion of ALITO, J.), but instead as an act of compelled self-incrimination implicating the Fifth Amendment, see *United States v. Hubbell,* 530 U.S. 27, 49–55, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000) (THOMAS, J., dissenting); Nagareda, Compulsion "To Be a Witness" and the Resurrection of Boyd, 74 N.Y.U. L. Rev. 1575, 1619, and n. 172 (1999). But the common law of searches and seizures does not appear to have confronted a case where private documents equivalent to a mailed letter were entrusted to a bailee and then subpoenaed. As a result, "[t]he common-law rule regarding subpoenas for documents held by third parties entrusted with information from the target is ... unknown and perhaps unknowable." Dripps, Perspectives on The Fourth Amendment Forty Years Later: Toward the Realization of an Inclusive Regulatory Model, 100 Minn. L. Rev. 1885, 1922 (2016). Given that (perhaps insoluble) uncertainty, I am content to adhere to *Jackson* and its implications for now.

To be sure, we must be wary of returning to the doctrine of *Boyd v. United States,* 116 U.S. 616, 6 S.Ct. 524, 29 L.Ed. 746. *Boyd* invoked the Fourth Amendment to restrict the use of subpoenas even for ordinary business records and, as Justice ALITO notes, eventually proved unworkable. See *ante,* at 2253 (dissenting opinion); 3 W. LaFave, J. Israel, N. King, & O. Kerr, Criminal Procedure § 8.7(a), pp. 185–187 (4th ed. 2015). But if we were to overthrow *Jackson* too and deny Fourth Amendment protection to *any* subpoenaed materials, we would do well to reconsider the scope of the Fifth Amendment while we're at it. Our precedents treat the right against self-incrimination as applicable only to testimony, not the production of incriminating evidence. See *Fisher v. United States,* 425 U.S. 391, 401, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). But there is substantial evidence that the privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incriminating evidence. Nagareda, *supra,* at 1605–1623; *Rex v. Purnell,* 96 Eng. Rep. 20 (K.B. 1748); Slobogin, Privacy at Risk 145 (2007).

***2272 ***

What does all this mean for the case before us? To start, I cannot fault the Sixth Circuit for holding that *Smith* and *Miller* extinguish any *Katz*-based Fourth Amendment interest in third party cell-site data. That is the plain effect of their categorical holdings. Nor can I fault the Court today for its implicit but unmistakable conclusion that the rationale of *Smith* and *Miller* is wrong; indeed, I agree with that. The Sixth Circuit was powerless to say so, but this Court can and should. At the same time, I do not agree with the Court's decision today to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared. Returning there, I worry, promises more trouble than help. Instead, I would look to a more traditional Fourth Amendment approach. Even if *Katz* may still supply one way to prove a Fourth Amendment interest, it has never been the only way. Neglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment.

Our case offers a cautionary example. It seems to me entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law. Yes, the telephone carrier holds the information. But 47 U.S.C. § 222 designates a customer's cell-site location information as "customer proprietary network information" (CPNI), § 222(h)(1)(A), and gives customers certain rights to control use of and access to CPNI about themselves. The statute generally forbids a carrier to "use, disclose, or permit access to individually identifiable" CPNI without the customer's consent, except as needed to provide the customer's telecommunications services. § 222(c)(1). It also requires the carrier to disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer." § 222(c)(2). Congress even afforded customers a private cause of action for damages against carriers who violate the Act's terms. § 207. Plainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right.

The problem is that we do not know anything more. Before the district court and court of appeals, Mr. Carpenter pursued only a *Katz* "reasonable expectations" argument. He did not invoke the law of property or any analogies to the common law, either there or in his petition for certiorari. Even in his merits brief before this Court, Mr. Carpenter's discussion of his positive law rights in cell-site data was cursory. He offered no analysis, for example, of what rights state law might provide him in addition to those supplied by § 222. In these

circumstances, I cannot help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument.

Unfortunately, too, this case marks the second time this Term that individuals have forfeited Fourth Amendment arguments based on positive law by failing to preserve them. See *Byrd,* 584 U.S., at ——, 138 S.Ct., at 1526. Litigants have had fair notice since at least *United States v. Jones* (2012) and *Florida v. Jardines* (2013) that arguments like these may vindicate Fourth Amendment interests even where *Katz* arguments do not. Yet the arguments have gone unmade, leaving courts to the usual *Katz* handwaving. These omissions do not serve the development of a sound or fully protective Fourth Amendment jurisprudence.

All Citations

138 S.Ct. 2206, 201 L.Ed.2d 507, 86 USLW 4491, 18 Cal. Daily Op. Serv. 6081, 2018 Daily Journal D.A.R. 6026, 27 Fla. L. Weekly Fed. S 415

Footnotes

* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.,* 200 U.S. 321, 337, 26 S.Ct. 282, 50 L.Ed. 499.

1 Justice KENNEDY believes that there is such a rubric—the "property-based concepts" that *Katz* purported to move beyond. *Post,* at 2224 (dissenting opinion). But while property rights are often informative, our cases by no means suggest that such an interest is "fundamental" or "dispositive" in determining which expectations of privacy are legitimate. *Post,* at 2227 - 2228. Justice THOMAS (and to a large extent Justice GORSUCH) would have us abandon *Katz* and return to an exclusively property-based approach. *Post,* at 2235 - 2236, 2244 - 2246 (THOMAS J., dissenting); *post,* at 2264 - 2266 (GORSUCH, J., dissenting). *Katz* of course "discredited" the "premise that property interests control," 389 U.S., at 353, 88 S.Ct. 507, and we have repeatedly emphasized that privacy interests do not rise or fall with property rights, see, *e.g., United States v. Jones,* 565 U.S. 400, 411, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (refusing to "make trespass the exclusive test"); *Kyllo v. United States,* 533 U.S. 27, 32, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property."). Neither party has asked the Court to reconsider *Katz* in this case.

2 Justice KENNEDY argues that this case is in a different category from *Jones* and the dragnet-type practices posited in *Knotts* because the disclosure of the cell-site records was subject to "judicial authorization." *Post,* at 2230 - 2232. That line of argument conflates the threshold question whether a "search" has occurred with the separate matter of whether the search was reasonable. The subpoena process set forth in the Stored Communications Act does not determine a target's expectation of privacy. And in any event, neither *Jones* nor *Knotts* purported to resolve the question of what authorization may be required to conduct such electronic surveillance techniques. But see *Jones,* 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring in judgment) (indicating that longer term GPS tracking may require a warrant).

3 The parties suggest as an alternative to their primary submissions that the acquisition of CSLI becomes a search only if it extends beyond a limited period. See Reply Brief 12 (proposing a 24–hour cutoff); Brief for United States 55–56 (suggesting a seven-day cutoff). As part of its argument, the Government treats the seven days of CSLI requested from Sprint as the pertinent period, even though Sprint produced only two days of records. Brief for United States 56. Contrary to Justice KENNEDY's assertion, *post,* at 2233, we need

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.

4 Justice GORSUCH faults us for not promulgating a complete code addressing the manifold situations that may be presented by this new technology—under a constitutional provision turning on what is "reasonable," no less. *Post,* at 2266 - 2268. Like Justice GORSUCH, we "do not begin to claim all the answers today," *post,* at 2268, and therefore decide no more than the case before us.

5 See *United States v. Dionisio,* 410 U.S. 1, 14, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973) ("No person can have a reasonable expectation that others will not know the sound of his voice"); *Donovan v. Lone Steer, Inc.,* 464 U.S. 408, 411, 415, 104 S.Ct. 769, 78 L.Ed.2d 567 (1984) (payroll and sales records); *California Bankers Assn. v. Shultz,* 416 U.S. 21, 67, 94 S.Ct. 1494, 39 L.Ed.2d 812 (1974) (Bank Secrecy Act reporting requirements); *See v. Seattle,* 387 U.S. 541, 544, 87 S.Ct. 1737, 18 L.Ed.2d 943 (1967) (financial books and records); *United States v. Powell,* 379 U.S. 48, 49, 57, 85 S.Ct. 248, 13 L.Ed.2d 112 (1964) (corporate tax records); *McPhaul v. United States,* 364 U.S. 372, 374, 382, 81 S.Ct. 138, 5 L.Ed.2d 136 (1960) (books and records of an organization); *United States v. Morton Salt Co.,* 338 U.S. 632, 634, 651–653, 70 S.Ct. 357, 94 L.Ed. 401 (1950) (Federal Trade Commission reporting requirement); *Oklahoma Press Publishing Co. v. Walling,* 327 U.S. 186, 189, 204–208, 66 S.Ct. 494, 90 L.Ed. 614 (1946) (payroll records); *Hale v. Henkel,* 201 U.S. 43, 45, 75, 26 S.Ct. 370, 50 L.Ed. 652 (1906) (corporate books and papers).

1 Justice Brandeis authored the principal dissent in *Olmstead*. He consulted the "underlying purpose," rather than "the words of the [Fourth] Amendment," to conclude that the wiretap was a search. 277 U.S., at 476, 48 S.Ct. 564. In Justice Brandeis' view, the Framers "recognized the significance of man's spiritual nature, of his feelings and of his intellect" and "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations." *Id.,* at 478, 48 S.Ct. 564. Thus, "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed," should constitute an unreasonable search under the Fourth Amendment. *Ibid.*

2 National Archives, Library of Congress, Founders Online, https://founders.archives.gov (all Internet materials as last visited June 18, 2018).

3 A Century of Lawmaking For A New Nation, U.S. Congressional Documents and Debates, 1774–1875 (May 1, 2003), https://memory.loc.gov/ammem/amlaw/lawhome.html.

4 Corpus of Historical American English, https://corpus.byu.edu/coha; Google Books (American), https://googlebooks.byu.edu/x.asp; Corpus of Founding Era American English, https://lawncl.byu.edu/cofea.

5 Readex, America's Historical Newspapers (2018), https://www.readex.com/content/americas-historical-newspapers.

6 Writs of assistance were "general warrants" that gave "customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws." *Stanford v. Texas,* 379 U.S. 476, 481, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965).

7 "Every subject has a right to be secure from all unreasonable searches and seizures of his person, his house, his papers, and all his possessions. All warrants, therefore, are contrary to right, if the cause or foundation

of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the person or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws." Mass. Const., pt. I, Art. XIV (1780).

8 The answer to that question is not obvious. Cell-site location records are business records that mechanically collect the interactions between a person's cell phone and the company's towers; they are not private papers and do not reveal the contents of any communications. Cf. Schnapper, Unreasonable Searches and Seizures of Papers, 71 Va. L. Rev. 869, 923–924 (1985) (explaining that business records that do not reveal "personal or speech-related confidences" might not satisfy the original meaning of "papers").

9 Carpenter relies on an order from the Federal Communications Commission (FCC), which weakly states that " '*[t]o the extent* [a customer's location information] is property, ... it is better understood as belonging to the customer, not the carrier.' " Brief for Petitioner 34, and n. 23 (quoting 13 FCC Rcd. 8061, 8093 ¶ 43 (1998); emphasis added). But this order was vacated by the Court of Appeals for the Tenth Circuit. *U.S. West, Inc. v. FCC,* 182 F.3d 1224, 1240 (1999). Notably, the carrier in that case argued that the FCC's regulation of customer information was a taking of *its* property. See *id.,* at 1230. Although the panel majority had no occasion to address this argument, see *id.,* at 1239, n. 14, the dissent concluded that the carrier had failed to prove the information was "property" at all, see *id.,* at 1247–1248 (opinion of Briscoe, J.).

10 Kugler & Strahilevitz, Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory, 2015 S.Ct. Rev. 205, 261; Bradley, Two Models of the Fourth Amendment, 83 Mich. L. Rev. 1468 (1985); Kerr, Four Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 505 (2007); Solove, Fourth Amendment Pragmatism, 51 Boston College L. Rev. 1511 (2010); Wasserstom & Seidman, The Fourth Amendment as Constitutional Theory, 77 Geo. L.J. 19, 29 (1988); Colb, What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 Stan. L. Rev. 119, 122 (2002); Clancy, The Fourth Amendment: Its History and Interpretation § 3.3.4, p. 65 (2008); *Minnesota v. Carter,* 525 U.S. 83, 97, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (Scalia, J., dissenting); *State v. Campbell,* 306 Ore. 157, 164, 759 P.2d 1040, 1044 (1988); Wilkins, Defining the "Reasonable Expectation of Privacy": an Emerging Tripartite Analysis, 40 Vand. L. Rev. 1077, 1107 (1987); Yeager, Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment, 84 J.Crim. L. & C. 249, 251 (1993); Thomas, Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment, 80 Notre Dame L. Rev. 1451, 1500 (2005); *Rakas v. Illinois,* 439 U.S. 128, 165, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978) (White, J., dissenting); Cloud, Rube Goldberg Meets the Constitution: The Supreme Court, Technology, and the Fourth Amendment, 72 Miss. L.J. 5, 7 (2002).

1 Any other interpretation of the Fourth Amendment's text would run into insuperable problems because it would apply not only to subpoenas *duces tecum* but to all other forms of compulsory process as well. If the Fourth Amendment applies to the compelled production of documents, then it must also apply to the compelled production of testimony—an outcome that we have repeatedly rejected and which, if accepted, would send much of the field of criminal procedure into a tailspin. See, *e.g.,* *United States v. Dionisio,* 410 U.S. 1, 9, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973) ("It is clear that a subpoena to appear before a grand jury is not a 'seizure' in the Fourth Amendment sense, even though that summons may be inconvenient or burdensome"); *United States v. Calandra,* 414 U.S. 338, 354, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974) ("Grand jury questions ... involve no independent governmental invasion of one's person, house, papers, or effects"). As a matter of original

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

understanding, a subpoena *duces tecum* no more effects a "search" or "seizure" of papers within the meaning of the Fourth Amendment than a subpoena *ad testificandum* effects a "search" or "seizure" of a person.

2 All that the Court can say in response is that we have "been careful not to uncritically extend existing precedents" when confronting new technologies. *Ante,* at 2222. But applying a categorical rule categorically does not "extend" precedent, so the Court's statement ends up sounding a lot like a tacit admission that it is overruling our precedents.

3 See, *e.g.,* Freedom of Information Act, 5 U.S.C. § 552(a) ("Each agency shall make available to the public information as follows ..."); Privacy Act, 5 U.S.C. § 552a(d)(1) ("Each agency that maintains a system of records shall ... upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof ..."); Fair Credit Reporting Act, 15 U.S.C. § 1681j(a)(1)(A) ("All consumer reporting agencies ... shall make all disclosures pursuant to section 1681g of this title once during any 12–month period upon request of the consumer and without charge to the consumer"); Right to Financial Privacy Act of 1978, 12 U.S.C. § 3404(c) ("The customer has the right ... to obtain a copy of the record which the financial institution shall keep of all instances in which the customer's record is disclosed to a Government authority pursuant to this section, including the identity of the Government authority to which such disclosure is made"); Government in the Sunshine Act, 5 U.S.C. § 552b(f)(2) ("Copies of such transcript, or minutes, or a transcription of such recording disclosing the identity of each speaker, shall be furnished to any person at the actual cost of duplication or transcription"); Cable Act, 47 U.S.C. § 551(d) ("A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator"); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(a)(1)(A) ("No funds shall be made available under any applicable program to any educational agency or institution which has a policy of denying, or which effectively prevents, the parents of students who are or have been in attendance at a school of such agency or at such institution, as the case may be, the right to inspect and review the education records of their children.... Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made").

4 See, *e.g.,* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(b)(1) ("No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information ...) of students without the written consent of their parents to any individual, agency, or organization ..."); Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1) ("A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d)"); Driver Privacy Protection Act, 18 U.S.C. § 2721(a)(1) ("A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity ... personal information ..."); Fair Credit Reporting Act, 15 U.S.C. § 1681b(a) ("[A]ny consumer reporting agency may furnish a consumer report under the following circumstances and no other ..."); Right to Financial Privacy Act, 12 U.S.C. § 3403(a) ("No financial institution, or officer, employees, or agent of a financial institution, may provide to any Government authority access to or copies of, or the information contained in, the financial records of any customer except in accordance with the provisions of this chapter"); Patient Safety and Quality Improvement Act, 42 U.S.C. § 299b–22(b) ("Notwithstanding any other provision of

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Federal, State, or local law, and subject to subsection (c) of this section, patient safety work product shall be confidential and shall not be disclosed"); Cable Act, 47 U.S.C. § 551(c)(1) ("[A] cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator").

5 Carpenter also cannot argue that he owns the cell-site records merely because they fall into the category of records referred to as "customer proprietary network information." 47 U.S.C. § 222(c). Even assuming labels alone can confer property rights, nothing in this particular label indicates whether the "information" is "proprietary" to the "customer" or to the provider of the "network." At best, the phrase "customer proprietary network information" is ambiguous, and context makes clear that it refers to the *provider* 's information. The Telecommunications Act defines the term to include all "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1)(A). For Carpenter to be right, he must own not only the cell-site records in this case, but also records relating to, for example, the "technical configuration" of his subscribed service—records that presumably include such intensely personal and private information as transmission wavelengths, transport protocols, and link layer system configurations.

6 Thus, this is not a case in which someone has entrusted papers that he or she owns to the safekeeping of another, and it does not involve a bailment. Cf. *post,* at 2268 - 2269 (GORSUCH, J., dissenting).

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

June 28, 2016 | **Ken Wallentine**

G.B.'s "occasional sexual partner" cut him with a kitchen knife after she learned that he had slept with another woman. G.B. sought medical help at a fire station. Police officers went to the hospital and interviewed G.B., who identified his assailant and provided the address of the apartment where the stabbing occurred. He told the officers that he didn't want any action taken over the stabbing.

Officers went to the apartment and saw blood drops on the floor and a bloody doormat in the trash can. A witness told police that he saw a woman slash G.B. Officers searched that woman's car and found blood. They asked G.B. for a DNA sample to compare to the blood found in the car. G.B. refused.

Officers sought a search warrant for a buccal swab of G.B. A judge found that probable cause existed to believe that "on the person of [G.B.] … there is now being concealed evidence, namely the victim's cheek cells/saliva," and the judge issued a search warrant. G.B. challenged the search warrant, claiming that forcibly taking a buccal swab sample to extract DNA from a crime victim is improper.

The court held that "the probable cause to search is not negated because G.B. is a third party to the criminal proceeding." To determine the constitutionality of a search, the court weighs the reasonableness of the search, assessing the scope and manner of execution. In this case, the intrusion involved (a quick and painless buccal swab) was minimally invasive. Moreover, the court imposed tight restrictions on how the DNA profile could be used. The government could not use the sample to show that G.B. committed perjury and could not enter the profile into any database. The sample was also to be destroyed after the prosecution of G.B.'s assailant.

Most victims of violent crime are not so tight-lipped about their assailants. As this case shows, when victims do refuse to provide a DNA sample—such as in cases where the victim is a gang member or someone involved in a romantic dispute—the mere status as a victim and not a perpetrator won't prevent officers from obtaining a search warrant.

In re Grand Jury Witness G.B., 2016 WL 3031604 (D.C. Ct. App. 2016)

KeyCite Yellow Flag - Negative Treatment
Not Followed on State Law Grounds State v. Medina, Vt., July 11, 2014

133 S.Ct. 1958
Supreme Court of the United States

MARYLAND, Petitioner
v.
Alonzo Jay KING, Jr.

No. 12–207.
|
Argued Feb. 26, 2013.
|
Decided June 3, 2013.

Synopsis
Background: Following denial of his motion to suppress DNA evidence, defendant was convicted in the Maryland Circuit Court, Wicomico County, Kathleen L. Beckstead, J., of first-degree rape. Defendant appealed. The Court of Appeals of Maryland, Harrell, J., 425 Md. 550, 42 A.3d 549, reversed and remanded. State filed application for stay of judgment pending disposition of its petition for writ of certiorari. The Supreme Court, Chief Justice Roberts, as Circuit Justice, —— U.S.——, 133 S.Ct. 1, 183 L.Ed.2d 667,granted the stay. Certiorari was subsequently granted.

Holdings: The Supreme Court, Justice Kennedy, held that:

[1] search using buccal swab to obtain defendant's DNA sample after arrest for serious offense was reasonable under Fourth Amendment, abrogating *People v. Buza*, 129 Cal.Rptr.3d 753, *Mario W. v. Kaipio*, 228 Ariz. 207, 265 P.3d 389; and

[2] the analysis of defendant's DNA did not render the DNA identification impermissible under the Fourth Amendment.

Reversed.

Justice Scalia, filed a dissenting opinion, in which Justice Ginsburg, Justice Sotomayor, and Justice Kagan joined.

West Headnotes (40)

[1] **Searches and Seizures** Taking samples of blood, or other physical specimens; handwriting exemplars

Using a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a "search" under the Fourth Amendment. U.S.C.A. Const.Amend. 4.

81 Cases that cite this headnote

[2] **Searches and Seizures** Expectation of privacy

Virtually any intrusion into the human body will work an invasion of cherished personal security that is subject to constitutional scrutiny. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

[3] **Searches and Seizures** Taking samples of blood, or other physical specimens; handwriting exemplars

Searches and Seizures Persons, Places and Things Protected

The fact than an intrusion into the human body is negligible is of central relevance to determining reasonableness, although it is still a search as the law defines that term. U.S.C.A. Const.Amend. 4.

19 Cases that cite this headnote

[4] **Searches and Seizures** Fourth Amendment and reasonableness in general

The Fourth Amendment's proper function is to constrain, not against all intrusions as such, but against intrusions which are not justified in the circumstances, or which are made in an improper manner. U.S.C.A. Const.Amend. 4.

16 Cases that cite this headnote

[5] **Searches and Seizures** Fourth Amendment and reasonableness in general

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

The ultimate measure of the constitutionality of a governmental search is reasonableness. U.S.C.A. Const.Amend. 4.

31 Cases that cite this headnote

[6] **Searches and Seizures** Nature and source of information in general; suspicion or conjecture

In giving content to the inquiry whether an intrusion is reasonable, the Supreme Court has preferred some quantum of individualized suspicion as a prerequisite to a constitutional search or seizure, but the Fourth Amendment imposes no irreducible requirement of such suspicion. U.S.C.A. Const.Amend. 4.

13 Cases that cite this headnote

[7] **Searches and Seizures** Necessity of and preference for warrant, and exceptions in general

Searches and Seizures Expectation of privacy

In some circumstances, such as when faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, certain general, or individual, circumstances may render a warrantless search or seizure reasonable. U.S.C.A. Const.Amend. 4.

23 Cases that cite this headnote

[8] **Searches and Seizures** Necessity of and preference for warrant, and exceptions in general

The need for a warrant is perhaps least when the search involves no discretion that could properly be limited by the interpolation of a neutral magistrate between the citizen and the law enforcement officer. U.S.C.A. Const.Amend. 4.

9 Cases that cite this headnote

[9] **Searches and Seizures** Samples and tests; identification procedures

The constitutionality of the search authorized by Maryland DNA Collection Act, providing that all arrestees charged with serious crimes must furnish DNA sample on a buccal swab applied to the inside of the cheeks, would be analyzed by reference to reasonableness, not individualized suspicion, since the arrestee was already in valid police custody for a serious offense supported by probable cause, and the DNA collection was not subject to the judgment of officers whose perspective might be colored by their primary involvement in the often competitive enterprise of ferreting out crime. U.S.C.A. Const.Amend. 4; West's Ann.Md.Code, Public Safety, § 2–504(a)(3).

29 Cases that cite this headnote

[10] **Searches and Seizures** Fourth Amendment and reasonableness in general

Searches and Seizures Scope, Conduct, and Duration of Warrantless Search

Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution. U.S.C.A. Const.Amend. 4.

47 Cases that cite this headnote

[11] **Searches and Seizures** Necessity of and preference for warrant, and exceptions in general

To say that no warrant is required for a search is merely to acknowledge that rather than employing a per se rule of unreasonableness, the court balances the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable. U.S.C.A. Const.Amend. 4.

29 Cases that cite this headnote

[12] **Searches and Seizures** Expectation of privacy

The application of traditional standards of reasonableness requires a court to weigh the promotion of legitimate governmental interests

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

against the degree to which the search intrudes upon an individual's privacy. U.S.C.A. Const.Amend. 4.

33 Cases that cite this headnote

[13] **Searches and Seizures** Inventory or booking search

Searches and Seizures Samples and tests; identification procedures

Warrantless search in which buccal swab was applied to the inside of defendant's cheeks as part of routine booking procedure for serious offenses, as authorized by Maryland DNA Collection Act, was reasonable under Fourth Amendment; in light of the context of a valid arrest supported by probable cause, defendant's expectations of privacy were not offended by the minor intrusion of a brief swab of his cheeks which did not break the skin, the swab did not increase the indignity already attendant to normal incidents of arrest, the state had significant interest in the identification of defendant and of all arrestees, and DNA identification had unmatched potential to serve that interest; abrogating *People v. Buza*, 129 Cal.Rptr.3d 753, *Mario W. v. Kaipio*, 228 Ariz. 207, 265 P.3d 389. U.S.C.A. Const.Amend. 4; West's Ann.Md.Code, Public Safety, § 2–504(a)(3).

47 Cases that cite this headnote

[14] **Arrest** Grounds for warrantless arrest in general

Arrest Custody and Disposition of Prisoner

Probable cause provides legal justification for arresting a person suspected of crime, and for a brief period of detention to take the administrative steps incident to arrest. U.S.C.A. Const.Amend. 4.

16 Cases that cite this headnote

[15] **Arrest** Persons and personal effects; person detained for investigation

The government has the right to search the person of the accused when legally arrested. U.S.C.A. Const.Amend. 4.

6 Cases that cite this headnote

[16] **Arrest** Search

Individual suspicion is not necessary to justify a search incident to an arrest, because the constitutionality of a search incident to an arrest does not depend on whether there is any indication that the person arrested possesses weapons or evidence; the fact of a lawful arrest, standing alone, authorizes a search. U.S.C.A. Const.Amend. 4.

48 Cases that cite this headnote

[17] **Searches and Seizures** Inventory or booking search

The routine administrative procedures at a police station house incident to booking and jailing the suspect derive from different origins and have different constitutional justifications than, say, the search of a place, for the search of a place not incident to an arrest depends on the fair probability that contraband or evidence of a crime will be found in a particular place. U.S.C.A. Const.Amend. 4.

8 Cases that cite this headnote

[18] **Arrest** Custody and Disposition of Prisoner

Indictments and Charging Instruments Defendants

In every criminal case, it is known and must be known who has been arrested and who is being tried.

1 Cases that cite this headnote

[19] **Indictments and Charging Instruments** Defendants

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

An individual's identity is more than just his name or Social Security number, and the government's interest in identification goes beyond ensuring that the proper name is typed on the indictment.

2 Cases that cite this headnote

[20] **Arrest** Custody and Disposition of Prisoner

A suspect's criminal history is a critical part of his identity that officers should know when processing him for detention.

2 Cases that cite this headnote

[21] **Searches and Seizures** Samples and tests; identification procedures

The DNA collected from arrestees is an irrefutable identification of the person from whom it was taken.

8 Cases that cite this headnote

[22] **Searches and Seizures** Samples and tests; identification procedures

DNA is another metric of identification used to connect the arrestee with his or her public persona, as reflected in records of his or her actions that are available to the police.

1 Cases that cite this headnote

[23] **Searches and Seizures** Inventory or booking search

Law enforcement officers bear a responsibility for ensuring that the custody of an arrestee does not create inordinate risks for facility staff, for the existing detainee population, and for a new detainee.

4 Cases that cite this headnote

[24] **Bail** Matters considered

An arrestee's past conduct is essential to an assessment of the danger he poses to the public, and this will inform a court's determination whether the individual should be released on bail.

5 Cases that cite this headnote

[25] **Arrest** Custody and Disposition of Prisoner

It is reasonable in all respects for the State to use an accepted database to determine if an arrestee is the object of suspicion in other serious crimes, suspicion that may provide a strong incentive for the arrestee to escape and flee.

[26] **Arrest** Search

The standards traditionally governing a search incident to lawful arrest are not commuted to the stricter *Terry* standards. U.S.C.A. Const.Amend. 4.

15 Cases that cite this headnote

[27] **Criminal Law** Booking or biographical questions

Though the Fifth Amendment's protection against self-incrimination is not, as a general rule, governed by a reasonableness standard, questions reasonably related to the police's administrative concerns fall outside the protections of *Miranda* and the answers thereto need not be suppressed. U.S.C.A. Const.Amend. 5.

10 Cases that cite this headnote

[28] **Searches and Seizures** Samples and tests; identification procedures

The question of how long it takes to process identifying information obtained from a valid search goes only to the efficacy of the search for its purpose of prompt identification, not the constitutionality of the search. U.S.C.A. Const.Amend. 4.

[29] **Searches and Seizures** Inventory or booking search

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

The Fourth Amendment allows police to take certain routine administrative steps incident to arrest, such as booking, photographing, and fingerprinting. U.S.C.A. Const.Amend. 4.

26 Cases that cite this headnote

[30] **Searches and Seizures** Expectation of privacy

A significant government interest does not alone suffice to justify a search; the government interest must outweigh the degree to which the search invades an individual's legitimate expectations of privacy. U.S.C.A. Const.Amend. 4.

29 Cases that cite this headnote

[31] **Searches and Seizures** Fourth Amendment and reasonableness in general

Although the underlying command of the Fourth Amendment is always that searches and seizures be reasonable, what is reasonable depends on the context within which a search takes place. U.S.C.A. Const.Amend. 4.

24 Cases that cite this headnote

[32] **Searches and Seizures** Expectation of privacy

The legitimacy of certain Fourth Amendment privacy expectations vis-á-vis the State may depend upon the individual's legal relationship with the State. U.S.C.A. Const.Amend. 4.

5 Cases that cite this headnote

[33] **Searches and Seizures** Expectation of privacy

The reasonableness of any search must be considered in the context of the person's legitimate expectations of privacy. U.S.C.A. Const.Amend. 4.

31 Cases that cite this headnote

[34] **Searches and Seizures** Expectation of privacy

The expectations of privacy of an individual taken into police custody necessarily are of a diminished scope, for Fourth Amendment purposes. U.S.C.A. Const.Amend. 4.

35 Cases that cite this headnote

[35] **Arrest** Search not incident to arrest; time and distance factors

Both the person and the property in an arrestee's immediate possession may be searched at the station house. U.S.C.A. Const.Amend. 4.

2 Cases that cite this headnote

[36] **Searches and Seizures** Skin, strip, and body searches

A search of the detainee's person when he is booked into custody may involve a relatively extensive exploration, including requiring at least some detainees to lift their genitals or cough in a squatting position. U.S.C.A. Const.Amend. 4.

6 Cases that cite this headnote

[37] **Searches and Seizures** Expectation of privacy

Once an individual has been arrested on probable cause for a dangerous offense that may require detention before trial, his or her expectations of privacy and freedom from police scrutiny are reduced. U.S.C.A. Const.Amend. 4.

18 Cases that cite this headnote

[38] **Searches and Seizures** Samples and tests; identification procedures

Once defendant's DNA was lawfully collected from a buccal swab applied to the inside of his cheeks as part of routine booking procedure for serious offenses, as authorized by Maryland DNA Collection Act, the analysis of the DNA pursuant to procedures authorized by Congress and set forth in the FBI's Combined DNA

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Index System (CODIS) did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment; the CODIS loci came from noncoding parts of the DNA that did not reveal defendant's genetic traits, and the Act provided statutory protections guarding against further invasion of privacy. U.S.C.A. Const.Amend. 4; West's Ann.Md.Code, Public Safety, §§ 2–504(a)(3), 2–505(b)(1), 2–512(c).

113 Cases that cite this headnote

[39] **Searches and Seizures** Inventory or booking search

Searches and Seizures Samples and tests; identification procedures

DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure. U.S.C.A. Const.Amend. 4.

61 Cases that cite this headnote

[40] **Searches and Seizures** Samples and tests; identification procedures

When officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment. U.S.C.A. Const.Amend. 4.

84 Cases that cite this headnote

West Codenotes

Negative Treatment Reconsidered

West's Ann.Md.Code, Public Safety, § 2–504(a)(3)

****1962** *Syllabus* *

***435** After his 2009 arrest on first- and second-degree assault charges, respondent King was processed through a Wicomico County, Maryland, facility, where booking personnel used a cheek swab to take a DNA sample pursuant to the Maryland DNA Collection Act (Act). The swab was matched to an unsolved 2003 rape, and King was charged with that crime. He moved to suppress the DNA match, arguing that the Act violated the Fourth Amendment, but the Circuit Court Judge found the law constitutional. King was convicted of rape. The Maryland Court of Appeals set aside the conviction, finding unconstitutional the portions of the Act authorizing DNA collection from felony arrestees.

Held : When officers make an arrest supported by probable cause to hold for a serious offense and bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment. Pp. 1966 – 1980.

(a) DNA testing may "significantly improve both the criminal justice system and police investigative practices," *District Attorney's Office for Third Judicial Dist. v. Osborne,* 557 U.S. 52, 55, 129 S.Ct. 2308, 174 L.Ed.2d 38, by making it "possible to determine whether a biological tissue matches a suspect with near certainty," *id.,* at 62, 129 S.Ct. 2308. Maryland's Act authorizes law enforcement authorities to collect DNA samples from, as relevant here, persons charged with violent crimes, including first-degree assault. A sample may not be added to a database before an individual is arraigned, and it must be destroyed if, *e.g.,* he is not convicted. Only identity information may be added to the database. Here, the officer collected a DNA sample using the common "buccal swab" procedure, which is quick and painless, ****1963** requires no "surgical intrusio[n] beneath the skin," *Winston v. Lee,* 470 U.S. 753, 760, 105 S.Ct. 1611, 84 L.Ed.2d 662, and poses no threat to the arrestee's "health or safety," *id.,* at 763, 105 S.Ct. 1611. Respondent's identification as the rapist resulted in part through the operation of the Combined DNA Index System (CODIS), which connects DNA laboratories at the local, state, and national level, and which standardizes the points of comparison, *i.e.,* loci, used in DNA analysis. Pp. 1966 – 1969.

(b) The framework for deciding the issue presented is well established. Using a buccal swab inside a person's cheek to obtain a DNA sample is a search under the Fourth Amendment. And the fact that ***436** the intrusion is negligible is of central relevance to determining whether the search is reasonable, "the ultimate measure of the

constitutionality of a governmental search," *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 652, 115 S.Ct. 2386, 132 L.Ed.2d 564. Because the need for a warrant is greatly diminished here, where the arrestee was already in valid police custody for a serious offense supported by probable cause, the search is analyzed by reference to "reasonableness, not individualized suspicion," *Samson v. California,* 547 U.S. 843, 855, n. 4, 126 S.Ct. 2193, 165 L.Ed.2d 250, and reasonableness is determined by weighing "the promotion of legitimate governmental interests" against "the degree to which [the search] intrudes upon an individual's privacy," *Wyoming v. Houghton,* 526 U.S. 295, 300, 119 S.Ct. 1297, 143 L.Ed.2d 408. P. 1970.

(c) In this balance of reasonableness, great weight is given to both the significant government interest at stake in the identification of arrestees and DNA identification's unmatched potential to serve that interest. Pp. 1970 – 1977.

(1) The Act serves a well-established, legitimate government interest: the need of law enforcement officers in a safe and accurate way to process and identify persons and possessions taken into custody. "[P]robable cause provides legal justification for arresting a [suspect], and for a brief period of detention to take the administrative steps incident to arrest," *Gerstein v. Pugh,* 420 U.S. 103, 113–114, 95 S.Ct. 854, 43 L.Ed.2d 54; and the "validity of the search of a person incident to a lawful arrest" is settled, *United States v. Robinson,* 414 U.S. 218, 224, 94 S.Ct. 467, 38 L.Ed.2d 427. Individual suspicion is not necessary. The "routine administrative procedure [s] at a police station house incident to booking and jailing the suspect" have different origins and different constitutional justifications than, say, the search of a place not incident to arrest, *Illinois v. Lafayette,* 462 U.S. 640, 643, 103 S.Ct. 2605, 77 L.Ed.2d 65, which depends on the "fair probability that contraband or evidence of a crime will be found in a particular place," *Illinois v. Gates,* 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527. And when probable cause exists to remove an individual from the normal channels of society and hold him in legal custody, DNA identification plays a critical role in serving those interests. First, the government has an interest in properly identifying "who has been arrested and who is being tried." *Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.*, 542 U.S. 177, 191, 124 S.Ct. 2451, 159 L.Ed.2d 292. Criminal history is critical to officers who are processing a suspect for detention. They already seek identity information through routine and accepted means: comparing booking photographs to sketch artists' depictions, showing mugshots to potential witnesses, and comparing fingerprints against electronic databases of known criminals and unsolved crimes. The only difference between DNA analysis and fingerprint ****1964** databases is the unparalleled accuracy DNA provides. DNA is another metric of identification used to connect the arrestee with his or her public persona, as reflected in records of his ***437** or her actions that are available to the police. Second, officers must ensure that the custody of an arrestee does not create inordinate "risks for facility staff, for the existing detainee population, and for a new detainee." *Florence v. Board of Chosen Freeholders of County of Burlington,* 566 U.S. ——, ——, 132 S.Ct. 1510, 182 L.Ed.2d 566. DNA allows officers to know the type of person being detained. Third, "the Government has a substantial interest in ensuring that persons accused of crimes are available for trials." *Bell v. Wolfish,* 441 U.S. 520, 534, 99 S.Ct. 1861, 60 L.Ed.2d 447. An arrestee may be more inclined to flee if he thinks that continued contact with the criminal justice system may expose another serious offense. Fourth, an arrestee's past conduct is essential to assessing the danger he poses to the public, which will inform a court's bail determination. Knowing that the defendant is wanted for a previous violent crime based on DNA identification may be especially probative in this regard. Finally, in the interests of justice, identifying an arrestee as the perpetrator of some heinous crime may have the salutary effect of freeing a person wrongfully imprisoned. Pp. 1970 – 1975.

(2) DNA identification is an important advance in the techniques long used by law enforcement to serve legitimate police concerns. Police routinely have used scientific advancements as standard procedures for identifying arrestees. Fingerprinting, perhaps the most direct historical analogue to DNA technology, has, from its advent, been viewed as a natural part of "the administrative steps incident to arrest." *County of Riverside v. McLaughlin,* 500 U.S. 44, 58, 111 S.Ct. 1661, 114 L.Ed.2d 49. However, DNA identification is far superior. The additional intrusion upon the arrestee's privacy beyond that associated with fingerprinting is not significant, and DNA identification is markedly more accurate. It may not be as fast as fingerprinting, but rapid fingerprint analysis is itself of recent vintage, and the question of how long it takes to process identifying information goes to the efficacy of the search for its purpose of prompt identification, not the constitutionality of the search. Rapid

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

technical advances are also reducing DNA processing times. Pp. 1974 – 1977.

(d) The government interest is not outweighed by respondent's privacy interests. Pp. 1977 – 1980.

(1) By comparison to the substantial government interest and the unique effectiveness of DNA identification, the intrusion of a cheek swab to obtain a DNA sample is minimal. Reasonableness must be considered in the context of an individual's legitimate privacy expectations, which necessarily diminish when he is taken into police custody. *Bell, supra,* at 557, 99 S.Ct. 1861. Such searches thus differ from the so-called special needs searches of, *e.g.,* otherwise law-abiding motorists at checkpoints. See *Indianapolis v. Edmond,* 531 U.S. 32, 121 S.Ct. 447, 148 L.Ed.2d 333. The reasonableness inquiry considers two other circumstances in which particularized suspicion is ***438** not categorically required: "diminished expectations of privacy [and a] minimal intrusion." *Illinois v. McArthur,* 531 U.S. 326, 330, 121 S.Ct. 946, 148 L.Ed.2d 838. An invasive surgery may raise privacy concerns weighty enough for the search to require a warrant, notwithstanding the arrestee's diminished privacy expectations, but a buccal swab, which involves a brief and minimal intrusion with "virtually no risk, trauma, or pain," *Schmerber v. California,* 384 U.S. 757, 771, 86 S.Ct. 1826, 16 L.Ed.2d 908, does not increase the indignity already attendant to ****1965** normal incidents of arrest. Pp. 1977 – 1979.

(2) The processing of respondent's DNA sample's CODIS loci also did not intrude on his privacy in a way that would make his DNA identification unconstitutional. Those loci came from noncoding DNA parts that do not reveal an arrestee's genetic traits and are unlikely to reveal any private medical information. Even if they could provide such information, they are not in fact tested for that end. Finally, the Act provides statutory protections to guard against such invasions of privacy. Pp. 1979 – 1980.

425 Md. 550, 42 A.3d 549, reversed.

KENNEDY, J., delivered the opinion of the Court, in which ROBERTS, C.J., and THOMAS, BREYER, and ALITO, JJ., joined. SCALIA, J., filed a dissenting opinion, in which GINSBURG, SOTOMAYOR, and KAGAN, JJ., joined.

Attorneys and Law Firms

Katherine Winfree, Baltimore, MD, for Petitioner.

Michael R. Dreeben, for the United States as amicus curiae, by special leave of the Court, supporting the Petitioner.

Kannon K. Shanmugam, Washington, DC, for Respondent.

Douglas F. Gansler, Attorney General of Maryland, Katherine Winfree, Chief Deputy Attorney General, Counsel of Record, Brian S. Kleinbord, Robert Taylor, Jr., Assistant Attorneys General, Mary Ann Rapp Ince, Daniel J. Jawor, Carrie J. Williams, Assistant Attorneys General, Office of the Attorney General, Baltimore, MD, for Petitioner.

Paul B. DeWolfe, Public Defender, Stephen B. Mercer, Chief Attorney, Forensics Division Office of the Public Defender, Baltimore, MD, Kannon K. Shanmugam, Counsel of Record, James M. McDonald, Kristin A. Feeley, David M. Horniak, Williams & Connolly LLP, Washington, DC, for Respondent.

Opinion

Justice KENNEDY delivered the opinion of the Court.

***439** In 2003 a man concealing his face and armed with a gun broke into a woman's home in Salisbury, Maryland. He ***440** raped her. The police were unable to identify or apprehend the assailant based on any detailed description or other evidence they then had, but they did obtain from the victim a sample of the perpetrator's DNA.

In 2009 Alonzo King was arrested in Wicomico County, Maryland, and charged with first- and second-degree assault for menacing a group of people with a shotgun. As part of a routine booking procedure for serious offenses, his DNA sample was taken by applying a cotton swab or filter paper —known as a buccal swab—to the inside of his cheeks. The DNA was found to match the DNA taken from the Salisbury rape victim. King was tried and convicted for the rape. Additional DNA samples were taken from him and used in the rape trial, but there seems to be no doubt that it was the DNA from the cheek sample taken at the time he was booked in 2009 that led to his first having been linked to the rape and charged with its commission.

The Court of Appeals of Maryland, on review of King's rape conviction, ruled that the DNA taken when King was booked for the 2009 charge was an unlawful seizure because obtaining and using the cheek swab was an unreasonable

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

search of the person. It set the rape conviction aside. This ***441** Court granted certiorari and now reverses ****1966** the judgment of the Maryland court.

I

When King was arrested on April 10, 2009, for menacing a group of people with a shotgun and charged in state court with both first- and second-degree assault, he was processed for detention in custody at the Wicomico County Central Booking facility. Booking personnel used a cheek swab to take the DNA sample from him pursuant to provisions of the Maryland DNA Collection Act (or Act).

On July 13, 2009, King's DNA record was uploaded to the Maryland DNA database, and three weeks later, on August 4, 2009, his DNA profile was matched to the DNA sample collected in the unsolved 2003 rape case. Once the DNA was matched to King, detectives presented the forensic evidence to a grand jury, which indicted him for the rape. Detectives obtained a search warrant and took a second sample of DNA from King, which again matched the evidence from the rape. He moved to suppress the DNA match on the grounds that Maryland's DNA collection law violated the Fourth Amendment. The Circuit Court Judge upheld the statute as constitutional. King pleaded not guilty to the rape charges but was convicted and sentenced to life in prison without the possibility of parole.

In a divided opinion, the Maryland Court of Appeals struck down the portions of the Act authorizing collection of DNA from felony arrestees as unconstitutional. The majority concluded that a DNA swab was an unreasonable search in violation of the Fourth Amendment because King's "expectation of privacy is greater than the State's purported interest in using King's DNA to identify him." 425 Md. 550, 561, 42 A.3d 549, 556 (2012). In reaching that conclusion the Maryland Court relied on the decisions of various other courts that have concluded that DNA identification of arrestees is impermissible. See, *e.g.*, ***442** *People v. Buza,* 129 Cal.Rptr.3d 753 (App.2011) (officially depublished); *Mario W. v. Kaipio,* 228 Ariz. 207, 265 P.3d 389 (App.2011).

Both federal and state courts have reached differing conclusions as to whether the Fourth Amendment prohibits the collection and analysis of a DNA sample from persons arrested, but not yet convicted, on felony charges. This Court granted certiorari, 568 U.S. ——, 133 S.Ct. 594, 184 L.Ed.2d 390 (2012), to address the question. King is the respondent here.

II

The advent of DNA technology is one of the most significant scientific advancements of our era. The full potential for use of genetic markers in medicine and science is still being explored, but the utility of DNA identification in the criminal justice system is already undisputed. Since the first use of forensic DNA analysis to catch a rapist and murderer in England in 1986, see J. Butler, Fundamentals of Forensic DNA Typing 5 (2009) (hereinafter Butler), law enforcement, the defense bar, and the courts have acknowledged DNA testing's "unparalleled ability both to exonerate the wrongly convicted and to identify the guilty. It has the potential to significantly improve both the criminal justice system and police investigative practices." *District Attorney's Office for Third Judicial Dist. v. Osborne,* 557 U.S. 52, 55, 129 S.Ct. 2308, 174 L.Ed.2d 38 (2009).

A

The current standard for forensic DNA testing relies on an analysis of the chromosomes located within the nucleus of all human cells. "The DNA material in chromosomes is composed of 'coding' and 'noncoding' ****1967** regions. The coding regions are known as *genes* and contain the information necessary for a cell to make proteins.... Non-protein-coding regions ... are not related directly to making proteins, [and] have been referred to as 'junk' DNA." Butler 25. The adjective "junk" may mislead the layperson, for in fact this is the DNA region used with near certainty to identify a person. ***443** The term apparently is intended to indicate that this particular noncoding region, while useful and even dispositive for purposes like identity, does not show more far-reaching and complex characteristics like genetic traits.

Many of the patterns found in DNA are shared among all people, so forensic analysis focuses on "repeated DNA sequences scattered throughout the human genome," known as "short tandem repeats" (STRs). *Id.,* at 147–148. The alternative possibilities for the size and frequency of these STRs at any given point along a strand of DNA are known as

"alleles," *id.,* at 25; and multiple alleles are analyzed in order to ensure that a DNA profile matches only one individual. Future refinements may improve present technology, but even now STR analysis makes it "possible to determine whether a biological tissue matches a suspect with near certainty." *Osborne, supra,* at 62, 129 S.Ct. 2308.

The Act authorizes Maryland law enforcement authorities to collect DNA samples from "an individual who is charged with ... a crime of violence or an attempt to commit a crime of violence; or ... burglary or an attempt to commit burglary." Md. Pub. Saf. Code Ann. § 2–504(a)(3)(i) (Lexis 2011). Maryland law defines a crime of violence to include murder, rape, first-degree assault, kidnaping, arson, sexual assault, and a variety of other serious crimes. Md. Crim. Law Code Ann. § 14–101Code Ann. § 14–101 (Lexis 2012). Once taken, a DNA sample may not be processed or placed in a database before the individual is arraigned (unless the individual consents). Md. Pub. Saf. Code Ann. § 2–504(d)(1) (Lexis 2011). It is at this point that a judicial officer ensures that there is probable cause to detain the arrestee on a qualifying serious offense. If "all qualifying criminal charges are determined to be unsupported by probable cause ... the DNA sample shall be immediately destroyed." § 2–504(d)(2)(i). DNA samples are also destroyed if "a criminal action begun against the individual ... does not result in a conviction," "the conviction is finally reversed or vacated and no new trial is permitted," ***444** or "the individual is granted an unconditional pardon." § 2–511(a)(1).

The Act also limits the information added to a DNA database and how it may be used. Specifically, "[o]nly DNA records that directly relate to the identification of individuals shall be collected and stored." § 2–505(b)(1). No purpose other than identification is permissible: "A person may not willfully test a DNA sample for information that does not relate to the identification of individuals as specified in this subtitle." § 2–512(c). Tests for familial matches are also prohibited. See § 2–506(d) ("A person may not perform a search of the statewide DNA data base for the purpose of identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the DNA sample was acquired"). The officers involved in taking and analyzing respondent's DNA sample complied with the Act in all respects.

Respondent's DNA was collected in this case using a common procedure known as a "buccal swab." "Buccal cell collection involves wiping a small piece of filter paper or a cotton swab similar to a Q-tip against the inside cheek of an individual's ****1968** mouth to collect some skin cells." Butler 86. The procedure is quick and painless. The swab touches inside an arrestee's mouth, but it requires no "surgical intrusio[n] beneath the skin," *Winston v. Lee,* 470 U.S. 753, 760, 105 S.Ct. 1611, 84 L.Ed.2d 662 (1985), and it poses no "threa[t] to the health or safety" of arrestees, *id.,* at 763, 105 S.Ct. 1611.

B

Respondent's identification as the rapist resulted in part through the operation of a national project to standardize collection and storage of DNA profiles. Authorized by Congress and supervised by the Federal Bureau of Investigation, the Combined DNA Index System (CODIS) connects DNA laboratories at the local, state, and national level. Since its authorization in 1994, the CODIS system has grown to include all 50 States and a number of federal ***445** agencies. CODIS collects DNA profiles provided by local laboratories taken from arrestees, convicted offenders, and forensic evidence found at crime scenes. To participate in CODIS, a local laboratory must sign a memorandum of understanding agreeing to adhere to quality standards and submit to audits to evaluate compliance with the federal standards for scientifically rigorous DNA testing. Butler 270.

One of the most significant aspects of CODIS is the standardization of the points of comparison in DNA analysis. The CODIS database is based on 13 loci at which the STR alleles are noted and compared. These loci make possible extreme accuracy in matching individual samples, with a "random match probability of approximately 1 in 100 trillion (assuming unrelated individuals)." *Ibid.* The CODIS loci are from the non-protein coding junk regions of DNA, and "are not known to have any association with a genetic disease or any other genetic predisposition. Thus, the information in the database is only useful for human identity testing." *Id.,* at 279. STR information is recorded only as a "string of numbers"; and the DNA identification is accompanied only by information denoting the laboratory and the analyst responsible for the submission. *Id.,* at 270. In short, CODIS sets uniform national standards for DNA matching and then facilitates connections between local law enforcement agencies who can share more specific information about matched STR profiles.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

All 50 States require the collection of DNA from felony convicts, and respondent does not dispute the validity of that practice. See Brief for Respondent 48. Twenty-eight States and the Federal Government have adopted laws similar to the Maryland Act authorizing the collection of DNA from some or all arrestees. See Brief for State of California et al. as *Amici Curiae* 4, n. 1 (States Brief) (collecting state statutes). Although those statutes vary in their particulars, such as what charges require a DNA sample, their similarity means that this case implicates more than the specific Maryland ***446** law. At issue is a standard, expanding technology already in widespread use throughout the Nation.

III

A

[1] **[2]** Although the DNA swab procedure used here presents a question the Court has not yet addressed, the framework for deciding the issue is well established. The Fourth Amendment, binding on the States by the Fourteenth Amendment, provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." It can be agreed that using a ****1969** buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search. Virtually any "intrusio[n] into the human body," *Schmerber v. California,* 384 U.S. 757, 770, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966), will work an invasion of " 'cherished personal security' that is subject to constitutional scrutiny," *Cupp v. Murphy,* 412 U.S. 291, 295, 93 S.Ct. 2000, 36 L.Ed.2d 900 (1973) (quoting *Terry v. Ohio,* 392 U.S. 1, 24–25, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968)). The Court has applied the Fourth Amendment to police efforts to draw blood, see *Schmerber, supra* ; *Missouri v. McNeely,* 569 U.S. ——, 133 S.Ct. 1552, 185 L.Ed.2d 696 (2013), scraping an arrestee's fingernails to obtain trace evidence, see *Cupp, supra,* and even to "a breathalyzer test, which generally requires the production of alveolar or 'deep lung' breath for chemical analysis," *Skinner v. Railway Labor Executives' Assn.,* 489 U.S. 602, 616, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989).

[3] A buccal swab is a far more gentle process than a venipuncture to draw blood. It involves but a light touch on the inside of the cheek; and although it can be deemed a search within the body of the arrestee, it requires no "surgical intrusions beneath the skin." *Winston,* 470 U.S., at 760, 105 S.Ct. 1611. The fact than an intrusion is negligible is of central relevance to determining reasonableness, although it is still a search as the law defines that term.

B

[4] **[5]** **[6]** To say that the Fourth Amendment applies here is the beginning point, not the end of the analysis. "[T]he Fourth ***447** Amendment's proper function is to constrain, not against all intrusions as such, but against intrusions which are not justified in the circumstances, or which are made in an improper manner." *Schmerber, supra,* at 768, 86 S.Ct. 1826. "As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.' " *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 652, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995). In giving content to the inquiry whether an intrusion is reasonable, the Court has preferred "some quantum of individualized suspicion ... [as] a prerequisite to a constitutional search or seizure. But the Fourth Amendment imposes no irreducible requirement of such suspicion." *United States v. Martinez–Fuerte,* 428 U.S. 543, 560–561, 96 S.Ct. 3074, 49 L.Ed.2d 1116 (1976) (citation and footnote omitted).

[7] **[8]** In some circumstances, such as "[w]hen faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable." *Illinois v. McArthur,* 531 U.S. 326, 330, 121 S.Ct. 946, 148 L.Ed.2d 838 (2001). Those circumstances diminish the need for a warrant, either because "the public interest is such that neither a warrant nor probable cause is required," *Maryland v. Buie,* 494 U.S. 325, 331, 110 S.Ct. 1093, 108 L.Ed.2d 276 (1990), or because an individual is already on notice, for instance because of his employment, see *Skinner, supra,* or the conditions of his release from government custody, see *Samson v. California,* 547 U.S. 843, 126 S.Ct. 2193, 165 L.Ed.2d 250 (2006), that some reasonable police intrusion

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

on his privacy is to be expected. The need for a warrant is perhaps least when the search involves no discretion that could properly be limited by the "interpo[lation of] a neutral magistrate between the citizen and the law enforcement officer." **1970 *Treasury Employees v. Von Raab,* 489 U.S. 656, 667, 109 S.Ct. 1384, 103 L.Ed.2d 685 (1989).

[9] The instant case can be addressed with this background. The Maryland DNA Collection Act provides that, in order to obtain a DNA sample, all arrestees charged with serious crimes must furnish the sample on a buccal swab applied, as ***448** noted, to the inside of the cheeks. The arrestee is already in valid police custody for a serious offense supported by probable cause. The DNA collection is not subject to the judgment of officers whose perspective might be "colored by their primary involvement in 'the often competitive enterprise of ferreting out crime.' " *Terry, supra,* at 12, 88 S.Ct. 1868 (quoting *Johnson v. United States,* 333 U.S. 10, 14, 68 S.Ct. 367, 92 L.Ed. 436 (1948)). As noted by this Court in a different but still instructive context involving blood testing, "[b]oth the circumstances justifying toxicological testing and the permissible limits of such intrusions are defined narrowly and specifically in the regulations that authorize them.... Indeed, in light of the standardized nature of the tests and the minimal discretion vested in those charged with administering the program, there are virtually no facts for a neutral magistrate to evaluate." *Skinner, supra,* at 622, 109 S.Ct. 1402. Here, the search effected by the buccal swab of respondent falls within the category of cases this Court has analyzed by reference to the proposition that the "touchstone of the Fourth Amendment is reasonableness, not individualized suspicion." *Samson, supra,* at 855, n. 4, 126 S.Ct. 2193.

[10] **[11]** **[12]** Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution. Urgent government interests are not a license for indiscriminate police behavior. To say that no warrant is required is merely to acknowledge that "rather than employing a *per se* rule of unreasonableness, we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." *McArthur, supra,* at 331, 121 S.Ct. 946. This application of "traditional standards of reasonableness" requires a court to weigh "the promotion of legitimate governmental interests" against "the degree to which [the search] intrudes upon an individual's privacy." *Wyoming v. Houghton,* 526 U.S. 295, 300, 119 S.Ct. 1297, 143 L.Ed.2d 408 (1999). An assessment of reasonableness to determine the lawfulness of requiring this class of arrestees to provide a DNA sample is central to the instant case.

***449** IV

A

[13] **[14]** **[15]** **[16]** The legitimate government interest served by the Maryland DNA Collection Act is one that is well established: the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody. It is beyond dispute that "probable cause provides legal justification for arresting a person suspected of crime, and for a brief period of detention to take the administrative steps incident to arrest." *Gerstein v. Pugh,* 420 U.S. 103, 113–114, 95 S.Ct. 854, 43 L.Ed.2d 54 (1975). Also uncontested is the "right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested." *Weeks v. United States,* 232 U.S. 383, 392, 34 S.Ct. 341, 58 L.Ed. 652 (1914), overruled on other grounds, *Mapp v. Ohio,* 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961). "The validity of the search of a person incident to a lawful arrest has been regarded as settled from ****1971** its first enunciation, and has remained virtually unchallenged." *United States v. Robinson,* 414 U.S. 218, 224, 94 S.Ct. 467, 38 L.Ed.2d 427 (1973). Even in that context, the Court has been clear that individual suspicion is not necessary, because "[t]he constitutionality of a search incident to an arrest does not depend on whether there is any indication that the person arrested possesses weapons or evidence. The fact of a lawful arrest, standing alone, authorizes a search." *Michigan v. DeFillippo,* 443 U.S. 31, 35, 99 S.Ct. 2627, 61 L.Ed.2d 343 (1979).

[17] The "routine administrative procedure[s] at a police station house incident to booking and jailing the suspect" derive from different origins and have different constitutional justifications than, say, the search of a place, *Illinois v. Lafayette,* 462 U.S. 640, 643, 103 S.Ct. 2605, 77 L.Ed.2d 65 (1983); for the search of a place not incident to an arrest depends on the "fair probability that contraband or evidence

of a crime will be found in a particular place," *Illinois v. Gates,* 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). The interests are further different when an individual is formally processed ***450** into police custody. Then "the law is in the act of subjecting the body of the accused to its physical dominion." *People v. Chiagles,* 237 N.Y. 193, 197, 142 N.E. 583, 584 (1923) (Cardozo, J.). When probable cause exists to remove an individual from the normal channels of society and hold him in legal custody, DNA identification plays a critical role in serving those interests.

[18] **[19]** First, "[i]n every criminal case, it is known and must be known who has been arrested and who is being tried." *Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.*, 542 U.S. 177, 191, 124 S.Ct. 2451, 159 L.Ed.2d 292 (2004). An individual's identity is more than just his name or Social Security number, and the government's interest in identification goes beyond ensuring that the proper name is typed on the indictment. Identity has never been considered limited to the name on the arrestee's birth certificate. In fact, a name is of little value compared to the real interest in identification at stake when an individual is brought into custody. "It is a well recognized aspect of criminal conduct that the perpetrator will take unusual steps to conceal not only his conduct, but also his identity. Disguises used while committing a crime may be supplemented or replaced by changed names, and even changed physical features." *Jones v. Murray,* 962 F.2d 302, 307 (C.A.4 1992). An "arrestee may be carrying a false ID or lie about his identity," and "criminal history records ... can be inaccurate or incomplete." *Florence v. Board of Chosen Freeholders of County of Burlington,* 566 U.S. ——, ——, 132 S.Ct. 1510, 1521, 182 L.Ed.2d 566 (2012).

[20] A suspect's criminal history is a critical part of his identity that officers should know when processing him for detention. It is a common occurrence that "[p]eople detained for minor offenses can turn out to be the most devious and dangerous criminals. Hours after the Oklahoma City bombing, Timothy McVeigh was stopped by a state trooper who noticed he was driving without a license plate. Police stopped serial killer Joel Rifkin for the same reason. One of the terrorists ***451** involved in the September 11 attacks was stopped and ticketed for speeding just two days before hijacking Flight 93." *Id.,* at ——, 132 S.Ct., at 1520 (citations omitted). Police already seek this crucial identifying information. They use routine and accepted means as varied as comparing the suspect's booking photograph to sketch artists' depictions of persons of interest, showing his mugshot to potential witnesses, and of course making a computerized ****1972** comparison of the arrestee's fingerprints against electronic databases of known criminals and unsolved crimes. In this respect the only difference between DNA analysis and the accepted use of fingerprint databases is the unparalleled accuracy DNA provides.

[21] **[22]** The task of identification necessarily entails searching public and police records based on the identifying information provided by the arrestee to see what is already known about him. The DNA collected from arrestees is an irrefutable identification of the person from whom it was taken. Like a fingerprint, the 13 CODIS loci are not themselves evidence of any particular crime, in the way that a drug test can by itself be evidence of illegal narcotics use. A DNA profile is useful to the police because it gives them a form of identification to search the records already in their valid possession. In this respect the use of DNA for identification is no different than matching an arrestee's face to a wanted poster of a previously unidentified suspect; or matching tattoos to known gang symbols to reveal a criminal affiliation; or matching the arrestee's fingerprints to those recovered from a crime scene. See Tr. of Oral Arg. 19. DNA is another metric of identification used to connect the arrestee with his or her public persona, as reflected in records of his or her actions that are available to the police. Those records may be linked to the arrestee by a variety of relevant forms of identification, including name, alias, date and time of previous convictions and the name then used, photograph, Social Security number, or CODIS profile. These data, found in official records, are checked as a routine matter to produce a ***452** more comprehensive record of the suspect's complete identity. Finding occurrences of the arrestee's CODIS profile in outstanding cases is consistent with this common practice. It uses a different form of identification than a name or fingerprint, but its function is the same.

[23] Second, law enforcement officers bear a responsibility for ensuring that the custody of an arrestee does not create inordinate "risks for facility staff, for the existing detainee population, and for a new detainee." *Florence, supra,* at ——, 132 S.Ct., at 1518. DNA identification can provide untainted information to those charged with detaining suspects and detaining the property of any felon. For these purposes officers must know the type of person whom they are detaining, and DNA allows them to make critical choices about how to proceed.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> "Knowledge of identity may inform an officer that a suspect is wanted for another offense, or has a record of violence or mental disorder. On the other hand, knowing identity may help clear a suspect and allow the police to concentrate their efforts elsewhere. Identity may prove particularly important in [certain cases, such as] where the police are investigating what appears to be a domestic assault. Officers called to investigate domestic disputes need to know whom they are dealing with in order to assess the situation, the threat to their own safety, and possible danger to the potential victim." *Hiibel, supra,* at 186, 124 S.Ct. 2451.

Recognizing that a name alone cannot address this interest in identity, the Court has approved, for example, "a visual inspection for certain tattoos and other signs of gang affiliation as part of the intake process," because "[t]he identification and isolation of gang members before they are admitted protects everyone." *Florence, supra,* at ——, 132 S.Ct., at 1519.

Third, looking forward to future stages of criminal prosecution, "the Government has a substantial interest in ensuring that **1973 persons accused of crimes are available for trials." *453 *Bell v. Wolfish,* 441 U.S. 520, 534, 99 S.Ct. 1861, 60 L.Ed.2d 447 (1979). A person who is arrested for one offense but knows that he has yet to answer for some past crime may be more inclined to flee the instant charges, lest continued contact with the criminal justice system expose one or more other serious offenses. For example, a defendant who had committed a prior sexual assault might be inclined to flee on a burglary charge, knowing that in every State a DNA sample would be taken from him after his conviction on the burglary charge that would tie him to the more serious charge of rape. In addition to subverting the administration of justice with respect to the crime of arrest, this ties back to the interest in safety; for a detainee who absconds from custody presents a risk to law enforcement officers, other detainees, victims of previous crimes, witnesses, and society at large.

[24] Fourth, an arrestee's past conduct is essential to an assessment of the danger he poses to the public, and this will inform a court's determination whether the individual should be released on bail. "The government's interest in preventing crime by arrestees is both legitimate and compelling." *United States v. Salerno,* 481 U.S. 739, 749, 107 S.Ct. 2095, 95 L.Ed.2d 697 (1987). DNA identification of a suspect in a violent crime provides critical information to the police and judicial officials in making a determination of the arrestee's future dangerousness. This inquiry always has entailed some scrutiny beyond the name on the defendant's driver's license. For example, Maryland law requires a judge to take into account not only "the nature and circumstances of the offense charged" but also "the defendant's family ties, employment status and history, financial resources, reputation, character and mental condition, length of residence in the community." 1 Md. Rules 4–216(f)(1)(A), (C) (2013). Knowing that the defendant is wanted for a previous violent crime based on DNA identification is especially probative of the court's consideration of "the danger of the defendant to the alleged victim, another person, or the community." Rule 4–216(f)(1)(G); *454 see also 18 U.S.C. § 3142 (2006 ed. and Supp. V) (similar requirements).

This interest is not speculative. In considering laws to require collecting DNA from arrestees, government agencies around the Nation found evidence of numerous cases in which felony arrestees would have been identified as violent through DNA identification matching them to previous crimes but who later committed additional crimes because such identification was not used to detain them. See Denver's Study on Preventable Crimes (2009) (three examples), online at http://www.denverda.org/DNA_Documents/Denver% 27s% 20Preventable% 20Crimes% 20Study.pdf (all Internet materials as visited May 31, 2013, and available in Clerk of Court's case file); Chicago's Study on Preventable Crimes (2005) (five examples), online at http://www.denverda.org/DNA_ Documents/Arrestee_Database/Chicago% 20Preventable% 20CrimesFinal.pdf; Maryland Study on Preventable Crimes (2008) (three examples), online at http:// www.denverda.org/DNA_Documents/MarylandDNAarresteestudy.pdf.

Present capabilities make it possible to complete a DNA identification that provides information essential to determining whether a detained suspect can be released pending trial. See, *e.g.,* States Brief 18, n. 10 ("DNA identification database samples have been processed in as few as two days in California, although around 30 days has been average"). Regardless of when the initial bail decision is **1974 made, release is not appropriate until a further determination is made as to the person's identity in the sense not only of what his birth certificate states but also what other records and data disclose to give that identity more meaning in

the whole context of who the person really is. And even when release is permitted, the background identity of the suspect is necessary for determining what conditions must be met before release is allowed. If release is authorized, it may take time for the conditions to be met, and so the time before actual ***455** release can be substantial. For example, in the federal system, defendants released conditionally are detained on average for 112 days; those released on unsecured bond for 37 days; on personal recognizance for 36 days; and on other financial conditions for 27 days. See Dept. of Justice, Bureau of Justice Statistics, Compendium of Federal Justice Statistics 45 (NCJ–213476, Dec. 2006) online at http://bjs.gov/content/pub/pdf/cfjs04.pdf. During this entire period, additional and supplemental data establishing more about the person's identity and background can provide critical information relevant to the conditions of release and whether to revisit an initial release determination. The facts of this case are illustrative. Though the record is not clear, if some thought were being given to releasing the respondent on bail on the gun charge, a release that would take weeks or months in any event, when the DNA report linked him to the prior rape, it would be relevant to the conditions of his release. The same would be true with a supplemental fingerprint report.

[25] Even if an arrestee is released on bail, development of DNA identification revealing the defendant's unknown violent past can and should lead to the revocation of his conditional release. See 18 U.S.C. § 3145(a) (providing for revocation of release); see also States Brief 11–12 (discussing examples where bail and diversion determinations were reversed after DNA identified the arrestee's violent history). Pretrial release of a person charged with a dangerous crime is a most serious responsibility. It is reasonable in all respects for the State to use an accepted database to determine if an arrestee is the object of suspicion in other serious crimes, suspicion that may provide a strong incentive for the arrestee to escape and flee.

Finally, in the interests of justice, the identification of an arrestee as the perpetrator of some heinous crime may have the salutary effect of freeing a person wrongfully imprisoned for the same offense. "[P]rompt [DNA] testing ... would ***456** speed up apprehension of criminals before they commit additional crimes, and prevent the grotesque detention of ... innocent people." J. Dwyer, P. Neufeld, & B. Scheck, Actual Innocence 245 (2000).

[26] **[27]** Because proper processing of arrestees is so important and has consequences for every stage of the criminal process, the Court has recognized that the "governmental interests underlying a station-house search of the arrestee's person and possessions may in some circumstances be even greater than those supporting a search immediately following arrest." *Lafayette,* 462 U.S., at 645, 103 S.Ct. 2605. Thus, the Court has been reluctant to circumscribe the authority of the police to conduct reasonable booking searches. For example, "[t]he standards traditionally governing a search incident to lawful arrest are not ... commuted to the stricter *Terry* standards." *Robinson,* 414 U.S., at 234, 94 S.Ct. 467. Nor are these interests in identification served only by a search of the arrestee himself. "[I]nspection of an arrestee's personal property may assist the police in ascertaining or verifying his identity." ****1975** *Lafayette, supra,* at 646, 103 S.Ct. 2605. And though the Fifth Amendment's protection against self-incrimination is not, as a general rule, governed by a reasonableness standard, the Court has held that "questions ... reasonably related to the police's administrative concerns ... fall outside the protections of *Miranda* [*v. Arizona,* 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966)] and the answers thereto need not be suppressed." *Pennsylvania v. Muniz,* 496 U.S. 582, 601–602, 110 S.Ct. 2638, 110 L.Ed.2d 528 (1990).

B

DNA identification represents an important advance in the techniques used by law enforcement to serve legitimate police concerns for as long as there have been arrests, concerns the courts have acknowledged and approved for more than a century. Law enforcement agencies routinely have used scientific advancements in their standard procedures for the identification of arrestees. "Police had been using photography ***457** to capture the faces of criminals almost since its invention." S. Cole, Suspect Identities 20 (2001). Courts did not dispute that practice, concluding that a "sheriff in making an arrest for a felony on a warrant has the right to exercise a discretion ..., [if] he should deem it necessary to the safe-keeping of a prisoner, and to prevent his escape, or to enable him the more readily to retake the prisoner if he should escape, to take his photograph." *State ex rel. Bruns v. Clausmier,* 154 Ind. 599, 601, 603, 57 N.E. 541, 542 (1900). By the time that it had become "the daily practice of the police officers and detectives of crime to use photographic pictures for the discovery and identification of criminals," the courts likewise had come to the conclusion that "it would be

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

[a] matter of regret to have its use unduly restricted upon any fanciful theory or constitutional privilege." *Shaffer v. United States,* 24 App.D.C. 417, 426 (1904).

Beginning in 1887, some police adopted more exacting means to identify arrestees, using the system of precise physical measurements pioneered by the French anthropologist Alphonse Bertillon. Bertillon identification consisted of 10 measurements of the arrestee's body, along with a "scientific analysis of the features of the face and an exact anatomical localization of the various scars, marks, &c., of the body." Defense of the Bertillon System, N.Y. Times, Jan. 20, 1896, p. 3. "[W]hen a prisoner was brought in, his photograph was taken according to the Bertillon system, and his body measurements were then made. The measurements were made ... and noted down on the back of a card or a blotter, and the photograph of the prisoner was expected to be placed on the card. This card, therefore, furnished both the likeness and description of the prisoner, and was placed in the rogues' gallery, and copies were sent to various cities where similar records were kept." *People ex rel. Jones v. Diehl,* 53 A.D. 645, 646, 65 N.Y.S. 801, 802 (1900). As in the present case, the point of taking this information about each arrestee was not limited to verifying that the proper name ***458** was on the indictment. These procedures were used to "facilitate the recapture of escaped prisoners," to aid "the investigation of their past records and personal history," and "to preserve the means of identification for ... future supervision after discharge." *Hodgeman v. Olsen,* 86 Wash. 615, 619, 150 P. 1122, 1124 (1915); see also *McGovern v. Van Riper,* 137 N.J. Eq. 24, 33–34, 43 A.2d 514, 519 (Ch.1945) ("[C]riminal identification is said to have two main purposes: (1) The identification of the accused as the person who committed the crime for which he is being held; and, (2) the identification of the accused as the same person who has been previously charged with, or ****1976** convicted of, other offenses against the criminal law").

Perhaps the most direct historical analogue to the DNA technology used to identify respondent is the familiar practice of fingerprinting arrestees. From the advent of this technique, courts had no trouble determining that fingerprinting was a natural part of "the administrative steps incident to arrest." *County of Riverside v. McLaughlin,* 500 U.S. 44, 58, 111 S.Ct. 1661, 114 L.Ed.2d 49 (1991). In the seminal case of *United States v. Kelly,* 55 F.2d 67 (C.A.2 1932), Judge Augustus Hand wrote that routine fingerprinting did not violate the Fourth Amendment precisely because it fit within the accepted means of processing an arrestee into custody:

> "Finger printing seems to be no more than an extension of methods of identification long used in dealing with persons under arrest for real or supposed violations of the criminal laws. It is known to be a very certain means devised by modern science to reach the desired end, and has become especially important in a time when increased population and vast aggregations of people in urban centers have rendered the notoriety of the individual in the community no longer a ready means of identification.
>
> .....
>
> "We find no ground in reason or authority for interfering with a method of identifying persons charged with ***459** crime which has now become widely known and frequently practiced." *Id.,* at 69–70.

By the middle of the 20th century, it was considered "elementary that a person in lawful custody may be required to submit to photographing and fingerprinting as part of routine identification processes." *Smith v. United States,* 324 F.2d 879, 882 (C.A.D.C.1963) (Burger, J.) (citations omitted).

DNA identification is an advanced technique superior to fingerprinting in many ways, so much so that to insist on fingerprints as the norm would make little sense to either the forensic expert or a layperson. The additional intrusion upon the arrestee's privacy beyond that associated with fingerprinting is not significant, see Part V, *infra,* and DNA is a markedly more accurate form of identifying arrestees. A suspect who has changed his facial features to evade photographic identification or even one who has undertaken the more arduous task of altering his fingerprints cannot escape the revealing power of his DNA.

[28] The respondent's primary objection to this analogy is that DNA identification is not as fast as fingerprinting, and so it should not be considered to be the 21st-century equivalent. See Tr. of Oral Arg. 53. But rapid analysis of fingerprints is itself of recent vintage. The FBI's vaunted Integrated Automated Fingerprint Identification System (IAFIS) was only "launched on July 28, 1999. Prior to this time, the processing of ... fingerprint submissions was largely a manual, labor-intensive process, taking weeks or months to process a single submission." Federal Bureau of Investigation, Integrated Automated Fingerprint Identification System, online at http://www.fbi.gov/about-

us/cjis/fingerprints_biometrics/iafis/iafis. It was not the advent of this technology that rendered fingerprint analysis constitutional in a single moment. The question of how long it takes to process identifying information obtained from a valid search goes only to the efficacy of the search for its purpose of prompt identification, not the constitutionality of the search. Cf. ***460** *Ontario v. Quon,* 560 U.S. ——, ——, 130 S.Ct. 2619, 2632, 177 L.Ed.2d 216 (2010). Given the importance of DNA in the identification of police records pertaining to arrestees ****1977** and the need to refine and confirm that identity for its important bearing on the decision to continue release on bail or to impose of new conditions, DNA serves an essential purpose despite the existence of delays such as the one that occurred in this case. Even so, the delay in processing DNA from arrestees is being reduced to a substantial degree by rapid technical advances. See, *e.g.,* Attorney General DeWine Announces Significant Drop in DNA Turnaround Time (Jan. 4, 2013) (DNA processing time reduced from 125 days in 2010 to 20 days in 2012), online at http://ohioattorneygeneral.gov/Media/News–Releases/ January–2013/Attorney–General–DeWine–Announces–Significant–Drop; Gov. Jindal Announces Elimination of DNA Backlog, DNA Unit Now Operating in Real Time (Nov. 17, 2011) (average DNA report time reduced from a year or more in 2009 to 20 days in 2011), online at http://www.gov.state.la.us/index.cfm?md=newsroom&tmp=detail&articleID=3102. And the FBI has already begun testing devices that will enable police to process the DNA of arrestees within 90 minutes. See Brief for National District Attorneys Association as *Amicus Curiae* 20–21; Tr. of Oral Arg. 17. An assessment and understanding of the reasonableness of this minimally invasive search of a person detained for a serious crime should take account of these technical advances. Just as fingerprinting was constitutional for generations prior to the introduction of IAFIS, DNA identification of arrestees is a permissible tool of law enforcement today. New technology will only further improve its speed and therefore its effectiveness. And, as noted above, actual release of a serious offender as a routine matter takes weeks or months in any event. By identifying not only who the arrestee is but also what other available records disclose about his past to show who he is, the police can ensure that they have the proper person under arrest and that they have made the necessary ***461** arrangements for his custody; and, just as important, they can also prevent suspicion against or prosecution of the innocent.

[29] In sum, there can be little reason to question "the legitimate interest of the government in knowing for an absolute certainty the identity of the person arrested, in knowing whether he is wanted elsewhere, and in ensuring his identification in the event he flees prosecution." 3 W. LaFave, Search and Seizure § 5.3(c), p. 216 (5th ed. 2012). To that end, courts have confirmed that the Fourth Amendment allows police to take certain routine "administrative steps incident to arrest—*i.e.,* ... book[ing], photograph[ing], and fingerprint[ing]." *McLaughlin,* 500 U.S., at 58, 111 S.Ct. 1661. DNA identification of arrestees, of the type approved by the Maryland statute here at issue, is "no more than an extension of methods of identification long used in dealing with persons under arrest." *Kelly,* 55 F.2d, at 69. In the balance of reasonableness required by the Fourth Amendment, therefore, the Court must give great weight both to the significant government interest at stake in the identification of arrestees and to the unmatched potential of DNA identification to serve that interest.

V

A

[30] **[31]** **[32]** By comparison to this substantial government interest and the unique effectiveness of DNA identification, the intrusion of a cheek swab to obtain a DNA sample is a minimal one. True, a significant government interest does not alone suffice to justify a search. The government interest must outweigh the degree to which the search invades an individual's legitimate expectations of privacy. In considering ****1978** those expectations in this case, however, the necessary predicate of a valid arrest for a serious offense is fundamental. "Although the underlying command of the Fourth Amendment is always that searches and seizures be reasonable, what is reasonable ***462** depends on the context within which a search takes place." *New Jersey v. T.L.O.,* 469 U.S. 325, 337, 105 S.Ct. 733, 83 L.Ed.2d 720 (1985). " [T]he legitimacy of certain privacy expectations vis-á-vis the State may depend upon the individual's legal relationship with the State." *Vernonia School Dist. 47J,* 515 U.S., at 654, 115 S.Ct. 2386.

[33] The reasonableness of any search must be considered in the context of the person's legitimate expectations of privacy. For example, when weighing the invasiveness of urinalysis of high school athletes, the Court noted that "[l]egitimate privacy expectations are even less with regard to student

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

athletes.... Public school locker rooms, the usual sites for these activities, are not notable for the privacy they afford." *Id.*, at 657, 115 S.Ct. 2386. Likewise, the Court has used a context-specific benchmark inapplicable to the public at large when "the expectations of privacy of covered employees are diminished by reason of their participation in an industry that is regulated pervasively," *Skinner,* 489 U.S., at 627, 109 S.Ct. 1402, or when "the 'operational realities of the workplace' may render entirely reasonable certain work-related intrusions by supervisors and co-workers that might be viewed as unreasonable in other contexts," *Von Raab,* 489 U.S., at 671, 109 S.Ct. 1384.

[34] **[35]** **[36]** The expectations of privacy of an individual taken into police custody "necessarily [are] of a diminished scope." *Bell,* 441 U.S., at 557, 99 S.Ct. 1861. "[B]oth the person and the property in his immediate possession may be searched at the station house." *United States v. Edwards,* 415 U.S. 800, 803, 94 S.Ct. 1234, 39 L.Ed.2d 771 (1974). A search of the detainee's person when he is booked into custody may " 'involve a relatively extensive exploration,' " *Robinson,* 414 U.S., at 227, 94 S.Ct. 467, including "requir[ing] at least some detainees to lift their genitals or cough in a squatting position," *Florence,* 566 U.S., at ——, 132 S.Ct., at 1520.

[37] In this critical respect, the search here at issue differs from the sort of programmatic searches of either the public at large or a particular class of regulated but otherwise law-abiding citizens that the Court has previously labeled as " 'special needs' " searches. *Chandler v. Miller,* 520 U.S. 305, 314, 117 S.Ct. 1295, 137 L.Ed.2d 513 (1997). When the police stop a motorist at a checkpoint, ***463** see *Indianapolis v. Edmond,* 531 U.S. 32, 121 S.Ct. 447, 148 L.Ed.2d 333 (2000), or test a political candidate for illegal narcotics, see *Chandler, supra,* they intrude upon substantial expectations of privacy. So the Court has insisted on some purpose other than "to detect evidence of ordinary criminal wrongdoing" to justify these searches in the absence of individualized suspicion. *Edmond, supra,* at 38, 121 S.Ct. 447. Once an individual has been arrested on probable cause for a dangerous offense that may require detention before trial, however, his or her expectations of privacy and freedom from police scrutiny are reduced. DNA identification like that at issue here thus does not require consideration of any unique needs that would be required to justify searching the average citizen. The special needs cases, though in full accord with the result reached here, do not have a direct bearing on the issues presented in this case, because unlike the search of a citizen who has not been suspected of a wrong, a detainee has a reduced expectation of privacy.

****1979** The reasonableness inquiry here considers two other circumstances in which the Court has held that particularized suspicion is not categorically required: "diminished expectations of privacy [and] minimal intrusions." *McArthur,* 531 U.S., at 330, 121 S.Ct. 946. This is not to suggest that any search is acceptable solely because a person is in custody. Some searches, such as invasive surgery, see *Winston,* 470 U.S. 753, 105 S.Ct. 1611, or a search of the arrestee's home, see *Chimel v. California,* 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969), involve either greater intrusions or higher expectations of privacy than are present in this case. In those situations, when the Court must "balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable," *McArthur, supra,* at 331, 121 S.Ct. 946, the privacy-related concerns are weighty enough that the search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee.

Here, by contrast to the approved standard procedures incident to any arrest detailed above, a buccal swab involves an even more brief and still minimal intrusion. A gentle rub along the inside of the cheek does not break the skin, ***464** and it "involves virtually no risk, trauma, or pain." *Schmerber,* 384 U.S., at 771, 86 S.Ct. 1826. "A crucial factor in analyzing the magnitude of the intrusion ... is the extent to which the procedure may threaten the safety or health of the individual," *Winston, supra,* at 761, 105 S.Ct. 1611, and nothing suggests that a buccal swab poses any physical danger whatsoever. A brief intrusion of an arrestee's person is subject to the Fourth Amendment, but a swab of this nature does not increase the indignity already attendant to normal incidents of arrest.

B

[38] In addition the processing of respondent's DNA sample's 13 CODIS loci did not intrude on respondent's

privacy in a way that would make his DNA identification unconstitutional.

First, as already noted, the CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee. While science can always progress further, and those progressions may have Fourth Amendment consequences, alleles at the CODIS loci "are not at present revealing information beyond identification." Katsanis & Wagner, Characterization of the Standard and Recommended CODIS Markers, 58 J. Forensic Sci. S169, S171 (2013). The argument that the testing at issue in this case reveals any private medical information at all is open to dispute.

And even if non-coding alleles could provide some information, they are not in fact tested for that end. It is undisputed that law enforcement officers analyze DNA for the sole purpose of generating a unique identifying number against which future samples may be matched. This parallels a similar safeguard based on actual practice in the school drug-testing context, where the Court deemed it "significant that the tests at issue here look only for drugs, and not for whether the student is, for example, epileptic, pregnant, or diabetic." *Vernonia School Dist. 47J,* 515 U.S., at 658, 115 S.Ct. 2386. If in the future police analyze samples to determine, for instance, an arrestee's predisposition for a particular disease ***465** or other hereditary factors not relevant to identity, that case would present additional privacy concerns not present here.

Finally, the Act provides statutory protections that guard against further invasion of privacy. As noted above, the Act requires that "[o]nly DNA records that ****1980** directly relate to the identification of individuals shall be collected and stored." Md. Pub. Saf. Code Ann. § 2–505(b)(1). No purpose other than identification is permissible: "A person may not willfully test a DNA sample for information that does not relate to the identification of individuals as specified in this subtitle." § 2–512(c). This Court has noted often that "a 'statutory or regulatory duty to avoid unwarranted disclosures' generally allays ... privacy concerns." *NASA v. Nelson,* 562 U.S. ——, ——, 131 S.Ct. 746, 750, 178 L.Ed.2d 667 (2011) (quoting *Whalen v. Roe,* 429 U.S. 589, 605, 97 S.Ct. 869, 51 L.Ed.2d 64 (1977)). The Court need not speculate about the risks posed "by a system that did not contain comparable security provisions." *Id.,* at 606, 97 S.Ct. 869. In light of the scientific and statutory safeguards, once respondent's DNA was lawfully collected the STR analysis of respondent's DNA pursuant to CODIS procedures did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment.

* * *

[39] **[40]** In light of the context of a valid arrest supported by probable cause respondent's expectations of privacy were not offended by the minor intrusion of a brief swab of his cheeks. By contrast, that same context of arrest gives rise to significant state interests in identifying respondent not only so that the proper name can be attached to his charges but also so that the criminal justice system can make informed decisions concerning pretrial custody. Upon these considerations the Court concludes that DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure. When officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and ***466** analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.

The judgment of the Court of Appeals of Maryland is reversed.

It is so ordered.

Justice SCALIA, with whom Justice GINSBURG, Justice SOTOMAYOR, and Justice KAGAN join, dissenting.

The Fourth Amendment forbids searching a person for evidence of a crime when there is no basis for believing the person is guilty of the crime or is in possession of incriminating evidence. That prohibition is categorical and without exception; it lies at the very heart of the Fourth Amendment. Whenever this Court has allowed a suspicionless search, it has insisted upon a justifying motive apart from the investigation of crime.

It is obvious that no such noninvestigative motive exists in this case. The Court's assertion that DNA is being taken, not to solve crimes, but to *identify* those in the State's custody, taxes the credulity of the credulous. And the Court's comparison of Maryland's DNA searches to other techniques, such as fingerprinting, can seem apt only to those who know no more

than today's opinion has chosen to tell them about how those DNA searches actually work.

I

A

At the time of the Founding, Americans despised the British use of so-called "general warrants"—warrants not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application. The first ****1981** Virginia Constitution declared that "general warrants, whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed," or to search a person "whose offence is not particularly described and supported by evidence," "are ***467** grievous and oppressive, and ought not be granted." Va. Declaration of Rights § 10 (1776), in 1 B. Schwartz, The Bill of Rights: A Documentary History 234, 235 (1971). The Maryland Declaration of Rights similarly provided that general warrants were "illegal." Md. Declaration of Rights § XXIII (1776), in *id.,* at 280, 282.

In the ratification debates, Antifederalists sarcastically predicted that the general, suspicionless warrant would be among the Constitution's "blessings." Blessings of the New Government, Independent Gazetteer, Oct. 6, 1787, in 13 Documentary History of the Ratification of the Constitution 345 (J. Kaminski & G. Saladino eds. 1981). "Brutus" of New York asked why the Federal Constitution contained no provision like Maryland's, Brutus II, N.Y. Journal, Nov. 1, 1787, in *id.,* at 524, and Patrick Henry warned that the new Federal Constitution would expose the citizenry to searches and seizures "in the most arbitrary manner, without any evidence or reason." 3 Debates on the Federal Constitution 588 (J. Elliot 2d ed. 1854).

Madison's draft of what became the Fourth Amendment answered these charges by providing that the "rights of the people to be secured in their persons ... from all unreasonable searches and seizures, shall not be violated by warrants issued without probable cause ... or not particularly describing the places to be searched." 1 Annals of Cong. 434–435 (1789). As ratified, the Fourth Amendment's Warrant Clause forbids a warrant to "issue" except "upon probable cause," and requires that it be "particula[r]" (which is to say, *individualized*) to "the place to be searched, and the persons or things to be seized." And we have held that, even when a warrant is not constitutionally necessary, the Fourth Amendment's general prohibition of "unreasonable" searches imports the same requirement of individualized suspicion. See *Chandler v. Miller,* 520 U.S. 305, 308, 117 S.Ct. 1295, 137 L.Ed.2d 513 (1997).

Although there is a "closely guarded category of constitutionally permissible suspicionless searches," *id.,* at 309, 117 S.Ct. 1295, that ***468** has never included searches designed to serve "the normal need for law enforcement," *Skinner v. Railway Labor Executives' Assn.,* 489 U.S. 602, 619, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989) (internal quotation marks omitted). Even the common name for suspicionless searches—"special needs" searches—itself reflects that they must be justified, *always,* by concerns " other than crime detection." *Chandler, supra,* at 313–314, 117 S.Ct. 1295. We have approved random drug tests of railroad employees, yes—but only because the Government's need to "regulat[e] the conduct of railroad employees to ensure safety" is distinct from "normal law enforcement." *Skinner, supra,* at 620, 109 S.Ct. 1402. So too we have approved suspicionless searches in public schools—but only because there the government acts in furtherance of its "responsibilities ... as guardian and tutor of children entrusted to its care." *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 665, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995).

So while the Court is correct to note (*ante,* at 1969 – 1970) that there are instances in which we have permitted searches without individualized suspicion, "[i]n none of these cases ... did we indicate approval of a [search] whose primary ****1982** purpose was to detect evidence of ordinary criminal wrongdoing." *Indianapolis v. Edmond,* 531 U.S. 32, 38, 121 S.Ct. 447, 148 L.Ed.2d 333 (2000). That limitation is crucial. It is only when a governmental purpose aside from crime-solving is at stake that we engage in the free-form "reasonableness" inquiry that the Court indulges at length today. To put it another way, both the legitimacy of the Court's method and the correctness of its outcome hinge entirely on the truth of a single proposition: that the primary purpose of these DNA searches is something other than simply discovering evidence of criminal wrongdoing. As I detail below, that proposition is wrong.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

B

The Court alludes at several points (see *ante,* at 1970 – 1971, 1978 – 1979) to the fact that King was an arrestee, and arrestees may be validly searched incident to their arrest. But the Court does not really *rest* on this principle, and for good reason: ***469** The objects of a search incident to arrest must be either (1) weapons or evidence that might easily be destroyed, or (2) evidence relevant to the crime of arrest. See *Arizona v. Gant,* 556 U.S. 332, 343–344, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009); *Thornton v. United States,* 541 U.S. 615, 632, 124 S.Ct. 2127, 158 L.Ed.2d 905 (2004) (SCALIA, J., concurring in judgment). Neither is the object of the search at issue here.

The Court hastens to clarify that it does not mean to approve invasive surgery on arrestees or warrantless searches of their homes. *Ante,* at 1978 – 1979. That the Court feels the need to disclaim these consequences is as damning a criticism of its suspicionless-search regime as any I can muster. And the Court's attempt to distinguish those hypothetical searches from this real one is unconvincing. We are told that the "privacy-related concerns" in the search of a home "are weighty enough that the search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee." *Ante,* at 1979. But why are the "privacy-related concerns" not also "weighty" when an intrusion into the *body* is at stake? (The Fourth Amendment lists "persons" *first* among the entities protected against unreasonable searches and seizures.) And could the police engage, without any suspicion of wrongdoing, in a "brief and ... minimal" intrusion into the home of an arrestee—perhaps just peeking around the curtilage a bit? See *ante,* at 1979. Obviously not.

At any rate, all this discussion is beside the point. No matter the degree of invasiveness, suspicionless searches are *never* allowed if their principal end is ordinary crime-solving. A search incident to arrest either serves other ends (such as officer safety, in a search for weapons) or is not suspicionless (as when there is reason to believe the arrestee possesses evidence relevant to the crime of arrest).

Sensing (correctly) that it needs more, the Court elaborates at length the ways that the search here served the special purpose of "identifying" King. [1] But that ****1983** seems to ***470** me quite wrong—unless what one means by "identifying" someone is "searching for evidence that he has committed crimes unrelated to the crime of his arrest." At points the Court does appear to use "identifying" in that peculiar sense —claiming, for example, that knowing "an arrestee's past conduct is essential to an assessment of the danger he poses." *Ante,* at 1973. If identifying someone means finding out what unsolved crimes he has committed, then identification is indistinguishable from the ordinary law-enforcement aims that have never been thought to justify a suspicionless search. Searching every lawfully stopped car, for example, might turn up information about unsolved crimes the driver had committed, but no one would say that such a search was aimed at " identifying" him, and no court would hold such a search lawful. I will therefore assume that the Court means that the DNA search at issue here was useful to "identify" King in the normal sense of that word—in the sense that would identify the author of Introduction to the Principles of Morals and Legislation as Jeremy Bentham.

1

The portion of the Court's opinion that explains the identification rationale is strangely silent on the actual workings of the DNA search at issue here. To know those facts is to be instantly disabused of the notion that what happened had anything to do with identifying King.

King was arrested on April 10, 2009, on charges unrelated to the case before us. That same day, April 10, the police ***471** searched him and seized the DNA evidence at issue here. What happened next? Reading the Court's opinion, particularly its insistence that the search was necessary to know "who [had] been arrested," *ante,* at 1971, one might guess that King's DNA was swiftly processed and his identity thereby confirmed—perhaps against some master database of known DNA profiles, as is done for fingerprints. After all, was not the suspicionless search here crucial to avoid "inordinate risks for facility staff" or to "existing detainee population," *ante,* at 1972? Surely, then—*surely*—the State of Maryland got cracking on those grave risks immediately, by rushing to identify King with his DNA as soon as possible.

Nothing could be further from the truth. Maryland officials did not even begin the process of testing King's DNA that day. Or, actually, the next day. Or the day after that. And that was for a simple reason: Maryland law forbids them to do so. A "DNA sample collected from an individual charged with a crime ... *may not* be tested or placed in the statewide DNA data base system prior to the first scheduled arraignment

date." Md. Pub. Saf. Code Ann. § 2–504(d)(1) (Lexis 2011) (emphasis added). And King's first appearance in court was not until three days after his arrest. (I suspect, though, that they did not wait three days to ask his name or take his fingerprints.)

This places in a rather different light the Court's solemn declaration that the search here was necessary so that King could be identified at "every stage of the criminal process." *Ante,* at 1974. I hope that the Maryland officials who read the Court's opinion do not take it seriously. Acting on the Court's misperception of Maryland law could lead to jail time. See Md. Pub. Saf. Code Ann. § 2–512(c)–(e) (punishing by up to five years' imprisonment anyone who obtains or tests DNA information except as provided by statute). Does the Court really believe that Maryland did not know whom it was arraigning? The Court's response is to imagine that release on bail could take so long that the DNA results are ***472** returned in time, or perhaps that bail ****1984** could be revoked if the DNA test turned up incriminating information. *Ante,* at 1973 – 1974. That is no answer at all. If the purpose of this Act is to assess "whether [King] should be released on bail," *ante,* at 1973, why would it *possibly* forbid the DNA testing process to *begin* until King was arraigned? Why would Maryland resign itself to simply hoping that the bail decision will drag out long enough that the "identification" can succeed before the arrestee is released? The truth, known to Maryland and increasingly to the reader: this search had nothing to do with establishing King's identity.

It gets worse. King's DNA sample was not received by the Maryland State Police's Forensic Sciences Division until April 23, 2009—two weeks after his arrest. It sat in that office, ripening in a storage area, until the custodians got around to mailing it to a lab for testing on June 25, 2009—two months after it was received, and nearly *three* since King's arrest. After it was mailed, the data from the lab tests were not available for several more weeks, until July 13, 2009, which is when the test results were entered into Maryland's DNA database, *together with information identifying the person from whom the sample was taken*. Meanwhile, bail had been set, King had engaged in discovery, and he had requested a speedy trial—presumably not a trial of John Doe. It was not until August 4, 2009—four months after King's arrest—that the forwarded sample transmitted (*without* identifying information) from the Maryland DNA database to the Federal Bureau of Investigation's national database was matched with a sample taken from the scene of an unrelated crime years earlier.

A more specific description of exactly what happened at this point illustrates why, by definition, King could not have been *identified* by this match. The FBI's DNA database (known as CODIS) consists of two distinct collections. FBI, CODIS and NDIS Fact Sheet, http://www.fbi.gov/about-us/lab/codis/codis-and-ndis-fact-sheet (all Internet materials as visited May 31, 2013, and available in Clerk of Court's case ***473** file). One of them, the one to which King's DNA was submitted, consists of DNA samples taken from known convicts or arrestees. I will refer to this as the "Convict and Arrestee Collection." The other collection consists of samples taken from crime scenes; I will refer to this as the "Unsolved Crimes Collection." The Convict and Arrestee Collection stores "no names or other personal identifiers of the offenders, arrestees, or detainees." *Ibid.* Rather, it contains only the DNA profile itself, the name of the agency that submitted it, the laboratory personnel who analyzed it, and an identification number for the specimen. *Ibid.* This is because the submitting state laboratories are expected *already* to know the identities of the convicts and arrestees from whom samples are taken. (And, of course, they do.)

Moreover, the CODIS system works by checking to see whether any of the samples in the Unsolved Crimes Collection match any of the samples in the Convict and Arrestee Collection. *Ibid.* That is sensible, if what one wants to do is solve those cold cases, but note what it requires: that the identity of the people whose DNA has been entered in the Convict and Arrestee Collection *already be known*.[2] If one wanted to identify someone in custody using ****1985** his DNA, the logical thing to do would be to compare that DNA against the Convict and Arrestee Collection: to search, in other words, the collection that could be used (by checking back with the submitting state agency) to identify people, rather than the collection of evidence from unsolved crimes, whose perpetrators are by definition unknown. But that is not what was done. And that is because this search had nothing to do with identification.

In fact, if anything was "identified" at the moment that the DNA database returned a match, it was not King—his ***474** identity was already known. (The docket for the original criminal charges lists his full name, his race, his sex, his height, his weight, his date of birth, and his address.) Rather, what the August 4 match "identified" was *the previously-taken sample from the earlier crime*. That

sample was genuinely mysterious to Maryland; the State knew that it had probably been left by the victim's attacker, but nothing else. King was not identified by his association with the sample; rather, the sample was identified by its association with King. The Court effectively destroys its own "identification" theory when it acknowledges that the object of this search was "to see what [was] already known about [King]." King was who he was, and volumes of his biography could not make him any more or any less King. No minimally competent speaker of English would say, upon noticing a known arrestee's similarity "to a wanted poster of a previously unidentified suspect," *ante,* at 1972, that the *arrestee* had thereby been identified. It was the previously unidentified suspect who had been identified—just as, here, it was the previously unidentified rapist.

2

That taking DNA samples from arrestees has nothing to do with identifying them is confirmed not just by actual practice (which the Court ignores) but by the enabling statute itself (which the Court also ignores). The Maryland Act at issue has a section helpfully entitled "Purpose of collecting and testing DNA samples." Md. Pub. Saf. Code Ann. § 2–505. (One would expect such a section to play a somewhat larger role in the Court's analysis of the Act's purpose—which is to say, at least *some* role.) That provision lists five purposes for which DNA samples may be tested. By this point, it will not surprise the reader to learn that the Court's imagined purpose is not among them.

Instead, the law provides that DNA samples are collected and tested, as a matter of Maryland law, "as part of an official investigation into a crime." § 2–505(a)(2). (Or, as ***475** our suspicionless-search cases would put it: for ordinary law-enforcement purposes.) That is certainly how everyone has always understood the Maryland Act until today. The Governor of Maryland, in commenting on our decision to hear this case, said that he was glad, because "[a]llowing law enforcement to collect DNA samples ... is absolutely critical to our efforts to continue driving down crime," and "bolsters our efforts to resolve open investigations and bring them to a resolution." Marbella, Supreme Court Will Review Md. DNA Law, Baltimore Sun, Nov. 10, 2012, pp. 1, 14. The attorney general of Maryland remarked that he "look[ed] forward to the opportunity to defend this important crime-fighting tool," and praised the DNA database for helping to "bring to justice violent perpetrators." *Ibid.* Even this Court's order staying the decision below states that the statute "provides a valuable tool for investigating unsolved crimes and thereby helping to remove violent offenders from the general population"—with, unsurprisingly, no mention of identity. ****1986** 567 U.S. ——, ——, 133 S.Ct. 1, 3, 183 L.Ed.2d 667 (2012) (ROBERTS, C.J., in chambers).

More devastating still for the Court's "identification" theory, the statute *does* enumerate two instances in which a DNA sample may be tested for the purpose of identification: "to help identify *human remains,*" § 2–505(a)(3) (emphasis added), and "to help identify *missing individuals,*" § 2–505(a)(4) (emphasis added). No mention of identifying arrestees. *Inclusio unius est exclusio alterius*. And note again that Maryland forbids using DNA records "for any purposes other than those specified"—it is actually a crime to do so. § 2–505(b)(2).

The Maryland regulations implementing the Act confirm what is now monotonously obvious: These DNA searches have nothing to do with identification. For example, if someone is arrested and law enforcement determines that "a convicted offender Statewide DNA Data Base sample already exists" for that arrestee, "the agency is not required to obtain a new sample." ***476** Code of Md. Regs., tit. 29, § 05.01.04(B)(4) (2011). But how could the State know if an arrestee has already had his DNA sample collected, if the point of the sample is to identify who he is? Of course, if the DNA sample is instead taken in order to investigate crimes, this restriction makes perfect sense: Having previously placed an identified someone's DNA on file to check against available crime-scene evidence, there is no sense in going to the expense of taking a new sample. Maryland's regulations further require that the "individual collecting a sample ... verify the identity of the individual from whom a sample is taken by name and, if applicable, State identification (SID) number." § 05.01.04(K). (But how?) And after the sample is taken, it continues to be identified *by* the individual's name, fingerprints, etc., see § 05.01.07(B)—rather than (as the Court believes) being used *to identify* individuals. See § 05.01.07(B)(2) ("Records and specimen information shall *be identified by* ... [the] [n]ame of the donor" (emphasis added)).

So, to review: DNA testing does not even begin until after arraignment and bail decisions are already made. The samples sit in storage for months, and take weeks to test. When they are tested, they are checked against the Unsolved Crimes Collection—rather than the Convict and Arrestee Collection, which could be used to identify them. The Act forbids

the Court's purpose (identification), but prescribes as its purpose what our suspicionless-search cases forbid ("official investigation into a crime"). Against all of that, it is safe to say that if the Court's identification theory is not wrong, there is no such thing as error.

II

The Court also attempts to bolster its identification theory with a series of inapposite analogies. See *ante,* at 1974 – 1977.

Is not taking DNA samples the same, asks the Court, as taking a person's photograph? No—because that is not a Fourth Amendment search at all. It does not involve a ***477** physical intrusion onto the person, see *Florida v. Jardines,* 569 U.S. 1, ——, 133 S.Ct. 1409, 1413–1414, 185 L.Ed.2d 495 (2013), and we have never held that merely taking a person's photograph invades any recognized "expectation of privacy," see *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). Thus, it is unsurprising that the cases the Court cites as authorizing photo-taking do not even mention the Fourth Amendment. See *State ex rel. Bruns v. Clausmier,* 154 Ind. 599, 57 N.E. 541 (1900) (libel), ****1987** *Shaffer v. United States,* 24 App.D.C. 417 (1904) (Fifth Amendment privilege against self-incrimination).

But is not the practice of DNA searches, the Court asks, the same as taking "Bertillon" measurements—noting an arrestee's height, shoe size, and so on, on the back of a photograph? No, because that system was not, in the ordinary case, used to solve unsolved crimes. It is possible, I suppose, to imagine situations in which such measurements might be useful to generate leads. (If witnesses described a very tall burglar, all the "tall man" cards could then be pulled.) But the obvious primary purpose of such measurements, as the Court's description of them makes clear, was to verify that, for example, the person arrested today is the same person that was arrested a year ago. Which is to say, Bertillon measurements were *actually* used as a system of identification, and drew their primary usefulness from that task. [3]

It is on the fingerprinting of arrestees, however, that the Court relies most heavily. *Ante,* at 1975 – 1977. The Court does not actually say whether it believes that taking a person's fingerprints is a Fourth Amendment search, and our cases provide no ready answer to that question. Even assuming so, however, law enforcement's post-arrest use of fingerprints ***478** could not be more different from its post-arrest use of DNA. Fingerprints of arrestees are taken primarily to identify them (though that process sometimes solves crimes); the DNA of arrestees is taken to solve crimes (and nothing else). Contrast CODIS, the FBI's nationwide DNA database, with IAFIS, the FBI's Integrated Automated Fingerprint Identification System. See FBI, Integrated Automated Fingerprint Identification System, http://www.fbi.gov/about-us/cjis/fingerprints_ biometrics/iafis/iafis (hereinafter *IAFIS*).

Fingerprints	DNA Samples
The "average response time for an electronic criminal fingerprint submission is about 27 minutes." *IAFIS*.	DNA analysis can take months —far too long to be useful for identifying someone.
IAFIS includes detailed identification information, including "criminal histories; mug shots; scars and tattoo photos; physical characteristics like height, weight, and hair and eye color."	CODIS contains "[n]o names or other personal identifiers of the offenders, arrestees, or detainees." See CODIS and NDIS Fact Sheet.
"Latent prints" recovered from crime scenes are not systematically compared against the database of known	The entire *point* of the DNA database is to check crime scene evidence against the profiles of arrestees and convicts as they come in.

fingerprints, since that requires further forensic work. [4]

**1988 *479 The Court asserts that the taking of fingerprints was " constitutional for generations prior to the introduction" of the FBI's rapid computer-matching system. *Ante,* at 1977. This bold statement is bereft of citation to authority because there is none for it. The "great expansion in fingerprinting came before the modern era of Fourth Amendment jurisprudence," and so we were never asked to decide the legitimacy of the practice. *United States v. Kincade,* 379 F.3d 813, 874 (C.A.9 2004) (Kozinski, J., dissenting). As fingerprint databases expanded from convicted criminals, to arrestees, to civil servants, to immigrants, to everyone with a driver's license, Americans simply "became accustomed to having our fingerprints on file in some government database." *Ibid.* But it is wrong to suggest that this was uncontroversial at the time, or that this Court blessed universal fingerprinting for "generations" before it was possible to use it effectively for identification.

The Court also assures us that "the delay in processing DNA from arrestees is being reduced to a substantial degree by rapid technical advances." *Ante,* at 1977. The idea, presumably, is that the snail's pace in this case is atypical, so that DNA is now readily usable for identification. The Court's proof, however, is nothing but a pair of press releases —each of which turns out to undercut this argument. We learn in them that reductions in backlog have enabled Ohio and Louisiana crime labs to analyze a submitted DNA sample in twenty days. [5] But that is *still longer* than the *eighteen* days that Maryland needed to analyze King's sample, *480 once it worked its way through the State's labyrinthine bureaucracy. What this illustrates is that these times do not take into account the many other sources of delay. So if the Court means to suggest that Maryland is unusual, that may be right—it may qualify in this context as a paragon of efficiency. (Indeed, the Governor of Maryland was hailing the elimination of that State's backlog more than five years ago. See Wheeler, O'Malley Wants to Expand DNA Testing, Baltimore Sun, Jan. 11, 2008, p. 5B.) Meanwhile, the Court's holding will result in the dumping of a large number of arrestee samples—many from minor offenders—onto an already overburdened system: Nearly one-third of Americans will be arrested for some offense by age 23. See Brame, Turner, Paternoster, & Bushway, Cumulative Prevalence of Arrest From Ages 8 to 23 in a National Sample, 129 Pediatrics 21 (2011).

The Court also accepts uncritically the Government's representation at oral argument that it is developing devices that will be able to test DNA in mere minutes. At most, this demonstrates that it may one day be possible to design a program that uses DNA for a purpose other than crime-solving—not that Maryland has in fact designed such a program today. And that is the main point, which the Court's discussion of the brave new world of instant DNA analysis should not obscure. The issue before us is not whether DNA can *some day* be used for identification; nor even whether it can *today* be used for **1989 identification; but whether it *was used for identification here.*

Today, it can fairly be said that fingerprints really are used to identify people—so well, in fact, that there would be no need for the expense of a separate, wholly redundant DNA confirmation of the same information. What DNA adds—what makes it a valuable weapon in the law-enforcement arsenal—is the ability to solve unsolved crimes, by matching old crime-scene evidence against the profiles of people whose identities are already known. That is what was going on when King's *481 DNA was taken, and we should not disguise the fact. Solving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches. The Fourth Amendment must prevail.

* * *

The Court disguises the vast (and scary) scope of its holding by promising a limitation it cannot deliver. The Court repeatedly says that DNA testing, and entry into a national DNA registry, will not befall thee and me, dear reader, but only those arrested for "serious offense[s]." *Ante,* at 1979 – 1980; see also *ante,* at 1965, 1969 – 1970, 1972 – 1973, 1974, 1976 – 1977, 1977, 1977 – 1978 (repeatedly limiting the analysis to "serious offenses"). I cannot imagine what principle could possibly justify this limitation, and the Court does not attempt to suggest any. If one believes that DNA will "identify" someone arrested for assault, he must believe that it will "identify" someone arrested for a traffic offense. This Court does not base its judgments on senseless distinctions. At the end of the day, *logic will out.* When there comes before us the taking of DNA from an arrestee for a traffic violation, the Court will predictably (and quite rightly) say, "We can find

no significant difference between this case and *King*." Make no mistake about it: As an entirely predictable consequence of today's decision, your DNA can be taken and entered into a national DNA database if you are ever arrested, rightly or wrongly, and for whatever reason.

The most regrettable aspect of the suspicionless search that occurred here is that it proved to be quite unnecessary. All parties concede that it would have been entirely permissible, as far as the Fourth Amendment is concerned, for Maryland to take a sample of King's DNA as a consequence of his conviction for second-degree assault. So the ironic result of the Court's error is this: The only arrestees to whom the outcome here will ever make a difference are those ***482** who *have been acquitted* of the crime of arrest (so that their DNA could not have been taken upon conviction). In other words, this Act manages to burden uniquely the sole group for whom the Fourth Amendment's protections ought to be most jealously guarded: people who are innocent of the State's accusations.

Today's judgment will, to be sure, have the beneficial effect of solving more crimes; then again, so would the taking of DNA samples from anyone who flies on an airplane (surely the Transportation Security Administration needs to know the "identity" of the flying public), applies for a driver's license, or attends a public school. Perhaps the construction of such a genetic panopticon is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection.

I therefore dissent, and hope that today's incursion upon the Fourth Amendment, ****1990** like an earlier one,[6] will some day be repudiated.

All Citations

569 U.S. 435, 133 S.Ct. 1958, 186 L.Ed.2d 1, 81 USLW 4343, 13 Cal. Daily Op. Serv. 5551, 2013 Daily Journal D.A.R. 6991, 24 Fla. L. Weekly Fed. S 234

Footnotes

* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.,* 200 U.S. 321, 337, 26 S.Ct. 282, 50 L.Ed. 499.

1 The Court's insistence (*ante,* at 1978) that our special-needs cases "do not have a direct bearing on the issues presented in this case" is perplexing. Why spill so much ink on the special need of identification if a special need is not required? Why not just come out and say that any suspicionless search of an arrestee is allowed if it will be useful to solve crimes? The Court does not say that because most Members of the Court do not believe it. So whatever the Court's major premise—the opinion does not really contain what you would call a rule of decision—the *minor* premise is "this search was used to identify King." The incorrectness of that minor premise will therefore suffice to demonstrate the error in the Court's result.

2 By the way, this procedure has nothing to do with exonerating the wrongfully convicted, as the Court soothingly promises. See *ante,* at 1974. The FBI CODIS database includes DNA from *unsolved* crimes. I know of no indication (and the Court cites none) that it also includes DNA from all—or even any—crimes whose perpetrators have already been convicted.

3 Puzzlingly, the Court's discussion of photography and Bertillon measurements repeatedly cites state cases (such as *Clausmier*) that were decided before the Fourth Amendment was held to be applicable to the States. See *Wolf v. Colorado,* 338 U.S. 25, 69 S.Ct. 1359, 93 L.Ed. 1782 (1949); *Mapp v. Ohio,* 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961). Why the Court believes them relevant to the meaning of that Amendment is therefore something of a mystery.

4 See, *e.g.,* FBI, Privacy Impact Assessment: Integrated Automated Fingerprint Identification System (IAFIS)/ Next Generation Identification (NGI) Repository for Individuals of Special Concern (RISC), http://www.fbi. gov/ foia/privacy-impact-assessments/iafis-ngi-risc (searches of the "Unsolved Latent File" may "take considerably more time").

5 See Attorney General DeWine Announces Significant Drop in DNA Turnaround Time (Jan. 4, 2013), http://ohioattorneygeneral.gov/Media/News–Releases/January–2013/Attorney–General–DeWine–Announces–Significant–Drop; Gov. Jindal Announces Elimination of DNA Backlog (Nov. 17, 2011), http:// www.gov.state.la.us/index.cfm?md=newsroom&tmp =detail&articleID=3102.

6 Compare, *New York v. Belton,* 453 U.S. 454, 101 S.Ct. 2860, 69 L.Ed.2d 768 (1981) (suspicionless search of a car permitted upon arrest of the driver), with *Arizona v. Gant,* 556 U.S. 332, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009) (on second thought, no).

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

PLAYLIST

NATIONAL

A woman whose rape DNA led to her arrest sues the city of San Francisco

September 13, 2022 · 10:56 AM ET

THE ASSOCIATED PRESS



Attorneys Adanté Pointer (left) and Patrick Buelna, who represent a woman whose DNA from a sexual assault case was used by San Francisco police to arrest her in an unrelated crime, speak during a news conference announcing their lawsuit against the city on Monday.

Jeff Chiu/AP

SAN FRANCISCO — A rape victim whose DNA from her sexual assault case was used by San Francisco police to arrest her in an unrelated property crime on Monday filed a lawsuit against the city.

During a search of a San Francisco Police Department crime lab database, the woman's DNA was tied to a burglary in late 2021. Her DNA had been collected and stored in the system as part of a 2016 domestic violence and sexual assault case, then-District Attorney Chesa Boudin said in February in a shocking revelation that raised privacy concerns.



LAW

San Francisco DA drops charges against woman linked to crime through rape victim DNA

"This is government overreach of the highest order, using the most unique and personal thing we have – our genetic code – without our knowledge to try and connect us to crime," the woman's attorney, Adante Pointer, said in a statement.

The revelation prompted a national outcry from advocates, law enforcement, legal experts and lawmakers. Advocates said the practice could affect victims' willingness to come forward to law enforcement authorities.

Federal law already prohibits the inclusion of victims' DNA in the national Combined DNA Index System. There is no corresponding law in California to prohibit local law enforcement databases from retaining victims' profiles and searching them years later for entirely different purposes.

Sponsor Message

California moves to ban using rape DNA for unrelated cases

California lawmakers last month approved a bill that would prohibit using the DNA profiles collected by police from sexual assault survivors and other victims for any purpose other than aiding in identifying the perpetrator. Local law enforcement agencies would also be prohibited from retaining and then searching victim DNA to incriminate them in unrelated crimes under the legislation, which is pending before Gov. Gavin Newsom.



NATIONAL

S.F. police face criticism for using rape victims' DNA to identify potential suspects

Boudin said the report was found among hundreds of pages of evidence against a woman who had been recently charged with a felony property crime. After learning the source of the DNA evidence, Boudin dropped the felony property crime charges against the woman.

The police department's crime lab stopped the practice shortly after receiving a complaint from the district attorney's office and formally changed its operating procedure to prevent the misuse of DNA collected from sexual assault victims, Police Chief Bill Scott said.

Scott said at a police commission meeting in March that he had discovered 17 crime victim profiles, 11 of them from rape kits, that were matched as potential suspects using a crime victims database during unrelated investigations. Scott said he believes the only person arrested was the woman who filed the lawsuit Monday.

Sponsor Message

The woman filed the lawsuit under the alias of Jane Doe to protect her privacy, Pointer said The Associated Press generally does not name people who say they have been sexually assaulted unless they choose to be named.

California allows local law enforcement crime labs to operate their own forensic databases that are separate from federal and state databases. The law also lets municipal labs perform forensic analysis, including DNA profiling, and use those databases — without regulation by the state or others.

rape kit san francisco

What makes us different

Financial independence means we can focus on the truth and tell stories that would otherwise not be told. As a nonprofit, your support is our greatest strength. You experience that difference in our exceptional news and programming. You make it possible.

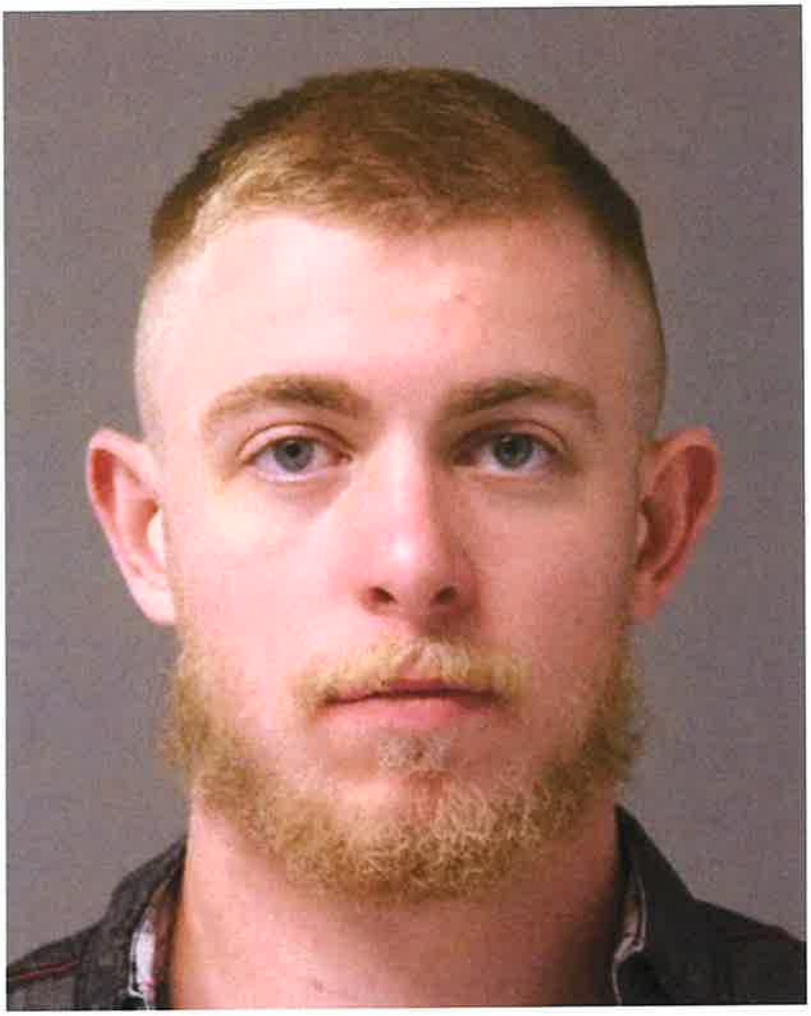
DONATE NOW

More Stories From NPR

https://www.wdel.com/news/new-castle-county-police-make-arrest-in-2016-murder/article_ab50166a-f8e1-11e8-954f-835a8aef94b2.html

New Castle County Police make arrest in 2016 murder

Joe Irizarry
Dec 5, 2018 - 6:01 pm



An arrest has been made in a Darley Woods homicide--almost two years to the day it happened.

New Castle County Police arrested Seth Kinderman, 22, in the death of Jakeith Latham, 34, of Clayton, New Jersey.

On December 20, 2016, officers went to the 1000 block of Linda Road in the Darley Woods community after a witness called 911 to report an unconscious man on the sidewalk. The victim, Latham, was found with a gunshot wound to his upper body.

Multiple investigative leads led police to Kinderman, and he was arrested on December 5, 2018.

Kinderman was charged with first-degree murder, first-degree felony robbery, and two counts of possession of a firearm during the commission of a felony.

> "Our thoughts and prayers remain with Mr. Latham's family as they continue to cope with his passing," said Chief of Police Col. Vaughn M. Bond, Jr. in a statement. "Mr. Latham was an upstanding young man with a promising future whose life ended in a senseless act of violence. I remain extremely grateful for the dedication, perseverance, and commitment that our officers have shown throughout this nearly two-year long investigation. I hope that the Latham family will find some sense of peace knowing that the person responsible for this crime has been apprehended."

Kinderman was arraigned at Justice of the Peace Court 2, and he is being held on more than $1 million cash bail.

delaware online

CRIME

County arrests suspect in 2016 Brandywine Hundred homicide



Josephine Peterson
The News Journal

Published 7:47 p.m. ET Dec. 5, 2018 | **Updated 8:09 p.m. ET Dec. 5, 2018**

County police made an arrest Wednesday related to a New Jersey man killed in 2016.

A 34-year-old from New Jersey was found dead lying on the sidewalk in the 1000 block of Linda Road. Jakeith Latham had been shot in his upper body in December 2016, Master Cpl. Michel Eckerd of New Castle County Police said.

More: Police ID NJ man found shot to death in Darley Woods

Seth Kinderman, a 22-year-old from the Elsmere-area, was charged Wednesday with first-degree murder, first-degree felony robbery, two counts of possession of a firearm during the commission of a felony.

Kinderman was jailed on $1,180,000 cash bail.

"I hope that the Latham family will find some sense of peace knowing that the person responsible for this crime has been apprehended," stated Colonel Vaughn M. Bond, Jr.

Bond asks the county to come forward with any information on unsolved homicides.

SHOOTING SUSPECTS:

Police looking for Seaford shooting suspect

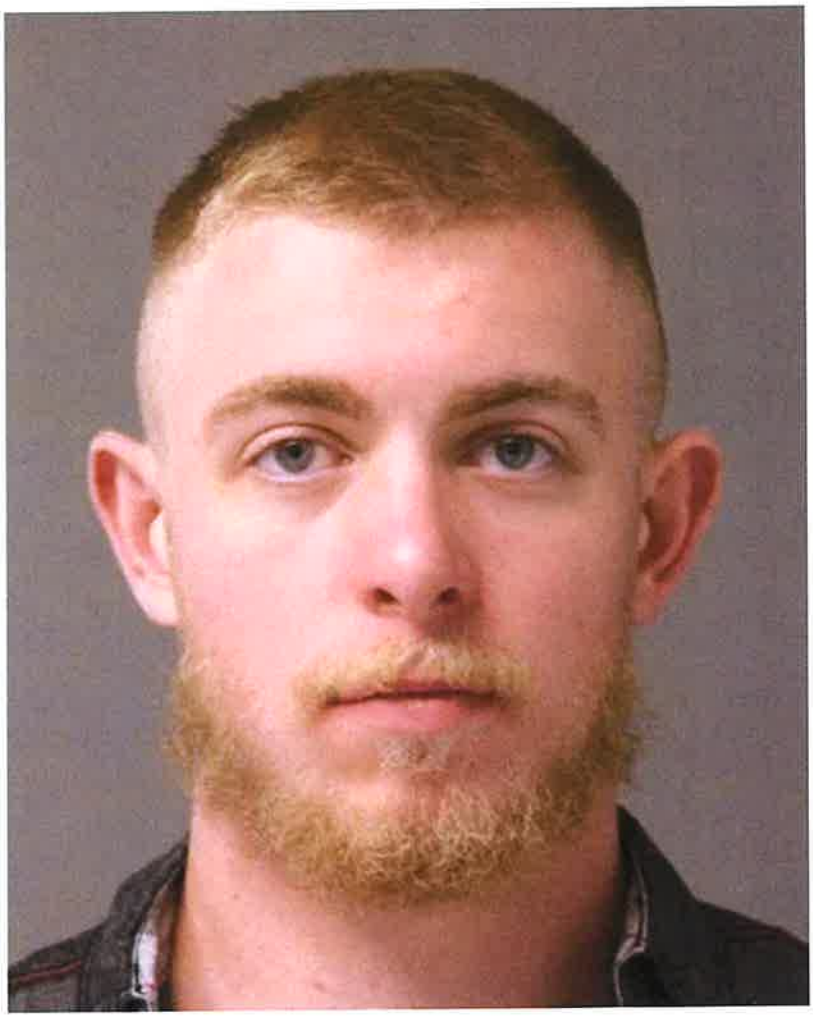
26-year-old Wilmington man charged with October shooting

Contact Josephine Peterson at (302) 324-2856 or jhpeterson@delawareonline.com. Follow her @jopeterson93.

https://www.wdel.com/news/wilmington-man-gets-38-years-for-killing-victim-during-2016-parking-lot-diabetic-testing-strip/article_d6779692-fc6b-11ec-b6f2-239cd886cdf8.html

Wilmington man gets 38 years for killing victim during 2016 parking lot diabetic testing strip sale

DJ McAneny
Jul 5, 2022 - 10:23 am



A 25-year-old Wilmington man received 38 years in prison for arranging the sell a victim diabetic test strip kits, then murdering him when he showed up to the site of the sale.

According to the Delaware Department of Justice, Seth Kinderman was convicted of second-degree murder, possession of a firearm during commission of a felony, and first-degree attempted robbery in the shooting death of Jakeith Latham, 34, of Clayton, New Jersey, in the 1000 block of Linda Road in the Darley Woods community on December 20, 2016.

Authorities said after Kinderman killed Latham, he drove the victim's vehicle to a nearby neighborhood, dumped the body, and attempted to set the vehicle on fire. The case went cold for two years, but after New Castle County Police obtained genetic evidence through a genealogy testing service, Kinderman was arrested and charged on December 5, 2018.

"This was fantastic work by our partners at New Castle County PD," said Attorney General Kathy Jennings. "Cold cases – particularly cases that have gone cold for years – are difficult to crack. We are here today because of the tenacity and ingenuity of New Castle County PD, whose use of this new technology is a testament to modern policing. Their work has brought closure to this case; our thoughts now are with the victim's family, whom I hope find peace."



New Castle County Police make arrest in 2016 murder

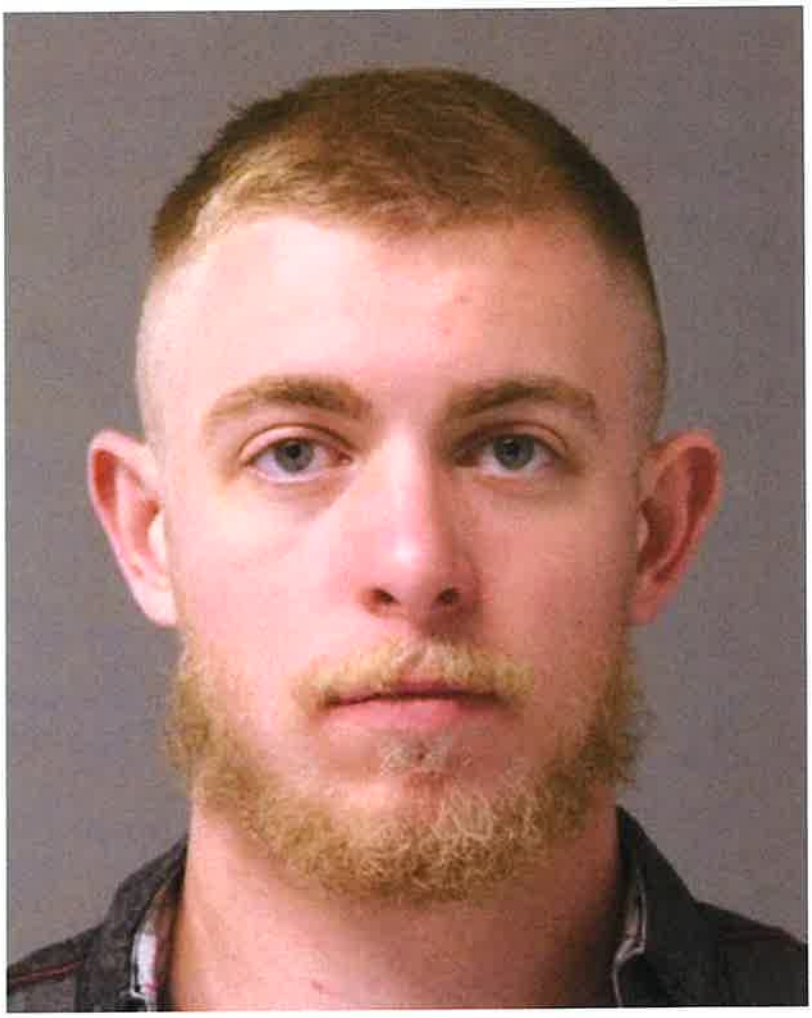
DJ McAneny
Digital Editor

Digital Editor for WDEL.com, with more than a decade's worth of experience crafting the news for the online landscape. Please note new email address: dmcaneny@forevermediainc.com.

https://www.wdel.com/news/wilmington-man-gets-38-years-for-killing-victim-during-2016-parking-lot-diabetic-testing-strip/article_d6779692-fc6b-11ec-b6f2-239cd886cdf8.html

Wilmington man gets 38 years for killing victim during 2016 parking lot diabetic testing strip sale

DJ McAneny
Jul 5, 2022 - 10:23 am



A 25-year-old Wilmington man received 38 years in prison for arranging the sell a victim diabetic test strip kits, then murdering him when he showed up to the site of the sale.

According to the Delaware Department of Justice, Seth Kinderman was convicted of second-degree murder, possession of a firearm during commission of a felony, and first-degree attempted robbery in the shooting death of Jakeith Latham, 34, of Clayton, New Jersey, in the 1000 block of Linda Road in the Darley Woods community on December 20, 2016.

Authorities said after Kinderman killed Latham, he drove the victim's vehicle to a nearby neighborhood, dumped the body, and attempted to set the vehicle on fire. The case went cold for two years, but after New Castle County Police obtained genetic evidence through a genealogy testing service, Kinderman was arrested and charged on December 5, 2018.

"This was fantastic work by our partners at New Castle County PD," said Attorney General Kathy Jennings. "Cold cases – particularly cases that have gone cold for years – are difficult to crack. We are here today because of the tenacity and ingenuity of New Castle County PD, whose use of this new technology is a testament to modern policing. Their work has brought closure to this case; our thoughts now are with the victim's family, whom I hope find peace."



New Castle County Police make arrest in 2016 murder

DJ McAneny
Digital Editor

Digital Editor for WDEL.com, with more than a decade's worth of experience crafting the news for the online landscape. Please note new email address: dmcaneny@forevermediainc.com.

delaware online

CRIME

Cold case murder defendant gets 38-year sentence



Xerxes Wilson
Delaware News Journal

Published 4:33 p.m. ET July 5, 2022 | **Updated 12:38 p.m. ET July 7, 2022**

A New Castle County man has been sentenced to 38 years in prison for the 2016 killing of Jakeith Latham near Claymont.

Delaware Department of Justice prosecutors said that evidence showed Seth Kinderman set up a transaction to sell Latham diabetic test strips but instead shot him when he arrived. The 34-year-old from New Jersey was found dead, lying on the sidewalk in the 1000 block of Linda Road.

Prosecutors said in a news release that Kinderman then drove the victim's vehicle to a nearby neighborhood where he "discarded" the body and attempted to set fire to the vehicle. Kinderman was not arrested until roughly two years after the murder. Prosecutors said genetic evidence "secured" through a "genealogy testing service" ultimately cracked the case.

Kinderman pleaded guilty to charges including second-degree murder, attempted robbery and a weapons charge. He was sentenced on Friday.

2021 WL 4851971
Only the Westlaw citation is currently available.

UNPUBLISHED OPINION. CHECK COURT RULES BEFORE CITING.

Superior Court of Delaware.

STATE of Delaware,
v.
Kwesi HUDSON, Defendant.

ID NO. 1809009750
|
Date Submitted: September 27, 2021
|
Date Decided: October 15, 2021

Upon the Defendant's Motion in Limine. **DENIED**.

Attorneys and Law Firms

John W. Downs, Esquire, and Jenna Milecki, Enquire, Deputy Attorney Generals, Department of Justice, Wilmington, Delaware, Attorneys for the State of Delaware.

Raymond Armstrong, Esquire, Wilmington, Delaware, Attorney for Defendant.

ORDER

SCOTT, J.

INTRODUCTION

***1** Before the Court is Defendant Kwesi Hudson's ("Mr. Hudson") Motion in *Limine* pursuant to Delaware Rule of Evidence 401, 402, 403, and 702 and *Daubert v. Merrell Dow Pharmaceuticals, Inc* [1] (the "Motion"). After reviewing the Motion and the State of Delaware's (the "State") Response, Mr. Hudson's Motion is **DENIED.**

BACKGROUND

On February 13, 2017, in North Wilmington, Mr. Hudson approached victim, L.M., at her apartment and forced her, at gunpoint, into her car. Mr. Hudson sexually assaulted L.M. and drove her to three banks to withdraw cash from the ATMs.

On February 19, 2017, in the area of Route 7 in Wilmington, Mr. Hudson approached victim S.C. and forced her into her apartment at gunpoint. Mr. Hudson sexually assaulted S.C. with the firearm he carried. Mr. Hudson then forced S.C. into her car and drove her to four banks to withdraw cash from the ATMs. The victim fled at the last stop and escaped.

On March 6, 2017, in the Pike Creek area of Wilmington, Mr. Hudson approached victim J.B. and attempted to force her into her apartment at gunpoint. J.B.'s boyfriend come to the door Mr. Hudson fled the scene.

The Delaware State Police and New Castle County Police, as well as law enforcement in Pennsylvania, believed Mr. Hudson committed several robberies in Delaware and Pennsylvania.

On May 9, 2017, Mr. Hudson committed a robbery at a pharmacy in Upper Chichester, PA. Police found a black ski mask and pellet gun near the scene. Upon DNA analysis for the ski mask, it was determined the DNA found on the mask matched Mr. Hudson's known DNA sample.

On May 24, 2017, Mr. Hudson committed a robbery at a pharmacy in Media, PA. Police apprehended him and took him into custody.

Upon investigation, Mr. Hudson was identified as a suspect in the three sexual assaults and robberies on female victims from February – March of 2017.

On July 13, 2018, the pellet gun left behind at the Upper Chichester pharmacy robbery and known DNA samples from victims L.M., S.C., and J.B. was submitted to DNA Labs International.

DNA Labs International used probabilistic genotyping method, STRmix™ ("STRmix") on the sample which contained multiple DNA samples, known as mixture DNA. In the Lab's report, dated August 15, 2018, it stated "The DNA profile obtained from the extract is approximately 320 trillion times more probable if the sample originated from [victim S.C.] ... and two unknown person than if it originated from three unknown persons. Therefore, there is extremely strong support than [S.C.] and two unknown persons contributed to this DNA profile, rather than three known persons."

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

PARTIES' ASSERTIONS

A. The State

The State intends to introduce expert testimony on the DNA mixture evidence report from DNA Labs International. The State intends to call Alicia M. Cadenas ("Ms. Cadenas"), a Forensic DNA Analyst who worked on and completed the report in contention between the parties. The report found "The DNA profile obtained from the extract is approximately 320 trillion times more probable if the sample originated from [victim S.C.] and two unknown persons than if it originated from three unknown persons. Therefore, there is extremely strong support [victim S.C.] and two unknown persons contributed to this DNA profile, rather than three unknown persons."

B. Mr. Hudson

***2** Mr. Hudson argues the introduction of such expert testimony would violate D.R.E. 401, 402, 403, and 702. Mr. Hudson further asserts, with respect to a Daubert analysis, the conclusions made by DNA Labs International on the mixture DNA analysis are based on "unfounded and unsupported pseudoscience," based on "a lab technician's interpretation of unknown mathematical computation" and the probability results are not based on "concrete or scientifically accepted practices." To buttress these claims, Mr. Hudson relies solely on the "KEY TAKEWAY" statements made in the first nine pages of the two-hundred-fifty-page draft report titled, "DNA Mixture Interpretation: A NIST Scientific Foundation Review" (the "NIST Report")[2]. Mr. Hudson uses these generalized KEY TAKEAWAY points about mixture DNA analysis in an attempt to undermine the DNA mixture analysis of a specific probabilistic genotyping method, STRmix.

STANDARD OF REVIEW

Delaware Rule of Evidence 702 (D.R.E. 702) governs the admissibility of expert testimony and provides as follows:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
>
> (a) The expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
>
> (b) The testimony is based upon sufficient facts or data;
>
> (c) The testimony is the product of reliable principles and methods; and
>
> (d) The expert has reliably applied the principles and methods to the facts of the case.[3]

D.R.E. 702 is substantially similar to Federal Rule of Evidence 702,[4] which is governed by *Daubert v. Merrell Dow Pharmaceuticals, Inc.*,[5] and *Kumho Tire Co.*, Ltd. v. Carmichael.[6] In Daubert, the United States Supreme Court held that F.R.E. 702 requires the trial judge to act as a "gatekeeper" and determine whether the proffered expert testimony is not only relevant, but reliable.[7] The factors considered in this determination are "meant to be helpful, not definitive, and may or may not be pertinent depending on the nature of the issue, an expert's particular expertise, and the subject of the testimony."[8] Those factors include:

> (1) whether a theory or technique has been tested;
>
> (2) whether it has been subjected to peer review and publication;
>
> (3) whether a technique had a high known or potential rate of error and whether there are standards controlling its operation; and
>
> (4) whether the theory or technique enjoys general acceptance within a relevant scientific community.[9]

The focus of the Daubert analysis does not concern the resulting conclusions but rather the principles and methodology used to form the expert's opinion.[10]

In addition to the Daubert analysis, the Delaware Supreme Court created a five-prong test in determining the admissibility of scientific or technical expert's testimony. Therefore, this Court must also determine whether:[11]

> ***3** 1. The witness is qualified;[12]
>
> 2. The evidence is otherwise admissible, relevant, and reliable;[13]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

3. The bases for the opinion are those reasonably relied upon by experts in the field; [14]

4. The specialized knowledge being offered will assist the trier of fact to understand the evidence or determine a fact in issue; [15] and

5. The evidence does not create unfair prejudice, confuse the issues, or mislead the jury. [16]

"[T]he proponent of the proffered expert testimony bears the burden of establishing the relevance, reliability, and admissibility by a preponderance of the evidence." [17] However, the proponent must only demonstrate that the expert's opinions are reliable. [18] Thus, where an expert's opinion is challenged, "the trial judge must decide if the expert's testimony 'has a reliable basis in the knowledge and experience of the relevant discipline.' " [19]

DISCUSSION

By providing only a draft of the NIST Report, Mr. Hudson contends the expert testimony regarding the conclusions made by DNA Labs International are based on "unfounded and unsupported pseudoscience," based on "a lab technician's interpretation of unknown mathematical computation" and the probability results are not based on "concrete or scientifically accepted practices." For these reasons, Mr. Hudson requests to exclude DNA Labs International's Technician, Alicia M. Cadenas, from testifying. He simply copies the generalized "KEY TAKEAWAY" statements made in the first ten pages of the NIST Report.

In the States response to Mr. Hudson's Motion, the State submits an Affidavit from DNA Labs International ("DNA Labs Affidavit"). Therein, Rachel H. Oefelein, Director of Research & Innovation/Quality Assurance Manager/Senior DNA Analyst, and Cristina L. Rentas, Technical Leader/ Training Manager/Senior DNA Analyst for DNA Labs, refute Mr. Hudson's generalized points made in the Motion. The analysts not only attest to STRmix's reliability and internal validations, but also, they comment on every "KEY TAKEWAY." The DNA Labs affidavit speaks to how the method is tested used "lab-created mixtures" to gauge the reliability of the technology.

In addition to the DNA Labs Affidavit, the State attaches providing comments to NIST Article from the Scientific Working Group on DNA Analysis Methods (SWGDAM), the New York City Office of the Chief Medical Examiner, the National Institute of Standards and Technology, the Institute of Environmental Science and Research Limited, New Zealand, and the American Society of Criminal Laboratory Directors, Inc. All the organizations mentioned had concerns regarding the findings of the NIST Article, as well as harsh criticisms.

***4** Mr. Hudson has not refuted or responded to anything in the DNA Labs Affidavit, any comments made by organizations about the NIST article, or the assertion STRmix has been accepted in many other jurisdictions.

Daubert Factors Are Satisfied

This Court finds STRmix satisfies the Daubert Factors. In *United States v. Gissantaner*, the Sixth Circuit was tasked with applying the four inquiries required of Daubert to the same probabilistic genotyping software program present in this case, STRmix. Upon a lengthy analysis of the required factors, the court found "All in all, STRmix satisfies Rule 702 and the case law construing it. In the words of Rule 702, it is the 'product of reliable principles and methods.' " [20] This Court adopts the analysis and conclusion of the Federal Appellate Court as the same software and caselaw factors applied.

The five-prong test in determining the admissibility of scientific or technical expert's testimony is satisfied

Given Mr. Hudson's ground of contention with the expert testimony, the Court must focus on the first and third factors of Delaware Rule 703's five step analysis mentioned above: (1) the qualifications of the expert to testify and (3) the bases for the expert's opinion are those reasonably relied upon by experts in the field.

Ms. Cadenas' expert opinions are (1) relevant, (2) will assist the fact finder, and (3) will not create unfair prejudice.

In this Court's opinion, there is no doubt Ms. Cadenas' expert opinions satisfy the second (relevance), fourth (assistance to the fact finder) and fifth (avoidance of unfair prejudice) factors examined under the five-step admissibility analysis. [21] Expert testimony is relevant if it assists the fact finder in "understand[ing] the evidence or ... determin[ing] a

fact in issue." [22] And evidence creates unfair prejudice when it invites a decision on an improper basis, commonly, emotion rather than reason. [23]

Ms. Cadenas' testimony is relevant to understanding the DNA analysis from a swab taken from a gun, which was alleged to be belonging to Mr. Hudson. The testimony will assist the fact finder in understanding the results of the report and the method in which the sample was taken and analyzed. Mr. Hudson has not suggested Ms. Cadenas testimony will create any unfair prejudice. The fact finder may credit Ms. Cadenas testimony, or it may not. However, nothing in the record suggests Ms. Cadenas' testimony will appeal to or persuade the jury on any improper bias.

Ms. Cadenas is qualified to give her opinion.

Ms. Cadenas is qualified to give her opinion about DNA Labs International's use of STRmix based on her knowledge and expertise as a DNA Analyst, her education in forensic science, and her review and work on the DNA sample at issue here. A trial judge acts as a gatekeeper in deciding whether an expert "has a reliable basis in the knowledge and experience of [the relevant] discipline." [24] Delaware recognizes that an expert may be qualified by credentials outside of her formal training or designated specialty, and in determining admissibility, her qualifications must be scrutinized with "due regard" for the specialization of modern science. [25] And certainly, where appropriate, an expert might be rejected when her education, training, and experience doesn't align with the subject matter of the anticipated testimony. [26]

***5** Ms. Cadenas holds a M.S. in Forensic Science. She has worked in DNA analysis since 2008, is a Technical Leader/ Lab Supervisor/ Senior DNA Analyst for DNA Labs International, and personally performed the DNA analysis and provided a report on the DNA sample at issue in this case. Accordingly, Ms. Cadenas' education, training and experience align with the subject matter of the anticipated testimony. Her professional and practical expertise constitute "knowledge, skill, experience, or education" to allow her to give expert opinion in accordance with Rule 702.

Ms. Cadenas' DNA analysis opinions are reliable as they are based on reliable methodology relied upon by experts in the DNA analysis field.

Mr. Hudson contend Ms. Cadenas' opinions are based on an unreliable methodology, as the findings are based on "unfounded and unsupported pseudoscience," "a lab technician's interpretation of unknown mathematical computation," and the probability results are not based on "concrete or scientifically accepted practices."

When an expert speaks to scientific or specialized knowledge, it will be reliable when the testimony is required to be grounded in scientific methods and procedures and "supported by appropriate validation—i.e., 'good grounds,' based on what is known." [27] The method utilized by STRmix is reliable as there are internal and external validation checks to insure reliability. [28] Despite Mr. Hudson's assertion the results of the DNA analysis rely on "a lab technician's interpretation of unknown mathematical computation[,]" DNA technicians do not author analysis or interpretations. [29] Instead, the author of certificate of analysis in the case is a Senior DNA Analyst and serves as the Director of Research & Innovation and Quality Assurance Manager so results are not based on DNA technician findings. [30] Finally, to Mr. Hudson's contention the results reflect "if" and likelihood ratios rather than "concrete and scientifically accepted practices[,]" likelihood ratios have been used in DNA analysis since the introduction of DNA analysis in the 1980's. [31] The use of likelihood ratios, i.e. using statements including "if" and "than", minimize the risk of confusing the fact finder because the occurrence of "prosecutors' fallacy" and/ or "defense attorney's fallacy" decreases. [32] Ultimately, the likelihood of inadvertently reporting a transposed conditional decreases when likelihood ratios are used. [33] This method of reporting has also been studied extensively in peer reviewed published articles. [34]

Having considered the parties' arguments, this Court finds the methodology used in reaching Ms. Canedas' opinions to be reliable as the method is supported by appropriate validation in the DNA analysis field.

Daubert Hearing is Not Warranted

A Daubert hearing is not mandatory for all experts. [35] "A pretrial procedure of some sort is, however, required. The Judge must gather the necessary information and evaluate the reliability of the underlying principles, the methodology employed by the expert witness, and the potential relevance of the proposed evidence. [internal cite omitted] The Court, in the normal course, should be supplied with the expert's report and the expert's deposition testimony, as well as any

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

supporting affidavits, prior to making any determination as to whether a Daubert hearing is necessary. At that point, the Court should decide: 1) if a Daubert hearing should be held, and 2) on what issues. If, for special reasons, a Daubert hearing is deemed necessary, the Court should try to narrow the issues prior to the evidentiary hearing."[36] Just like in *Minner*, a Daubert hearing is not necessary because no special circumstances exist here, and the parties have provided this Court with sufficient evidentiary basis to perform its "gatekeeping" function.[37]

CONCLUSION

***6** This Court is satisfied in the State established STRmix has been examined and admitted in other courts of competent jurisdiction, particularly where federal courts have applied the Daubert Standard to STRmix and have admitted the testimony. Neither preclusion of the expert from testifying nor a hearing is necessary. Mr. Hudson may make their contentions known concerning the reliability and variability of the STRmix software on cross-examination and through their own expert witnesses if Mr. Hudson so chooses. Nothing in his motion demonstrates that a Daubert hearing, or preclusion of evidence is necessary or warranted, especially considering the DNA Labs Affidavit and the comments made about the draft NIST Article, which demonstrate, for purposes of defeating Mr. Hudson's motion, the STRmix method is scientifically valid and can be applied in this case.

For the reasons stated above, Mr. Hudson's Motion in *Limine* is **DENIED.**

IT IS SO ORDERED.

All Citations

Not Reported in Atl. Rptr., 2021 WL 4851971

Footnotes

1 509 U.S. 579 (1993)

2 The National Institute of Standard and Technology ("NIST") electronically published the NIST Report on June 9, 2021. The report was open for public comments until August 23, 2021, to allow NIST to review the comments before publishing the report in final form. Currently, there remains no final version of the NIST Report. *NIST Publishes Review of DNA Mixture Interpretation Methods*, NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY (June 9, 2021), https://www.nist.gov/news-events/news/2021/06/nist-publishes-review-dna-mixture-interpretation-methods.

3 D.R.E. 702.

4 *See* *M.G. Bancorporation, Inc. v. Le Beau*, 737 A.2d 513, 521 (Del. 1999), as modified on denial of reargument (May 27, 1999) ("Since Delaware Rule of Evidence 702 is identical to its federal counterpart, we rely upon the United States Supreme Court's most recent authoritative interpretation of Federal Rule of Evidence 702.").

5 509 U.S. 579 (1993).

6 526 U.S. 137 (1999).

7 *Daubert*, 509 U.S. at 589.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

8 *Norwood v. State*, 813 A.2d 1141 (Table), 2003 WL 29969, at *2 (Del. 2003).

9 *Daubert*, 509 U.S. at 592-93.

10 *Id.* at 594.

11 *Williams v. Desperito*, 2011 WL 7452803, at *3 (Del. Super. Ct. Oct. 24, 2011) (*citing* *Bowen v. E.I. DuPont de Nemours & Co., Inc.*, 906 A.2d 787, 795 (Del. 2006); *Tolson v. State*, 900 A.2d 639, 645 (Del. 2006)).

12 *See* D.R.E. 702.

13 *See* D.R.E. 401; D.R.E. 402.

14 *See* D.R.E. 703.

15 *See* D.R.E. 702.

16 *See* D.R.E. 403.

17 *Minner v. Am. Mortg. & Guar. Co.*, 791 A.2d 826, 843 (Del. Super. Ct. 2000).

18 *Williams*, 2011 WL 7452803, at *3 (*citing* *In re Asbestos Litig.*, 911 A.2d 1176, 1201 (Del. Super. 2006)).

19 *M.G. Bancorporation*, 737 A.2d at 521 (*citing* *Kumho*, 526 U.S. at 138 (*quoting* *Daubert*, 509 U.S. at 592)).

20 *United States v. Gissantaner*, 990 F.3d 457, 467 (6th Cir. 2021)

21 *Bowen*, 906 A.2d at 795.

22 *Daubert*, 509 U.S. at 591 (quoting Fed. R. Evid. 702).

23 *Henlopen Hotel, Inc. v. United Nat'l Ins. Co.*, 2020 WL 233333, at *5 (Del. Super. Ct. Jan. 10, 2020).

24 *Bowen*, 906 A.2d at 794 (Del. 2006) (*citing* *M.G. Bancorportation, Inc. v. Le Beau*, 737 A.2d 513, 522 (Del. 1999)).

25 *Id.* at 796.

26 *E.g.*, *Spencer v. Wal-Mart Stores East, LP*, 930 A.2d 881, 888-89 (Del. 2007) (affirming this Court's finding that a forensic architect was not qualified as an expert on ice and snow removal).

27 *Daubert*, 509 U.S. at 590.

28 State's Resp. Def's Mot. Limine Ex. B. DNA Labs International Affidavit at p. 2.

29 *Id.* at p. 3.

30 *Id.*

31 *Id.* at p. 1.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

32 *Id.* at p. 3.

33 State's Resp. Def's Mot. Limine Ex. B. DNA Labs International Affidavit at p. 3.

34 *Id.*

35 *Minner v. Am. Mortg. & Guar. Co.*, 791 A.2d 826, 845 (Del. Super. Ct. 2000).

36 *Id.* at 845–46.

37 *Id.* at 846.

End of Document © 2022 Thomson Reuters. No claim to original U.S. Government Works.

2021 WL 211150
Only the Westlaw citation is currently available.

UNPUBLISHED OPINION. CHECK COURT RULES BEFORE CITING.

Superior Court of Delaware.

STATE of Delaware
v.
Jeffrey KING, Defendant.

I.D. No. 1909016237
|
Date Submitted: November 9, 2020
|
Date Decided: January 21, 2021

Upon Defendant's Motion to Suppress Evidence, Amended Motion to Suppress Buccal Swabbing and Motion to Suppress Statements, ***GRANTED in Part and DENIED in Part***

Attorneys and Law Firms

Eric H. Zubrow, Esquire, Erika R. Flaschner, Esquire, Delaware Department of Justice, Wilmington, Delaware, Attorneys for the State.

Kevin J. O'Connell, Esquire, Christina L. Ruggiero, Esquire, Delaware Office of Defense Services, Wilmington, Delaware, Attorneys for Jeffrey King.

DAVIS, J.

I. INTRODUCTION

***1** This is a criminal action. On September 30, 2019, the State of Delaware obtained an indictment against Defendant Jeffrey King charging him with two counts of Unlawful Sexual Intercourse First Degree.

Defendant Jeffrey King has filed three motions to suppress: (i) a Motion to Suppress Evidence seized from Mr. King's residence and vehicle (the "Search Warrant Motion"), (ii) an Amended Motion to Suppress Buccal Swabbing (the "Buccal Swabbing Motion") and (iii) a Motion to Suppress Defendant's Statements (the "*Miranda* Motion"). Mr. King argues that the search of his residence and vehicle violated the Fourth and Fourteenth Amendment of the United States Constitution and Article I, § 6 of the Delaware Constitution Mr. King also contends that a buccal swab taken from him violated the Fourth Amendment of the United States Constitution, Article I, § 6 of the Delaware Constitution and 11 DEL. C. 23. Finally, Mr. King claims that his statements were obtained in violation of *Miranda*. The State opposed, in part, the Search Warrant Motion, the Buccal Swabbing Motion and the Miranda Motion.

On November 9, 2020, the Court held a hearing on the motions. At the conclusion of the hearing, the Court took the motions under advisement. For the reasons set forth below, the Search Warrant and Buccal Swabbing Motions are **DENIED,** and the *Miranda* Motion is **DENIED in part** and **GRANTED in part**.

II. RELEVANT FACTS

A. THE AUGUST 4, 1993 ASSAULT

On August 4, 1993, a woman (the "Woman") [1] was attacked in Newark, Delaware. [2] The attacker took her clothing and her identification card. [3] The attacker penetrated her vaginally with his penis. [4] The attacker then fled with her personal items including the Woman's "North Carolina driver's license, University of Delaware ID, 'Carolina' t-shirt, denim shorts and panties." [5] The Woman immediately reported the attack to police. [6] The police initiated an investigation. [7] The Woman underwent a Sexual Assault Nurse Examination ("SANE") during which her vagina was swabbed for DNA. [8] The police were unable to solve this case in 1993.

B. DNA EVIDENCE LEADS POLICE TO SUSPECT MR. KING OF THE 1993 ASSAULT.

The police reopened and reassigned the case to Detective Gerasimov in November 2017. [9] Investigators identified Mr. King as a suspect. [10]

In August 2019, Newark Police Department detectives conducted surveillance on Mr. King, his residence and place of employment. [11] On August 14, 2019, Mr. King purchased a Wawa iced tea in a plastic bottle, drank from the bottle and placed the bottle in a plastic Wawa bag. [12] Mr. King subsequently discarded the plastic Wawa bag containing the empty plastic Wawa iced tea bottle in a Walmart trash can. [13]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

***2** Investigators seized the plastic Wawa bag from the Walmart trash can and sent the Wawa iced tea bottle to the Delaware Division of Forensic Science to process for DNA evidence. [14] The Division of Forensic Science prepared a report comparing swabs from the Wawa iced tea bottle to the vaginal swabs from the SANE kit. [15] The report indicated that the vaginal swab matched the bottle sample. [16] The probability of randomly selecting an unrelated individual with a matching DNA profile was one in > 7,000,000,000,000 (7 trillion). [17]

Using this information, the Newark Police Department obtained a search warrant permitting them to obtain DNA from Mr. King by buccal swab or blood draw. [18]

C. THE POLICE SEARCH MR. KING'S RESIDENCE AND VEHICLE.

On October 3, 2019, a Pennsylvania court issued search warrants (the "Pennsylvania Search Warrants") for Mr. King's residence at 123 Wesley Lane, Coatesville PA, 19320 and Mr. King's vehicle, a 2013 Chevrolet Silverado. [19] The Pennsylvania Search Warrant applications were identical except for the search location. The supporting probable cause affidavits contained, among other facts, the information about the investigation leading to Mr. King's DNA match with the vaginal swabs from the 1993 assault.

The search warrants sought:

a) Any items (letters, notes, papers, documents, identifications, etc.) in whatever form they may be found, that are associated with the identified victim, to include but not limited to items containing personal identifying information of the identified victim. Personal identifying information is to include but is not limited to name, date of birth, driver's license number(s), address(es), etc.;

b) Any items (letters, notes, papers, documents, etc.) in whatever form they may be found, that would show Jeffrey KING's travel plans, destinations, family relations, and/or other information related to Newark, DE and elsewhere.

c) Any items (letters, notes papers, documents, contact books, etc.) in whatever form they may be found, containing any identifying information (names, phone numbers, etc.) that would lead to identifying any friends or associates of Jeffrey King;

d) Any and all photo albums and loose photographs depicting Jeffrey KING;

e) Journals, dairies [sic], newspaper articles in whatever form they may be found, and/or any other records that are related to the incident described in this affidavit or any other serious crimes;

f) All electronic devices that can easily be used to connect to the internet for accessing and using web-based services or strong digital data, which includes but is not limited the accessing and viewing web pages, submitting online form [sic], conducting electronic communications, etc. These electronic devices include but are not limited to computers, mobile phones, tablets, iPads, PDAs, etc.;

g) All external memory devices that can easily be used to store electronic data, including but not limited to hard drives, external hard drives, SIM cards, USB drives, floppy disks, cassette tapes, compact disks, RAM or ROM units, SIM cads, cellular phones, computers, etc.;

h) "Carolina" t-shirt, denim shorts, and panties;

i) Receipts and other paperwork related to rental of storage unit(s) and/or offsite storage locations. [20]

***3** The Pennsylvania Search Warrant applications also describe how Detective Gerasimov knows, "[f]rom a combination of education, training, experience discussions with other law enforcement officers, and study of legal documents," that sexual offenders keep items they've taken from victims as trophies; and also keep written journals, diaries and other records in easily accessible locations such as homes, vehicles, storage sheds and storage containers. [21] On the same basis, the Pennsylvania Search Warrant applications provide that Detective Gerasimov knows that suspects conduct research and attempt to access updated information about crimes they committed using electronic devices with internet access; and that those devices are in easily accessible locations. [22] In addition, the Pennsylvania Search Warrant applications state that Detective Gerasimov knows that suspects use storage facilities to store items. [23] Finally, on the same basis, Detective Gerasimov knows that people keep photos of themselves, family and friends; as well as contact information thereof in easily accessible locations. [24]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Police executed the Pennsylvania Search Warrants on October 3, 2019.[25] Investigators located older photos of Mr. King in the residence.[26] Investigators recovered nothing else of evidentiary value from the residence or vehicle.[27]

D. MR. KING'S OCTOBER 3, 2019 ARREST AND INTERROGATION.

Coatesville Police arrested Mr. King and transported him to the Coatesville Police Department station on October 3, 2019.[28] During booking, the booking officer asked Mr. King for pedigree information.[29] An officer also asked for his cellphone passcode.[30] While escorting Mr. King to an interrogation room, an officer explained that Mr. King might have to wait for someone to interview him.[31] Mr. King asked, "Do I need my lawyer?"[32] The officer responded, "No, I'm just telling you this is our interview room."[33]

At 3:20 PM, officers entered the room to interview Mr. King.[34] One of the officers read Mr. King's *Miranda* rights.[35] Mr. King read and signed a *Miranda* form.[36] The officer asked if Mr. King would make a statement and Mr. King responded, "Sure, why not."[37]

At 4:19 PM, the officers informed Mr. King that they had evidence linking him to a sexual assault and Mr. King stated, "I think I need to call a lawyer."[38] The officers told him that this was the only chance he would have to respond to allegations and Mr. King asked, "Or what? What happens?"[39] For the next two minutes, the officers talked about how Mr. King had the opportunity to tell the police the "full story."[40] The officers also warned him that staying silent may not be in his best interest.[41] Then, during an additional two minutes, the officers described potential consequences that a victim might feel.[42] Finally, the officers referenced Mr. King's earlier statement, saying, "You said it out of your own mouth, you're a person that tries to make things right."[43]

At this point, Mr. King reiterated that he thought that he "better call an attorney."[44] An interrogating officer said, "you have those rights and I'm willing to go over those rights again with you."[45] Mr. King said, "I guess I'm going to jail."[46] The officer then said, "Yes, you have the right to an attorney but think about doing the right thing."[47] Mr. King said, "I guess I'm going to jail aren't I? I need an attorney."[48] The officer then responded, "That's clear at this point," and ended the interview.[49]

III. PARTIES' CONTENTIONS

A. THE SEARCH WARRANT MOTION

***4** Mr. King argues that the Pennsylvania Search Warrant's supporting affidavits were invalid because there is an insufficient factual nexus between the alleged crime and Mr. King's residence and vehicle. As such, Mr. King claims that these affidavits do not support a finding of probable cause and the issuance of the Pennsylvania Search Warrants.

The State contends that the affidavits sufficiently set out facts supporting a finding of probable cause for searching Mr. King's residence or vehicle. The State additionally argues that there is nothing suggesting that evidence related to the crime would not be at his residence or vehicle.

B. THE BUCCAL SWAB MOTION

Mr. King argues that the police violated his reasonable expectation of privacy under the Fourth Amendment by (i) constantly surveilling him for several days and (ii) conducting a warrantless search by seizing a Wawa iced tea bottle that he discarded in a public trashcan at Walmart. Alternatively, Mr. King contends that the Delaware Constitution guarantees a higher privacy expectation in one's garbage than that guaranteed under the Fourth Amendment. Mr. King claims that that State violated his Fourth Amendment rights by seizing his DNA from the Wawa iced tea bottle in a warrantless search. Mr. King argues that without the DNA sample seized from the Wawa iced tea bottle, then there is insufficient evidence to make a probable cause finding and to justify the buccal swab search warrant.

The State argues that Mr. King had neither a subjective nor an objectively reasonable expectation of privacy in the Wawa iced tea bottle. Furthermore, the State contends that swabbing the Wawa iced tea bottle is not a search for Fourth Amendment purposes and required no warrant.

C. THE *MIRANDA* MOTION

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Mr. King argues that the police officers obtained several statements in violation of *Miranda*. Mr. King contends that these officers misled him on whether he needed a lawyer, therefore preventing him from voluntarily waiving his *Miranda* rights. Mr. King notes that the police officers continued asking questions even after Mr. King invoked his right to counsel. Finally, even if Mr. King ambiguously invoked his right to counsel, Mr. King argues that the police officers should have either reread the *Miranda* warnings or clarified the ambiguous invocation.

The State contends that Mr. King voluntarily and knowingly waived his *Miranda* rights; and that the police stopped questioning Mr. King after he clearly invoked his right to counsel.

IV. DISCUSSION

A. THE AFFIDAVIT ESTABLISHED A LOGICAL NEXUS BETWEEN THE EVIDENCE SOUGHT AND MR. KING'S RESIDENCE AND VEHICLE.

The Court finds that from the four corners of the probable cause affidavit, the police had probable cause to believe that Mr. King's residence had evidence of the unlawful sexual intercourse.

Under Delaware's four-corners test for probable cause, "sufficient facts must appear on the face of the affidavit so ... a reviewing Court can verify the existence of probable cause." [50] The test for probable cause only requires "that a probability ... of criminal activity be established." [51] To establish probable cause to search a location, "first, there must be probable cause that a crime was committed, and second, there must be probable cause to believe that evidence of such a crime can be found" at the location. [52] In other words, there must be a "logical nexus between the items sought and the place to be searched." [53] The nexus "can be inferred from the type of crime, the nature of the items sought, the extent of an opportunity for concealment and normal inferences to where a criminal would hide [evidence of the crime]." [54] If there is no nexus between the items sought and the place to be searched, the evidence "will be inadmissible at trial." [55]

***5** First, the Court finds that the affidavits established probable cause that a crime was committed because both affidavits included the Woman's description of her sexual assault. [56]

Second, the Court finds that the affidavits established a logical nexus between the items sought and Mr. King's vehicle and residence. The Pennsylvania Search Warrant supporting affidavits included statements, based on training and experience, that sexual assault offenders keep evidence from their assaults in easily accessible places. The Court considers it logical to infer that if Mr. King committed the sexual assault, and sexual offenders keep evidence from sexual assaults in easily accessible places such as their homes and vehicles, then Mr. King would keep such evidence in his home and vehicle. The Pennsylvania Search Warrants were limited to a search for specific types of evidence—*e.g.*, the Carolina t-shirt, information kept about the Woman, possible off-site storage, old photographs that would assist in identification The Pennsylvania Search Warrants were not general warrants but were tailored for the circumstances surrounding the alleged offenses. Therefore, the Court **DENIES** the Search Warrant Motion.

B. THE BUCCAL SWABBING DID NOT VIOLATE MR. KING'S RIGHTS UNDER THE U.S. CONSTITUTION OR DELAWARE LAW.

On a motion to suppress evidence seized during a warrantless search, the state must show, by a preponderance, of evidence that the challenged search did not violate a defendant's rights under the U.S. Constitution or Delaware law. [57] To raise a claim that a warrantless search was illegal, the defendant "must have a reasonable expectation of privacy." [58] Under the *Katz* test, a defendant has a reasonable expectation of privacy when (1) a person exhibits an actual (subjective) expectation of privacy and (2) the expectation is one that society is prepared to recognize as objectively reasonable. [59] Government action that invades on an area where a person has an objectively reasonable expectation of privacy is "an unconstitutional search." [60]

i. The police did not violate Mr. King's reasonable expectation of privacy by surveilling him, his residence and his place of employment.

The Court finds that the police surveillance of Mr. King was not an illegal search. "It is well-established that '[w]hat a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection.' " [61] The police surveillance

of Mr. King only extended to what would have been visible to the public, from a distance and in a manner that did not obstruct his activities. These facts put the case "outside the purview of the Fourth Amendment." [62]

***6** Mr. King argues that the surveillance violated the Delaware constitution under *State v. Holden.* [63] *Holden* held that surreptitiously placing a GPS unit on a car and tracking a location 24 hours a day for multiple weeks "violated the Defendant's reasonable expectation of privacy and state Constitutional rights." [64] GPS surveillance that exposes "the whole of one's movement over a prolonged period of time tells a vastly different story than movement over a day as may be completed by manned surveillance." [65] In this case, the Newark Police Department's manned surveillance does not violate Mr. King's expectation of privacy in the same way prolonged GPS surveillance would. The Newark Police Department only observed Mr. King in public locations and did not surreptitiously observe Mr. King inside his home or in other private locations as was done with the GPS device.

ii. Mr. King did not have a reasonable expectation of privacy in the Wawa iced tea bottle.

The Court finds that Mr. King did not have a reasonable expectation of privacy in items that he deposited in a publicly accessible trash can. First, Mr. King took no action showing that he sought to preserve the Wawa iced tea bottle as private when he discarded the bottle in a public trashcan. Therefore, he did not exhibit an actual expectation of privacy in the Wawa iced tea bottle. [66]

Second, even if Mr. King had a subjective expectation of privacy when he discarded the Wawa iced tea bottle, that expectation of privacy would not be objectively reasonable. The Fourth Amendment does not require warrants to search trash left outside the curtilage of the home. [67] States, however, "may surely construe their own constitutions as imposing more stringent constraints on police conduct that does the Federal Constitution." [68] Nonetheless, Delaware courts have held that there is no expectation of privacy in trash outside the curtilage of the home nor in public trash containers. [69] Under Delaware law, throwing away trash in a public trash container is "tantamount to 'throwing away' a subjective expectation of privacy in it that society accepts as reasonably acceptable." [70]

Mr. King exhibited no actual expectation of privacy nor would such an expectation be reasonable. Therefore, seizing the Wawa iced tea bottle was not an illegal search under the Fourth Amendment or the Delaware Constitution.

iii. Mr. King did not have a reasonable expectation of privacy in the DNA collected from the Wawa iced tea bottle.

The Court also finds that Mr. King did not have a reasonable expectation of privacy in his DNA collected from the Wawa iced tea bottle. DNA analysis that only provides identification is "no more a search than an analysis of latent fingerprints." [71] Such analysis of physical characteristics " 'involves none of the probing into an individual's private life and thoughts that marks' a Fourth Amendment search." [72] The DNA laboratory report only reported that Mr. King's DNA sample matched the one previously taken from the victim. [73] There was no additional information that violated a protected privacy interest, such as private medical information. [74] Therefore, the Court finds that the State did not violate Mr. King's reasonable expectation of privacy by testing his DNA for identification purposes.

iv. The buccal swabbing search warrant affidavit set forth sufficient facts to find probable cause.

***7** "The affidavit in support of a search warrant must set forth facts adequate to warrant a reasonable man in the belief that an offense has been committed and that seizable property would be found in a particular place or on a particular person." [75] The Buccal Swab Search Warrant affidavit set forth sufficient facts to believe that an offense was committed because it described the sexual assault. [76] This affidavit also set forth how the Newark Police Department obtained the DNA sample and that the Delaware Division of Forensic Science matched the DNA sample to the one taken from the victim. [77] The Court finds that the affidavit set forth sufficient facts to find probable cause for the search warrant authorizing a DNA sample collection from Mr. King. The Court therefore **DENIES** the Buccal Swabbing Motion.

C. THE POLICE VIOLATED MR. KING'S *MIRANDA* RIGHTS BY CONTINUING TO QUESTION HIM AFTER HE INVOKED HIS RIGHT TO COUNSEL.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Mr. King alleges that the police violated his *Miranda* rights by (1) deceiving him about his need for an attorney at the outset of the interrogation and (2) failing to stop questioning him after he invoked his right to counsel. The Court agrees that the police violated his *Miranda* rights by failing to stop questioning after Mr. King invoked his right to counsel.

Under *Miranda v. Arizona*, the prosecution is barred from using statements obtained during a "custodial interrogation of the defendant unless it demonstrates the use of procedural safeguards to secure the privilege against self-incrimination." [78] A custodial interrogation is "questioning initiated by law enforcement officers after a person has been taken into custody or otherwise deprived of his freedom of action in any significant way. [79] Interrogation refers not only to express questioning but also to its functional equivalent *i.e.* any practice "that the police should know is reasonably likely to evoke an incriminating response from a suspect." [80]

i. Statements made after Mr. King signed the* Miranda *form but before he invoked his right to counsel are admissible.

Delaware determines whether a suspect waives his *Miranda* rights under a two-part test. First, the suspect must voluntarily waive his *Miranda* rights and the waiver cannot result from "intimidation, coercion or deception." [81] Second, the suspect must be fully aware of the nature of the *Miranda* rights and the consequences of waiver. [82] The Court may only find *Miranda* waiver if " 'the totality of the circumstances surrounding the interrogation' reveal both an uncoerced choice and the requisite level of comprehension." [83]

Mr. King argues that he did not waive his *Miranda* rights because the police deceived him by answering "no" when he asked if he needed a lawyer. [84] The police officer escorting Mr. King was explaining that Mr. King would have to wait for someone to speak with him for a period, and that he would be on camera when Mr. King asked if he needed a lawyer. [85] The officer responded, "No, I'm just telling you that this room right here is our interview room." [86] Before the interrogation began, the interrogating officer read the *Miranda* rights to Mr. King. [87] Mr. King subsequently read and signed the *Miranda* form. [88] Under the totality of the circumstances, the Court finds that Mr. King's waiver was not coerced by deception and he understood the consequences of waiver. Therefore, the Court finds that Mr. King's statements made after he signed the *Miranda* form through when he invoked his right to counsel are admissible.

ii. Mr. King's statements made after 4:19 PM on October 3, 2019 are inadmissible.

***8** Whether to suppress a defendant's statements under *Miranda* "embodies two distinct inquiries." [89] First, the Court determines whether the defendant "actually invoked his right to counsel." [90] Second, if the defendant invoked his right to counsel, courts may admit his responses to further questioning if he "(a) initiated further discussions with the police, and (b) knowingly and intelligently waived the right he had invoked." [91]

The Court finds that Mr. King invoked his right to counsel. An explicit request for counsel is an unequivocal assertion of the right to counsel. [92] If the request for counsel is ambiguous, however, Delaware has adopted "the clarification approach." [93] Under the clarification approach, the interrogating officer must limit questions after the ambiguous assertion of the right to counsel "to those designed to elicit definitive indications of intent." [94] "[T]he clarifiying questions may not coerce or intimidate the suspect or otherwise discourage his effort to secure counsel." [95] Whether a statement is an ambiguous invocation of *Miranda* is "determined on a case-by-case basis, analyzing the totality of the circumstances." [96]

A mere expression that the defendant thinks he needs counsel is not an explicit invocation of the right to counsel. [97] It is, however, an ambiguous invocation of the right to counsel requiring clarification by the interrogating officer. [98] The Court thus finds that Mr. King ambiguously invoked the right to counsel by saying, he "thinks" he needs a lawyer.

Instead of clarifying Mr. King's ambiguous invocation of *Miranda*, however, the police officers discouraged Mr. King from securing counsel. The police officers told Mr. King that speaking to them without counsel was his only chance to explain his side of the story. [99] The police also attempted to discouraged Mr. King from securing counsel by appealing to his sense of morality. [100] Even after Mr. King reiterated that he "think[s] [he] better call an attorney," [101] the interrogating officer continued to discourage Mr. King from seeking counsel. [102]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

The police officers had to know that these statements were "reasonably likely to evoke an incriminating response" from Mr. King.[103] This means that the statements were custodial interrogation under *Miranda*.[104] The police violated his rights under Delaware law by failing to limit their questioning to clarifying questions after Mr. King ambiguously invoked his right to counsel. Therefore, the Court **GRANTS** the *Miranda* Motion with respect to statements made after 4:19 PM on October 3, 2019.

D. THE COURT WILL RESERVE RULING ON THE CELLPHONE EVIDENCE.

***9** Mr. King also sought to suppress evidence on his cellphone because the police obtained his cellphone passcode in violation of *Miranda*. At the motions hearing, the State represented that it would not use evidence obtained from Mr. King's cellphone. The Court will consider Mr. King's motion to suppress cellphone evidence if the State indicates that it will use such evidence.

V. CONCLUSION

For the foregoing reasons, the Court will **GRANT in Part and DENY in Part** the *Miranda* Motion, and will **DENY** the Search Warrant Motion and the Buccal Swabbing Motion.

All Citations

Not Reported in Atl. Rptr., 2021 WL 211150

Footnotes

1 The name is not relevant to the decision here.

2 Mot. to Suppress Evid. (hereafter "Search Warrant Mot.") ¶ 4.

3 *Id.*

4 *Id.*

5 *Id.*; *Id.* Ex. A (Search Warrant Affidavit of Probable Cause).

6 State's Resp. to Def.'s Mot. to Suppress (hereafter "Search Warrant Mot. Resp.") 1.

7 *Id.*

8 *Id.* 1-2.

9 Search Warrant Mot. Ex. A.

10 *Id.*

11 Amend. Mot. to Suppress Buccal Swabbing (hereafter "Amend. Buccal Swabbing Mot.") ¶ 2.

12 *Id.*

13 *Id.*

14 *Id.*

15 State's Resp. to Def.'s Amend Mot. to Suppress Buccal Swabbing (hereafter "Amend. Buccal Swabbing Mot. Resp.") Ex. A.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

16 *Id.*

17 *Id.*

18 Amend. Buccal Swabbing Mot. ¶ 1.

19 Search Warrant Mot. Ex. A; Search Warrant Mot. Ex. B (Search warrants for Mr. King's vehicle and residence).

20 Search Warrant Mot. Ex. A.

21 *Id.*

22 *Id.*

23 *Id.*

24 *Id.*

25 Search Warrant Mot. Resp. 2.

26 *Id.*

27 *Id.*

28 *Id.*; State's Resp. to Mot. to Suppress Def.'s Statement (hereafter "*Miranda* Mot. Resp.") 2.

29 *Miranda* Mot. Resp. Ex. A at 7:00 (Arresting officer body camera footage).

30 *Id.* Ex. A at 7:30.

31 *Id.* Ex. A at 11:50.

32 *Id.* Ex. A at 12:05.

33 *Id.* Ex. A at 12:07.

34 *Id.* Ex. B at 3:20 PM (Interrogation room footage).

35 *Id.* Ex. B at 3:27 PM.

36 *Id.* Ex. B at 3:28 PM.

37 *Id.* Ex. B at 3:28 PM.

38 *Id.* Ex. B at 4:19 PM.

39 *Id.* Ex. B at 4:20 PM.

40 *Id.* Ex. B at 4:20-4:22 PM.

41 *Id.*

42 *Id.* Ex. B at 4:22-4:24 PM.

43 *Id.* Ex. B at 4:24 PM.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

44 *Id.* Ex. B at 4:24 PM.

45 *Id.* Ex. B at 4:24 PM.

46 *Id.* Ex. B at 4:24 PM.

47 *Id.* Ex. B at 4:24 PM.

48 *Id.* Ex. B at 4:25 PM.

49 *Id.* Ex. B at 4:25 PM.

50 *Pierson v. State*, 338 A.2d 571, 573 (Del. 1975).

51 *Jensen v. State*, 482 A.2d 105, 112 (Del. 1984) (citing *Spinelli v. United States*, 393 U.S. 410, 419 (1969)).

52 *State v. Cannon*, 2007 WL 1849022, at *4 (Del. Super. June 27, 2007).

53 *Dorsey v. State*, 761 A.2d 807, 811 (Del. 2000).

54 *State v. Ivins*, 2004 WL 1172351, at *4 (Del. Super. May 21, 2004).

55 *Id.*

56 Search Warrant Mot. Ex. A; Search Warrant Mot. Ex. B.

57 *See State v. Coursey*, 136 A.3d 316, 321 (Del. Super. 2016).

58 *Rodriguez v. State*, 2013 WL 5494720, at *1 (Del. Sept. 30, 2013) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)).

59 *State v. Guaradarrama*, 2016 WL 7235694, at *6 (Del. Super. Dec. 14, 2016)

60 *State v. Holden*, 54 A.3d 1123, 1132 (Del. Super. 2010).

61 *Kowalski v. Scott*, 2005 WL 703757, at *1 (3d. Cir. Mar. 29, 2005) (citing *Katz*, 389 U.S. at 351).

62 *See id.* ("The video surveillance of [the defendant] was taken only while [he] was in full view of many strangers, in public areas.... It was also taken from a distance, and in a manner that did not obstruct [his] activities. Together these facts put the video surveillance in this case outside the purview of the Fourth Amendment").

63 54 A.3d 1123 (Del. Super. 2010).

64 *Id.* at 1134.

65 *Id.* at 1132.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

66 *See* *Bond v. U.S.*, 529 U.S. 334, 334 (2000) ("First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that 'he [sought] to preserve [something] as private.' ") (citing *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

67 *See* *United States v. Edwards*, 717 Fed. Appx. 166, 168 (3d Cir. 2017) (citing *California v. Greenwood*, 486 U.S. 35, 40-42 (1988)).

68 *Greenwood*, 486 U.S. at 43 (1988).

69 *See* *State v. Ranken*, 25 A.3d 845, 852 (Del. Super. 2010) (holding, under *Greenwood*, that a defendant did not have a reasonable expectation to privacy in trash left outside the curtilage of his property under the Fourth Amendment); *State v. Grossberg*, 1998 WL 283491, at *4 (Del. Super. Mar. 18, 1998) (holding that the defendant did not have a reasonable expectation of privacy under the Fourth Amendment in trash thrown away in a public trash container).

70 *Grossberg*, 1998 WL 283491, at *4 (Del. Super. Mar. 18, 1998).

71 *Commonwealth v. Arzola*, 26 N.3d 185, 191 (Mass. 2015); *see also* *Maryland v. King*, 569 U.S. 435, 469 (2013) (holding that DNA sample analysis used for identification and did not reveal genetic traits is constitutional).

72 *Raynor v. State*, 99 A.3d 753, 761 (Md. 2014) (citing *United States v. Dionisio*, 410 U.S. 1, 15 (1973)).

73 Amend. Buccal Swabbing Mot. Resp. Ex. A (Supplemental DNA Laboratory Report).

74 *See* *King*, 569 U.S. at 464 (2013).

75 *Jensen*, 482 A.2d at 110-11 (Del. 1984).

76 Amend. Buccal Swabbing Mot. Ex. A (Probable Cause Affidavit).

77 *Id.*

78 *Miranda v. Arizona*, 384 U.S. 436, 444 (1966).

79 *Id.*

80 *Rhode Island v. Innis*, 446 U.S. 291, 301 (1980).

81 *Bennett v. State*, 2010 WL 987025, at *3 (Del. Mar. 18, 2010).

82 *See id.*

83 *Id.*

84 *Miranda* Mot. ¶ 14.

85 *Miranda* Mot. Resp. Ex. A 11:55-12:05.

86 *Id.* at 12:06-12:10.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

87 *Miranda* Mot. Resp. Ex. B 3:27 PM.

88 *Id.* at 3:28 PM.

89 *Smith v. Illinois*, 469 U.S. 91, 95 (1981).

90 *Id.*

91 *Id.*

92 *See* *Crawford v. State*, 580 A.2d 571, 574 (Del. 1990) ("Where a suspect has made an explicit request for the assistance of counsel, the duty imposed upon the police is clear: no further questioning may occur until counsel is provided or the suspect himself initiates further conversation").

93 *Id.* at 577.

94 *Id.* at 575.

95 *Id.* at 577.

96 *See* *State v. Pulliam*, 2012 WL 6845693, at *5 (Del. Super. Dec. 13, 2012).

97 *See* *Holmes v. State*, 2016 WL 1055050, at *4-*5 (Del. Mar. 14, 2016).

98 *See id.* at *5 ("Holmes did not unequivocally invoke his right to an attorney, but the officer still sought clarification by reminding Holmes of his right to counsel. Holmes cut the officer's reminder short and continued to talk. The totality of the circumstances clearly show that Holmes knew of, and chose not to invoke, his *Miranda* rights.")

99 *Miranda* Mot. Reply Ex. B 4:20 PM.

100 *See e.g. Miranda* Mot. Reply Ex. B 4:22-23 PM ("Just imagine for one second that's your daughter, every day they wake up, every time they turn a corner on the street, they have panic attacks ... just for a second let that resonate").

101 *Miranda* Mot. Reply Ex. B 4:24 PM.

102 *See Miranda* Mot. Reply Ex. B 4:24 PM ("Yes, you have the right to an attorney but think about doing the right thing").

103 *See* *Innis*, 446 U.S. at 301 (1980).

104 *Id.*

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

222 A.3d 582
Superior Court of Delaware.

STATE of Delaware,
v.
Steven PIERCE, Defendant.

I.D. No. 1610003829
|
Submitted: February 8, 2019
|
Decided: March 6, 2019

Synopsis

Background: Defendant, who was charged with murder in the first degree and possession of a deadly weapon during the commission of a felony, filed motion in limine to exclude expert testimony.

[Holding:] The Superior Court, Rocanelli, J., held that as matter of first impression, wireless networking data used to geolocate defendant's cell phone was reliable and, thus, admissible.

Motion denied.

Procedural Posture(s): Pre-Trial Hearing Motion.

West Headnotes (7)

[1] **Searches and Seizures** Probable or Reasonable Cause

To satisfy Fourth Amendment, search warrant is required to be based on a finding of probable cause for government search of cell phone. U.S. Const. Amend. 4.

[2] **Criminal Law** Subjects of Expert Testimony

Under *Daubert* standard to determine admissibility of expert testimony, court asks whether: (i) witness is qualified as expert by knowledge, skill, experience, training or education; (ii) evidence is relevant and reliable; (iii) expert's opinion is based upon information reasonably relied upon by experts in the particular field; (iv) the expert testimony will assist trier of fact to understand the evidence or to determine fact in issue; and (v) expert testimony will not create unfair prejudice or confuse or mislead jury.

[3] **Criminal Law** Necessity and sufficiency

When assessing the second factor of the *Daubert* standard—the reliability of the expert's opinion—trial courts consult a non-exclusive list of four questions: (1) whether the opinion at issue is susceptible to testing and has been subjected to such testing; (2) whether the opinion has been subjected to peer review; (3) whether there is a known or potential rate of error associated with methodology used and whether there are standards controlling technique's operation; and (4) whether the theory has been accepted in scientific community.

[4] **Criminal Law** Subjects of Expert Testimony

Criminal Law Basis of Opinion

As the gatekeeper for expert testimony, trial judge's role is to make certain that expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field.

[5] **Criminal Law** Evidence calculated to create prejudice against or sympathy for accused

Criminal Law Particular tests or experiments

Wireless networking data used to geolocate defendant's cell phone was reliable and, thus, admissible in murder case; reliability of the location data had been tested, it had been subject to peer review in the relevant scientific

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

community, it was substantiated by other mechanisms of geolocation, it was widely accepted in the computer science industry and reasonably relied upon by law enforcement, and probative value of the location data substantially outweighed danger of unfair prejudice. Del. R. Evid. 403.

1 Cases that cite this headnote

[6] **Criminal Law** Particular tests or experiments

Any questions regarding the strength of each wireless signal went to the weight and not the admissibility of the evidence when determining if wireless networking data used to geolocate defendant's cell phone was reliable and, thus, admissible in murder case.

1 Cases that cite this headnote

[7] **Criminal Law** Aid to jury

Expert testimony must help the fact finder understand the evidence or determine a fact in issue.

***583** ***Upon Defendant's Motion in Limine to Exclude Expert Testimony*, DENIED**

Attorneys and Law Firms

Annemarie H. Puit, Esquire, Matthew B. Frawley, Esquire, Jenna R. Milecki, Esquire (argued), Department of Justice, Wilmington, Delaware, Attorneys for the State.

Eugene J. Maurer, Jr., Esquire, Elise K. Wolpert, Esquire (argued), Wilmington, Delaware, Attorneys for Defendant.

OPINION

Rocanelli, J.

This is a murder case. The State alleges that Defendant, Steven Pierce, shot and killed his girlfriend, Heather Stamper, on July 9, 2016 in her Delaware City home. The State proposes to introduce evidence tracking Defendant's movements for the 23-hour period before and after the approximate time of death. Defendant seeks to exclude the Google Wi-Fi Location Data [1] used to "geolocate" Defendant's cell phone on the grounds that the proposed evidence is not sufficiently reliable under the *Daubert* standard and would mislead and confuse the jury. The State argues that the technology at issue is reliable and would be helpful to the finder of fact. The reliability of Google's Wi-Fi Location Data is an issue of first impression in Delaware.

***584 PROCEDURAL HISTORY**

Defendant was indicted by the Grand Jury on December 5, 2016, and charged with Murder in the First Degree and Possession of a Deadly Weapon During the Commission of a Felony for the intentional murder of Heather Stamper. The case was specially assigned to this Trial Judge. The trial was initially scheduled for January 2018 but was rescheduled when Defendant retained new counsel who was unavailable for that trial date. [2] A new trial date was set for August 2018.

On June 5, 2018, Defendant sought permission of the Court to file two motions after the deadline imposed by the Court for pre-trial motions: a motion to suppress certain evidence and a *Daubert* motion. The Court did not address the motion to suppress because the parties reached an agreement that the State would not use the challenged evidence in the State's case-in-chief. Regarding the *Daubert* motion, the Court conducted an office conference on June 28, 2018, at which time it became clear that resolution of the novel issue involved would require that the trial date be rescheduled again. Accordingly, the Court conducted a hearing on July 6, 2018 to address Defendant personally regarding his right to a speedy trial.

The Court found that Defendant's waiver of his speedy trial rights was knowing, intelligent, and voluntary. By Order dated July 6, 2018, the Court granted Defendant's Motion to File a *Daubert* Motion Out-Of-Time, over the State's objection. A new Trial Scheduling Order was issued, setting the date for trial as April 2, 2019, and setting forth deadlines for discovery and briefing in connection with Defendant's *Daubert* motion.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

The Court conducted a *Daubert* hearing on November 27, 2018. In support of the reliability of the State's proposed evidence, the State presented the testimony of Andrew Rist, an engineer, and Anthony Vega, a law enforcement officer. The State's two witnesses were subject to cross-examination by Defendant. The parties submitted post-hearing briefs.

THE TECHNOLOGY AT ISSUE [3]

According to the United States Supreme Court, in 2018, there were 396 million cell phone service accounts in the United States. [4] The High Court emphasized that there are more cell phone accounts in the United States than there are people. [5] The most popular mobile devices have one of two operating systems that control the functioning of the phone. For Apple phones, it is iPhone Operating System ("iOS") and for Google phones and many other phone manufacturers, it is Android.

Defendant's phone was a MetroPCS phone with the Android operating system. While there are similarities between Apple's iOS and Google's Android as it relates to capturing user data, the technology at issue in this case involves location data derived from communications between an Android mobile device and Google. (The data is referenced herein as "Google Wi-Fi Location Data"). Specifically, the subject of the *Daubert* motion in ***585** this case was the Wi-Fi-sourced geolocation information associated with a unique Google account transmitted from the Android operating system on Defendant's mobile device and stored by Google.

A cell phone using the Android operating system serves as a data collection device as it continuously collects and sends information to Google as "events" approximately every 10-20 minutes. Meanwhile, other programs on the phone are running, either actively by the cell phone user, or idly in the background. These applications often rely upon Google Wi-Fi Location Data to customize information sent by Google to the user. [6] With each event, there are various categories of information sent back to Google, including the device's location history which is comprised of GPS, cellular data, and recognized Wi-Fi signals. Google collects and retains fairly detailed location information, including time-stamped barometer readings to determine the device's altitude, such as the floor within a building, and Wi-Fi scans recorded with a time stamp for each location, noting latitude, longitude, and estimated accuracy.

Google Wi-Fi Location Data is not considered first-generation technology for geolocation. Global Positioning System ("GPS"), a utility owned by the United States government, uses satellites for positioning, navigation, and timing ("PNT") services. [7] GPS receiver equipment is found in many mobile devices, including cell phones and vehicle navigation systems. Mobile devices exchange signals with GPS satellites and use the transmitted information to calculate the user's position. [8] Under open skies, "GPS-enabled smartphones are typically accurate to within a 4.9 meter radius." [9] The accuracy of GPS can be compromised by many factors, including satellite signal blockage due to tall buildings or trees, indoor or underground use, and poor atmospheric conditions. [10] Nevertheless, the reliability of GPS is well established. [11]

Another method for geolocation is Cell-Site Location Information ("CSLI"), which refers to the information collected as a cell phone connects to nearby cell towers. [12] Although cell site records are generated by cell phone service providers for commercial purposes, law enforcement agencies routinely request and use historical CSLI for criminal investigatory purposes. [13] With information from multiple cell towers, a technique called "triangulation" is used to identify the location of a cell phone, and by extension, the cell phone user's approximate location within 50 meters. [14] Like GPS, the reliability of CSLI is well established. [15]

***586** The underlying premise of Google Wi-Fi Location Data is the same as GPS and CSLI. A Wi-Fi positioning system relies upon Wi-Fi signals to determine the distance between the device and the signal access point ("AP"). Wi-Fi Access Points are the devices that create a wireless local area network, such as a router in an office, business, or home, by projecting a Wi-Fi signal to a designated area. Included in the location data sent to Google by Android devices are Wi-Fi scans, which include a list of the Wi-Fi APs the device could "see" at that particular time and location. [16] Generally, in order for a device to see a Wi-Fi AP, the device will be within 150 feet of a signal, much closer than with cell tower positioning. Google collects and stores the locations and strength of Wi-Fi APs, identified by their Media Access Control ("MAC") address, in order to locate mobile devices. When multiple signals are in range, Google Location Services uses multilateration to identify the device location, with more signals providing a more accurate location.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Wi-Fi APs were first mapped by Google as part of its Street View program using vehicles which physically drove around with Wi-Fi receivers to collect street level pictures and record Wi-Fi signals, a process known as "wardriving." This mapping method was the subject of the Zandbergen paper published in 2004.[17] Since that time, Wi-Fi AP locations have been mapped and maintained by Google through a process called "crowdsourcing," whereby information sent back to Google by individual cell phones is used to identify the location of Wi-Fi APs.[18] Crowdsourcing allows more data to be collected more frequently and provides for greater accuracy as more users contribute to data regarding the location of Wi-Fi APs.

PROPOSED EVIDENCE PLACING DEFENDANT AT OR NEAR MURDER SCENE[19]

Defendant's cell phone ("Target Device") was seized on July 9, 2016, the day Heather Stamper was found dead in her home in Delaware City, Delaware. The phone number for the Target Device matches the phone number that Defendant identified as his own phone number during his July 9, 2016 interview with the police.

[1] Through a search warrant,[20] Detective Csapo of the Delaware State Police ***587** obtained Google location data for the Target Device, International Mobile Equipment Identity ("IMEI") number 359696076323056 ("Target IMEI").[21] Google responded to the search warrant in accordance with the Federal Electronic Communications Privacy Act[22] and provided the following information for each time-stamped event for the time period from 6:53 p.m. on July 8, 2016, through 5:49 p.m. on July 9, 2016: identity of account as piercesteve91@gmail.com; date; Universal Time Coordinated (UTC); date and time in Eastern Daylight Time (EDT) using military time; latitude; longitude; map display radius in meters; map display radius in miles; source (GPS or Wi-Fi); and device tag.

Agent Vega analyzed the data associated with the Target IMEI and mapped the geolocation of the Target Device by plotting the latitude, longitude, and estimated radius of GPS and Wi-Fi coordinates, showing those locations using Google Earth. In addition to the Google Wi-Fi and GPS location data, Agent Vega used surveillance video to prepare a PowerPoint presentation tracking Defendant. Time-stamped photographs taken from video surveillance correspond to the Google Wi-Fi Location Data and GPS data to show Defendant and/or the Target Device travelling throughout this time period: in Heather Stamper's vehicle; driving on the streets of Delaware City and heading towards New Castle; at a check-out counter in a New Castle liquor store; driving towards Delaware City; in the vicinity of Heather Stamper's home; travelling towards and in the vicinity of Defendant's mother's home; with Defendant's mother entering a convenience store; and in various other locations nearby during the next day.

STANDARD FOR ADMISSIBILITY OF EXPERT TESTIMONY

[2] The Delaware Supreme Court has adopted the *Daubert* standard to determine the admissibility of expert testimony.[23] Under this standard, the Court asks whether: (i) the witness is "qualified as an expert by knowledge, skill, experience, training or education;" (ii) the evidence is relevant and reliable; (iii) the expert's opinion is based upon information "reasonably relied upon by experts in the particular field;" (iv) the expert testimony will "assist the trier of fact to understand the evidence or to determine a fact in issue;" and (v) the expert testimony will not create unfair prejudice or confuse or mislead the jury.[24]

[3] When assessing the second factor of the *Daubert* standard—the reliability of the expert's opinion—trial courts consult a non-exclusive list of four more questions: (1) whether the opinion at issue is susceptible to testing and has been subjected to such testing; (2) whether the opinion has been subjected to peer review; (3) whether there is a known or potential rate of error associated with the methodology used and whether there are standards controlling the technique's operation; and (4) whether the theory has been accepted in the scientific community.[25]

*588 THE TECHNOLOGY IS RELIABLE AND WILL ASSIST THE FACT-FINDER

[4] **[5]** As the gatekeeper, the trial judge's role "is to make certain that an expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

field."[26] Neither the parties nor the Court has identified a reported decision applying the *Daubert* standard involving testimony by a computer scientist or engineer addressing reliability of Google Wi-Fi Location Data.[27] Accordingly, this Court's reasoned analysis regarding the reliability of Google WiFi Location Data is not informed by rulings of other trial courts.

(i) The State's expert witnesses are qualified as experts by knowledge, skill, experience, training and education.

Defendant does not challenge Andrew Rist as an expert in the computer science field. Rist has an undergraduate degree in mechanical engineering and a master's degree in manufacturing engineering, and has worked as an engineer for Oracle Corporation for more than 20 years.[28] Since 2008, Rist has been an Interoperability Architect reporting to Oracle's Chief Technology Officer, and his recent professional focus has been collection and interpretation of communications data, particularly data sent back to Google by cell phones.

Defendant also does not challenge Anthony Vega as an expert witness. Agent Vega is a Detective with the Philadelphia Police Department's Major Crimes Unit, Task Force Officer with the Federal Bureau of Investigation ("FBI"), and member of FBI's Cellular Analysis Survey Team ("CAST"). Agent Vega testified regarding his training as a law enforcement officer generally and with respect to cell phone technology.

***589** Andrew Rist has the knowledge, skill, experience, training and education to be qualified as an expert in the field of computer technology and specifically with respect to Google Wi-Fi Location Data. Anthony Vega has the knowledge, skill, experience, training, and education to be qualified as an expert in the use of computer technology for criminal investigations. Thus, the first factor of the *Daubert* standard is satisfied.

(ii) Google's Wi-Fi Location Data is relevant and reliable.[29]

The relevance of the evidence is not challenged. However, Defendant challenges the reliability of the methodology underlying Google Wi-Fi Location Data.

(1) The use of Google's Wi-Fi Location Data to geolocate an individual based on signals sent to Google by that individual's cell phone is susceptible to testing and has been subjected to such testing by the State's expert, Andrew Rist.

By employing an industry standard testing method, Rist and his team at Oracle constructed a device, referred to as a "test rig," to understand the communications sent back and forth between Google and the Android operating system. The device consists of a bag containing 20 cell phones, each with an associated Google account, which operates as a "man-in-the-middle" exploit to observe the signals sent by the devices to Google.[30] For a period of approximately two years, Rist has tested and confirmed the accuracy of the Google Wi-Fi Location Data and other communications data by analyzing communications between the phones in the test rig and Google Application Programming Interface ("API") locations and various Google-owned domains. Over the two years of testing, Oracle has collected approximately 70,00 location data points from the devices in the test rig. Rist testified that the Google Wi-Fi Location Data is accurate and reliable.

In addition to Oracle's general testing of Google Wi-Fi Location Data collection through the use of the test rig, Rist deployed the test rig specifically in the vicinity of Heather Stamper's home to determine the strength of Wi-Fi signals in that area.[31] Rist concluded that the density of Wi-Fi signals for the Google Wi-Fi Location Data produced by Google in response to the search warrant in this case is reliable to identify the location of the Target Device within approximately 100 feet.[32] Rist also reviewed the report prepared by ***590** Agent Vega and concluded that the location information for the Target Device located in Agent Vega's PowerPoint presentation are consistent both generally with the data revealed by Rist's general testing and also consistent with Rist's specific findings using the test rig in the area around Heather Stamper's home.

Accordingly, the accuracy of the Google Wi-Fi Location Data has been tested. The Court is satisfied with the testing generally regarding the reliability of the Google Wi-Fi Location Data and specifically as determinative of the reliability of Google Wi-Fi Location Data for the Target Device.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

(2) Google Wi-Fi Location Data has been subjected to peer review in the relevant scientific community.

The accuracy of Wi-Fi location data is the subject of computer science publications and blogs. For example, a 2015 publication from the Technical Information Center of Denmark found that "APs can be very efficiently geolocated in a way that covers a large majority of individuals' mobility patterns."[33] The reliability of Wi-Fi positioning systems is supported by this study which finds "WiFi scans containing at least one visible AP can be used for discovering the location of the user, with a typical spatial resolution on the order of the tens of meters."[34] The Court is satisfied that the relevant scientific community is in agreement regarding the reliability of Google Wi-Fi Location Data. Accordingly, the accuracy of Google Wi-Fi Location Data has been subjected to peer review in the relevant scientific community.[35]

(3) Google Wi-Fi Location Data is verified by other mechanisms of determining geolocation of the Target Device.

[6] A mobile device will switch between GPS and Wi-Fi based on the strength of available signals to improve the accuracy of a location reading.[36] The mobile device prefers Wi-Fi because it uses less power and is available in settings where GPS signals are more limited, such as indoors, but GPS is used to supplement the available Wi-Fi signals. Data for GPS and Wi-Fi APs are both included in the Google location data provided in response to the search warrant for the Target Device. Importantly, Google Wi-Fi Location Data is consistent with the fixed GPS location data.[37] Where fixed GPS location data is not available, time stamps from video surveillance footage substantiate the reliability of the Wi-Fi-sourced readings. Accordingly, the accuracy of Google Wi-Fi Location Data is verified by other mechanisms of determining the geolocation of the Target Device.

(4) The reliability of Google Wi-Fi Location Data has been accepted in the marketplace and has also been accepted in the community as a whole.

Accurate geolocation of a mobile device is an important part of Google's business plan for the Android operating system.[38] Users of Google's applications do not pay a fee; Google's applications are free of ***591** charge to the user. Individuals everywhere rely upon this technology every day in myriad ways to access a variety of information based on their own location.[39] Merchants pay fees to Google for access to information collected by Google about users of Google applications, including user location. Merchants use this location information provided by Google to promote products, often targeting advertisements to specific geographical locations. For example, Google can send advertisements to users who are near a certain restaurant. Accordingly, the reliability of Google Wi-Fi Location Data is accepted by the community as a whole, and in the marketplace.

Therefore, the Court has assessed the second factor of the *Daubert* standard: the reliability of the Google W-Fi Location data has been tested; it has been subject to peer review in the relevant scientific community; it is substantiated by other mechanisms of geolocation; and it is accepted by the community as a whole. The Court finds that the methodology underlying Google Wi-Fi Location Data is reliable. Thus, the second factor of the *Daubert* standard is satisfied.

(iii) Google Wi-Fi Location Data is widely accepted in the computer science industry and reasonably relied upon by law enforcement.

It is acceptance by the scientific community, rather than by the courts, that is identified under *Daubert* as an indicator of a technique's reliability.[40] Google WiFi Location Data is widely accepted as reliable in the computer science community. In addition, Google Wi-Fi Location Data is generated for commercial purposes, which was recognized by *Carpenter* as an indicia of reliability.[41] Furthermore, law enforcement relies upon GPS, historical cell cite analysis,[42] and, more recently, Google Wi-Fi Location Data to place an individual at a specific location at a specific time. Thus, the third factor of *Daubert* is satisfied.

(iv) Expert testimony based on the Google Wi-Fi Location Data will assist the jury to understand the evidence and to determine a fact in issue.

[7] Expert testimony must help the fact finder understand the evidence or determine a fact in issue.[43] The jury in

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

this case will be charged with determining whether the State has established beyond a reasonable doubt that Defendant murdered Heather Stamper. Google Wi-Fi Location Data associated with Defendant's own cell phone will assist the jury in understanding Defendant's approximate location before, during, and after the murder. Thus, the fourth factor of *Daubert* is satisfied.

(v) The expert testimony will not create unfair prejudice or confuse or mislead the jury.

The technology at issue will not confuse or mislead the jury. Indeed, "cell phones ***592** and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[44] The technology, once explained, will be well within the jury's capability to comprehend and weigh. According to Defendant, the State has sufficient evidence, referencing GPS and surveillance footage specifically, without also using Google Wi-Fi Location Data, which according to Defendant, is duplicative and will mislead and confuse the jury. The Court is satisfied that the probative value of the Google Wi-Fi Location Data substantially outweighs the danger of unfair prejudice, confusion of the issues, misleading the jury, or needlessly presenting cumulative evidence.[45] Thus, the fifth factor of *Daubert* is satisfied.

CONCLUSION

The evidence is relevant and the experts presented by the State are qualified by knowledge, skill, training and education. The State has established by a preponderance of the evidence that the Google Wi-Fi Location Data is reliable: the Google Wi-Fi Location Data at issue is susceptible to testing and has been subjected to such testing; it has been subjected to peer review in the relevant scientific community; it is verified by other mechanisms of determining geolocation of the Target Device; it is accepted in the computer science/high tech community; and it is widely relied upon in the marketplace and by the community as a whole. Moreover, Google Wi-Fi Location Data will assist the trier of fact to understand the evidence and to determine a factual issue. Finally, the evidence will not create unfair prejudice or confusion.

NOW, THEREFORE, the Defendant's Motion *in Limine* to Exclude Expert Testimony is hereby DENIED.

IT IS SO ORDERED.

All Citations

222 A.3d 582

Footnotes

1 *See infra* p. 584–85.

2 The State did not oppose rescheduling the trial date. Defendant's new counsel did not enter his appearance until obtaining a new trial date.

3 Unless noted otherwise, the Court's discussion of the technology at issue is based on the testimony and expert report of Andrew Rist. *Daubert* Hearing Tr. 5:21—170:5 (J.A. 3); Andrew Rist Expert Rep. (J.A. 6).

4 *Carpenter v. United States*, —— U.S. ——, 138 S.Ct. 2206, 2211, 201 L.Ed.2d 507 (2018).

5 *Id.*

6 Countless applications rely upon the location of devices to provide cell phone users with accurate local weather forecasts, driving directions, nearby restaurant recommendations and reviews, the location of a lost device, news headlines, and a myriad of other information.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

7 The Global Positioning System: GPS Overview, GPS. GOV, https://www.gps.gov/systems/gps/.

8 *Id.*

9 GPS Accuracy, GPS.GOV, https://www.gps.gov/systems/gps/performance/accuracy/.

10 *Id.*

11 *See, e.g.*, *United States v. Brooks*, 715 F.3d 1069, 1078 (8th Cir. 2013); *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010).

12 *Carpenter*, 138 S.Ct. at 2211.

13 *See* *Id.* at 2223.

14 *See* *Id.* at 2219.

15 *Taylor v. State*, 23 A.3d 851, 856 (Del. 2011) (finding no abuse of discretion where, after a *Daubert* hearing, the trial court allowed expert testimony on cell phone data mapping, a recognized process deemed reliable by the law enforcement community); *State v. Thompson*, I.D. No. 1602016732 (Del. Super. May 30, 2017) (TRANSCRIPT) (admitting historical cell site evidence and denying Defendant's *Daubert* Motion without a hearing).

16 Andrew Rist explains that when cell phones "see" access points, this means that the phone is in the presence of one or more Wi-Fi signals.

17 Paul A. Zandbergen, *Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning* (2009).

18 An example of crowd-sourcing technology is a navigational system that uses real-time information collected from individual drivers to notify other local drivers of traffic, motor vehicle accidents, potholes, and law enforcement speed monitoring and to re-route a driver to a more efficient route using the crowd-sourced information. Parmy Olson, *What Waze Adds to Google: A View from Waze's CEO* (June 13, 2013).

19 Unless noted otherwise, the Court's discussion of the proposed evidence placing Defendant at or near the murder scene is based on the testimony and report of Anthony Vega. *Daubert* Hearing Tr. 170:12—223:15 (J.A. 3); Anthony Vega Rep. (J.A. 11).

20 To satisfy the Fourth Amendment, a search warrant is required based on a finding of probable cause for a government search of a cell phone. *Carpenter*, 138 S.Ct. at 2221. There is no challenge in this case to the search warrants by which the surveillance video, Defendant's cell phone data, or Google Wi-Fi Location Data was acquired by the State.

21 An IMEI is a unique identifier for a cell phone made of numerical digits that identify the make, model, and serial number for each mobile device.

22 18 U.S.C. § 2703.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

23 *See* *Eskin v. Carden*, 842 A.2d 1222, 1231 (Del. 2004) (citing *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993)).

24 *Id.* at 1227 (quoting *Cunningham v. McDonald*, 689 A.2d 1190, 1193 (Del.1997)).

25 *Sturgis v. Bayside Health Ass'n Chartered*, 942 A.2d 579, 584 (Del. 2007).

26 *Rodriguez v. State*, 30 A.3d 764, 769 (Del. 2011) (quoting *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 152, 119 S.Ct. 1167, 143 L.Ed.2d 238 (1999)).

27 The State has identified state courts in Virginia, California, and Colorado, and a federal court in New York, that have permitted FBI Agents to offer testimony based on Google Wi-Fi Location Data, including where admissibility of the evidence was not challenged by the defendant, and one instance where a trial court in New York disallowed such evidence using the *Frye* standard. *United States v. Pizarro*, 17-CR-151, at 1319, 1337 (S.D.N.Y.) (TRANSCRIPT) (finding FBI CAST agent to be qualified as an expert in historical cell site analysis and admitting Google Wi-Fi Location Data without challenge); *Commonwealth of Virginia v. Rolland Ellisworth Anderson*, Cases No. CR17-4909, 4910, 4911, 4913-00F (Va. Cir. Ct. Jan. 8, 2019) (ORDER) (denying the defendant's motion *in limine* to preclude the commonwealth from presenting data reports and testimony concerning Google location services); *People of the State of Colorado v. Glen Law Galloway*, Case No. 16CR2749, at 2 (Colo. Dist. Ct. Mar. 6, 2018) (ORDER) (denying motion to preclude expert opinion testimony concerning Google Wi-Fi Location Data because the defendant's objections go to the weight of the evidence and not its admissibility); *The People of the State of New York v. Johnny Oquendo*, Indictment No. 16-1154, Index No. 254831, at 2 (N.Y. Sup. Ct. Oct. 26, 2017) (*citing* *Frye v. United States*, 293 F. 1013, 1014 (D.C. Cir. 1923)) (precluding evidence of Google Wi-Fi Location Data where the testifying witness was neither a scientist nor an engineer); *Commonwealth of Virginia v. Nathanial Howard Moone III*, CR-16000297-00, CR-16000298, at 11 (Va. Cir. Ct. June 8, 2016) (TRANSCRIPT) (admitting Google Wi-Fi Location Data without objection).

28 The Court rejects Defendant's argument that a long-running feud between Google and Oracle undermines Rist's credibility. To the contrary, as an employee of Oracle, Rist has no incentive to inflate the reliability or exaggerate the accuracy of Google's technology.

29 Unless noted otherwise, the Court's discussion of the technology at issue is based on the testimony and expert report of Andrew Rist. *Daubert* Hearing Tr. 5:21—170:5 (J.A. 3); Andrew Rist Expert Rep. (J.A. 6).

30 The test rig includes both Android and Apple phones. The Oracle team has also studied the information that is sent back to Apple from iPhones.

31 Defendant's challenge to the two-year gap between the data produced by Google for the Target Device and the data collected by Rist's test rig can be addressed by cross-examination. These challenges go to the weight of the evidence and not the admissibility. *Daubert*, 509 U.S. at 596, 113 S.Ct. 2786 ("Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence.").

32 Rist was not provided with the raw data produced by Google in response to the search warrant for the Target Device. Rather, the data collected and relied upon by Rist was gathered independently of the data produced by Google and utilized in Agent Vega's Powerpoint presentation.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

33 Piotr Sapiezynski, et al., *Tracking Human Mobility Using WiFi Signals* 9 (2015).

34 *Id.* at 3.

35 The pace of technology advances within the computer science field results in peer review different from the peer review process in other sciences, such as life sciences.

36 Any questions regarding the strength of each Wi-Fi signal goes to the weight and not the admissibility of the evidence. *Daubert*, 509 U.S. at 596, 113 S.Ct. 2786.

37 Defendant is not challenging the accuracy of the GPS data and concedes its accuracy.

38 The Carpenter Court noted the business purposes of collecting accurate CSLI data in its discussion of the reliability of that data. *Carpenter*, 138 S.Ct. at 2212.

39 The information collected by Google for any given device with a Google account is accessible at maps.google.com/timeline, although the information available at this site is less detailed than the information produced by Google in response to the search warrant in this case. *Daubert* Hearing Tr. 27:11—28:5 (J.A. 3).

40 *United States v. Reynolds*, 626 Fed.Appx. 610, 616 (6th Cir. 2015) (citing *Daubert,* 509 U.S. at 593-94, 113 S.Ct. 2786).

41 As recognized by the United States Supreme Court in *Carpenter*, cell-site records are generated for commercial purposes. *Carpenter*, 138 S.Ct. at 2217.

42 *See* *Id.* at 2218.

43 *Cunningham*, 689 A.2d at 1193.

44 *Carpenter*, 138 S.Ct. at 2220 (citing *Riley v. California*, 573 U.S. 373, 385, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014)).

45 D.R.E. 403.

End of Document © 2022 Thomson Reuters. No claim to original U.S. Government Works.

DNA Deception

When they were sued last year for storing baby blood samples without parental consent, Texas health officials said they'd done it for medical research. They never said they turned over the blood spots to the federal government to help build a vast DNA database. A Texas Tribune review of nine years' worth of e-mails and internal documents on the Department of State Health Services' newborn blood screening program, released after the state settled the case so quickly that it never reached the discovery phase, shows an effort to limit the public's knowledge of the program.

BY **EMILY RAMSHAW** FEB. 22, 2010 5 AM CENTRAL

COPY LINK



Rodolfo Clix

When state health officials were sued last year for storing infant blood samples without parental consent, they said it was for medical research into birth defects, childhood cancer and environmental toxins. They never said they were turning over hundreds of dried blood samples to the federal government to help build a vast DNA database — a forensics tool designed to identify missing persons and crack cold cases.

A Texas Tribune review of nine years' worth of e-mails and internal documents on the Department of State Health Services' newborn blood screening program reveals the transfer of hundreds of infant blood spots to an Armed Forces lab to build a national and, someday, international mitochondrial DNA (mtDNA) registry. The records, released after the state agreed in December to destroy more than 5 million infant blood spots, also show an effort to limit the public's knowledge of aspects of the newborn blood program, and to manage the debate around it. But the plaintiffs who filed the lawsuit never saw them, because the state settled the case so quickly that it never reached the discovery phase.

DSHS spokeswoman Carrie Williams says that while the department's general philosophy was to save blood spots for public health research, "we did not have an exclusive policy." She says DSHS participated in the project because officials believed it would help in missing-persons cases — and knew the blood spots could not be linked back to a particular individual. "Our understanding of mtDNA is that it's not used to pinpoint exactly who a person is, but can help determine origins," Williams says. "Our intentions were good ones."

But Jim Harrington, the civil rights attorney who filed the blood spot lawsuit last year on behalf of five Texas parents, believes DSHS meant to deceive the public. When he was negotiating with state officials, he says, he specifically asked what research the blood spots were being used for — and there was no mention of the federal mtDNA project. He says he was stunned by how quickly the state settled the lawsuit. "Sometimes there are slam-dunk cases, but I'd never seen this kind of case settle without discovery," says Harrington, director of the Texas Civil Rights Project. "This explains the mystery of why they gave up so fast."

The Texas Tribune thanks its sponsors. Become one.

For decades, the state has screened newborns for a variety of birth defects, pricking their heels and collecting five drops of blood on a paper card. Until 2002, the cards were thrown out after a short storage period. But starting that year, the state health department began storing blood spots indefinitely, for "research into causes of selected diseases." Four years later, DSHS began contracting with Texas A&M University's School of Rural Public Health to warehouse the cards, which were accumulating at a rate of 800,000 a year. State health officials never notified parents of the changes; they didn't need consent for the birth-defect screening, so they didn't ask for it for research purposes. The agency's rationale was that it let parents who asked opt out of the newborn blood screening and de-identified all of the samples before shipping them off.

Over the last several years, researchers have requested Texas baby blood spots for a variety of medical projects: to study the gene involved in club foot, to inspect the DNA of infants who develop childhood cancer, to examine prenatal lead exposure. Those are the projects state health officials have touted repeatedly before lawmakers and critics. But the least publicized of these research projects is arguably the most interesting. Between 2003 and 2007, the state gave 800 de-identified blood samples to the Armed Forces DNA Identification Laboratory (AFDIL) to help create a national mtDNA database.

MtDNA is extremely valuable in forensics because it's easier to find and extract from human cells than nuclear DNA. In addition to blood, it can be identified in hair, bones, teeth and damaged or degraded biological samples and can be used to identify victims of mass disasters or to solve long-since-cold criminal cases. But it's only as valuable as its sample size. AFDIL scientists, in conjunction with the research branch of the Justice Department, approached Texas in a $1.9 million effort to expand the country's mtDNA database — part of the President's DNA Initiative launched under George W. Bush. The researchers wanted "anonymous and maternally unrelated" blood samples from Texas Caucasians, African-Americans and Asians — and from Hispanics and Native Americans in particular — to round out their genetic record. The researchers also took samples from prison populations and infant blood screening in other states, including Florida, Minnesota and California. They did not pay Texas for the samples.

Eventually, research proposals indicate, federal officials hoped to be able to share this data worldwide, "for international law enforcement and investigation in the context of homeland security and anti-terrorism efforts."

Whether Texas officials were concerned about the perception of the project, or simply didn't think it was newsworthy, they never mentioned it. In

presentations, in public reports and in e-mails sent to reporters as recently as last year, state health officials never brought up the federal project — even when they discussed the merits of roughly two dozen medical research projects designed to "unlock the causes of childhood disorders" like autism and diabetes.

In November, when The Texas Tribune first filed an open-records request with DSHS to review blood spot records, the agency said the information requested was confidential. Two weeks later, when the lawsuit settlement was formally signed, the Tribune asked again, and this time the agency relented. But the box of documents officials turned over hardly referenced the mtDNA project, aside from a single e-mail referencing a "US Department of Justice/National Institute of Justice and the Armed Forces Institute of Pathology/Armed Forces DNA Identification Laboratory." When the Tribune pressed health officials about the missing research files, they produced them, saying it was an oversight, and that the documents had been overlooked in their initial search.

The Texas Tribune thanks its sponsors. **Become one**.

The records the agency initially released paint a portrait of an agency that walked on eggshells around the baby blood spot collection — from 2001, when lawmakers first debated whether to warehouse the cards, through last year, when they passed a law in response to the civil rights lawsuit giving parents better options to opt out.

In 2001, when the Legislature considered a newborn-blood-spot collection bill that state health officials didn't like, they took action. In an e-mail chain, an associate commissioner described how she and another official "planted questions" and "planted a note" with sympathetic lawmakers (former state Reps. Bob Glaze, D-Gilmer, and Glen Maxey, D-Austin) before a public hearing. "I suspect this bill will die …" wrote the official, who no longer works for the state. (The bill didn't make it out of committee.) Glaze couldn't be reached for

comment. Maxey said he couldn't recall the bill but routinely met with health department staffers to pick their brains about pertinent bills.

E-mails indicate that in 2003, when the agency started to release blood spots for outside research, officials knew they had a parental consent issue on their hands — but tried to avoid it. When a researcher proposed a project, the director of birth defects monitoring wrote that he'd "prefer to not have to go through" the process of getting consent. Another agency official responded that parents "never consented for blood spots to be used for research. … On the other hand, I believe [the health department] already uses (deidentified?) blood spots for some research, so that might not be a big deal."

In 2006, when the agency was beginning to store blood spots at Texas A&M, the university asked for permission to put out a press release announcing it. The agency balked. "What do you think of this idea? Makes me a bit nervous," the manager of the birth defects surveillance division wrote in an e-mail to five of his colleagues. Another responded: "This makes me nervous. Genetic privacy is a big ethical issue & even though … approval is required for use of the spots in most situations and great care is taken to protect the identity of the spots, a press release would most likely only generate negative publicity." One official asked the university not to do it; the university agreed.

When asked about the e-mails, agency officials said a decision not to send out a press release "isn't an indication of our level of openness." "We don't routinely do news releases about every agency initiative or contract," Williams says, "and obviously this is a sensitive topic." But they acknowledged that staff members are not permitted to "plant" questions with lawmakers. Given that the e-mail exchange happened in 2001, and that the employee no longer works for the agency, Williams says, "there is no way for me to definitively tell if there was any punishment."

Scientists say baby blood spot research is incredibly valuable, and that the genetic origins of human diseases can be traced through mtDNA samples if there are enough available. They say there are fail-safe methods for stripping identifying information from the samples, so they could never be used for illicit purposes. The problem, some say, is that scientists have used the public's unease with the subject as an excuse not to talk about it. "As scientists, we've failed in teaching people about genetics in the United States," says Dr. Bennett Van Houten, a molecular oncologist at the University of Pittsburgh Cancer Institute who formerly worked at the University of Texas Medical Branch in Galveston. "We need to work harder at that — at teaching them the facts."

Williams says that at the direction of lawmakers last session, parents now receive more information at the hospital about the storage and use of bloodspots and are given a better opportunity to opt out. While the agency is destroying more than 5 million baby blood spots collected before the new legislation took effect, she says, officials are not asking outside researchers —

including those at the Armed Forces lab — to return the samples they were given. But they must destroy them when they are done with them.

“The core mission is to screen all babies for life-threatening disorders,” Williams says. “We care deeply about this mission, and we have made some changes and are moving forward.”

The Texas Tribune thanks its sponsors. **Become one**.

Texas Tribune donors or members may be quoted or mentioned in our stories, or may be the subject of them. For a complete list of contributors, click here.

READ MORE

What Greg Abbott’s decisive win over Beto O’Rourke portends for his future

Pay raises alone won’t solve staffing shortages in “nightmare” Texas youth prisons, ex-workers say

Texas’ execution of Stephen Barbee was prolonged while officials searched for a vein

As Trump announces his run, Cruz and Cornyn signal openness to other GOP presidential candidates

Quality journalism doesn't come free

Perhaps it goes without saying — but producing quality journalism isn't cheap. At a time when newsroom resources and revenue across the country are declining, The Texas Tribune remains committed to sustaining our

mission: creating a more engaged and informed Texas with every story we cover, every event we convene and every newsletter we send. As a nonprofit newsroom, we rely on members to help keep our stories free and our events open to the public. Do you value our journalism? Show us with your support.

YES, I'LL DONATE TODAY

The Texas Tribune thanks its sponsors.
Become one.

© 2022 The Texas Tribune

590 F.Supp.3d 901
United States District Court, E.D. Virginia, Richmond Division.

UNITED STATES of America
v.
Okello T. CHATRIE, Defendant.

Criminal Case No. 3:19cr130
|
Filed 03/03/2022

Synopsis

Background: Defendant moved to suppress evidence obtained from geofence search warrant.

Holdings: The District Court, M. Hannah Lauck, J., held that:

[1] geofence warrant lacked particularized probable cause, but

[2] good-faith exception to exclusionary rule applied.

Motion denied.

Procedural Posture(s): Pre-Trial Hearing Motion.

West Headnotes (34)

[1] **Searches and Seizures** Complaint, Application or Affidavit

Presumption of validity exists with respect to affidavit supporting search warrant. U.S. Const. Amend. 4.

[2] **Searches and Seizures** Necessity for writing; oral presentation or supplementation

Searches and Seizures Scope of inquiry or review, in general

In determining the validity of a search warrant, the magistrate or magistrate judge, and a reviewing court, will restrict their inquiries on probable cause to the facts set forth in the four corners of the officers' sworn affidavit. U.S. Const. Amend. 4.

[3] **Searches and Seizures** Warrants

The Fourth Amendment requires that a search warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and, (3) be issued by a neutral, disinterested magistrate. U.S. Const. Amend. 4.

[4] **Criminal Law** Search or Seizure Under Warrant

If a search warrant is invalid, the proper remedy in a criminal action is ordinarily to suppress the evidence derived from it. U.S. Const. Amend. 4.

[5] **Searches and Seizures** Probable Cause

Whether probable cause for a search exists is a practical, common-sense question, asking whether there is a fair probability that contraband or evidence of a crime will be found in a particular place. U.S. Const. Amend. 4.

[6] **Searches and Seizures** Probable Cause

Probable cause for a search requires only the kind of fair probability on which reasonable and prudent people, not legal technicians, would rely. U.S. Const. Amend. 4.

[7] **Searches and Seizures** Probable or Reasonable Cause

Officers must present sufficient information to the magistrate judge to allow him or her to exercise independent judgment in determining whether probable cause for a search exists. U.S. Const. Amend. 4.

[8] **Searches and Seizures** Probable or Reasonable Cause

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Magistrate cannot simply ratify the bare conclusions of others in determining whether probable cause for search exists. U.S. Const. Amend. 4.

[9] **Searches and Seizures** Scope of inquiry or review, in general

When reviewing the probable cause supporting a search warrant, a reviewing court must consider only the information presented to the magistrate who issued the warrant. U.S. Const. Amend. 4.

[10] **Searches and Seizures** Scope of inquiry or review, in general

Duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause for search existed. U.S. Const. Amend. 4.

[11] **Searches and Seizures** Particularity or generality and overbreadth in general

Search warrant must be no broader than probable cause on which it is based. U.S. Const. Amend. 4.

[12] **Searches and Seizures** Places, objects, or persons to be searched

Search warrants must demonstrate good reason to suspect or believe that anyone present at anticipated scene will probably be participant in criminal activity. U.S. Const. Amend. 4.

[13] **Arrest** What constitutes such cause in general

Searches and Seizures Probable Cause

At base, probable cause demands that law enforcement possess reasonable ground for belief of guilt particularized with respect to person to be searched or seized. U.S. Const. Amend. 4.

[14] **Searches and Seizures** Probable Cause

Person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person. U.S. Const. Amend. 4.

[15] **Searches and Seizures** Particularity or generality and overbreadth in general

Search warrant must be sufficiently particular; thus, a warrant must confine the executing officers' discretion by allowing them to seize only evidence of a particular crime. U.S. Const. Amend. 4.

[16] **Searches and Seizures** Objects or information sought

Search warrant must identify the items to be seized by their relation to designated crimes, and the description of the items must leave nothing to the discretion of the officer executing the warrant. U.S. Const. Amend. 4.

[17] **Searches and Seizures** Objects or information sought

So long as search warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish between those items which are to be seized and those that are not, the particularity standard is met. U.S. Const. Amend. 4.

[18] **Telecommunications** Carrier's cooperation; pen registers and tracing

Assuming Government's collection of location data was search, geofence warrant that covered 70,686 square meters of land around bank located in busy part of metro area lacked particularized probable cause to search every mobile device user within geofence; warrant sought location information for all account owners who entered geofence over span of an hour, warrant was completely devoid of any suggestion that all, or even substantial number of, individuals searched had participated in or

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

witnessed robbery, and warrant captured location data for user who may not have been remotely close enough to bank to participate in or witness robbery. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[19] **Searches and Seizures** Probable Cause

Fourth Amendment's probable cause requirement for search demands more than mere propinquity to a crime. U.S. Const. Amend. 4.

[20] **Arrest** Grounds for warrantless arrest in general

Searches and Seizures Probable Cause

Particularized probable cause cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be. U.S. Const. Amend. 4.

[21] **Telecommunications** Carrier's cooperation; pen registers and tracing

Geofence search warrant's three-step process by which law enforcement would attempt to narrow down list of mobile device users for which Government would obtain most invasive information did not cure defects with warrant's particularized probable cause; steps two and three of warrant left executing officer with unbridled discretion and lacked any semblance of objective criteria to guide how officers would narrow list of users. U.S. Const. Amend. 4.

[22] **Searches and Seizures** Objects or information sought

Search warrant that meets particularity requirement leaves executing officer with no discretion as what to seize. U.S. Const. Amend. 4.

[23] **Searches and Seizures** Particularity or generality and overbreadth in general

Fourth Amendment discretion must be confined to signing magistrate, not executing officers or third party. U.S. Const. Amend. 4.

[24] **Searches and Seizures** Abandoned, surrendered, or disclaimed items

Under third-party doctrine, person generally has no legitimate expectation of privacy in information he or she voluntarily turns over to third parties.

[25] **Criminal Law** Searches, seizures, and arrests

Criminal Law Exclusionary rule as a personal or individual right

The exclusionary rule is neither a personal constitutional right nor is it designed to redress the injury occasioned by an unconstitutional search; rather, the exclusionary rule is a prudential doctrine created to compel respect for constitutional rights. U.S. Const. Amend. 4.

[26] **Criminal Law** Purpose of Exclusionary Rule

The exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence; where suppression would not produce deterrent benefits, the exclusionary rule does not apply.

[27] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

Evidence obtained pursuant to search warrant issued by neutral magistrate need not be excluded if officer's reliance on warrant was objectively reasonable. U.S. Const. Amend. 4.

[28] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Generally, the fact that a neutral magistrate has issued a warrant suffices to establish that a law enforcement officer has acted in good faith in conducting the search; therefore, searches carried out pursuant to a warrant rarely require any deep inquiry into reasonableness.

[29] **Criminal Law** Exceptions Relating to Defects in Warrant

When considering motion to suppress fruits of novel investigative technique, courts generally decline to hold warrant facially deficient where legality of investigative technique is unclear and law enforcement seeks advice from counsel before applying for warrant.

[30] **Criminal Law** Exceptions Relating to Defects in Warrant

Consultation with government attorneys prior to seeking search warrant is relevant consideration in determining whether warrant was facially deficient, for purposes of good-faith exception to exclusionary rule. U.S. Const. Amend. 4.

[31] **Criminal Law** Electronic surveillance cases

Good-faith exception to exclusionary rule applied to location data obtained as a result of geofence search warrant that lacked particularized probable cause; detective relied on approval of three prior geofence warrants, detective sought advice from Government attorneys before applying for warrant, when detective applied for warrant, no court had yet ruled on legality of such technique, and permissibility of geofence warrants was complex topic. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[32] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

Magistrate approval and consultation with the prosecution alone cannot and should not mechanically trigger the good-faith exception to exclusionary rule.

[33] **Criminal Law** Abandonment of judicial role or lack of neutrality

Good-faith exception to exclusionary rule primarily looks to whether magistrate overstepped his or her judicial responsibilities and compromised his judicial neutrality, by, for example, actively participating in investigation, retaining pecuniary interest in issuing warrant, rubber stamping a warrant that contained a bare bones affidavit, or failing to make bare bones assessment of validity.

[34] **Searches and Seizures** Impartial magistrate requirement

As general principle, states are entitled to some flexibility and leeway in their designation of magistrates, so long as all are neutral and detached and capable of probable cause determination required of them. U.S. Const. Amend. 4.

Attorneys and Law Firms

***904** Kenneth R. Simon, Jr., Peter S. Duffey, United States Attorney's Office, Richmond, VA, Nathan Paul Judish, Pro Hac Vice, United States Department of Justice Computer Crime and Intellectual Property Section, Washington, DC, for United States of America.

Laura Jill Koenig, Paul Geoffrey Gill, Office of the Federal Public Defender, Richmond, VA, Michael William Price, Pro Hac Vice, National Association of Criminal Defense Lawyers, Washington, DC, for Defendant.

MEMORANDUM OPINION

M. Hannah Lauck, United States District Judge

***905 I. Introduction**

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Ratified in 1791, the Fourth Amendment to the United States Constitution guarantees to the people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. To that end, the Framers prohibited the issuance of a warrant, unless that warrant was based "upon probable cause" and unless it "particularly describ[ed] the place to be searched, and the persons or things to be seized." *Id.* The Supreme Court of the United States has since applied the principles embodied in this language to constantly evolving technology —from recording devices in public telephone booths, *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); to thermal-imaging equipment, *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001); and, most recently, to cell-site location data, *Carpenter v. United States*, —— U.S. ——, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018).

This case implicates the next phase in the courts' ongoing efforts to apply the tenets underlying the Fourth Amendment to previously unimaginable investigatory methods. In recent years, technology giant Google (and others) have begun collecting detailed swaths of location data from their users. Law enforcement has seized upon the opportunity presented by this informational stockpile, crafting "geofence" warrants that seek location data for every user within a particular area over a particular span of time. In the coming years, further case law will refine precisely whether and to what extent geofence warrants are permissible under the Fourth Amendment. In the instant case, although the Motion to Suppress must ultimately be denied, the Court concludes that this particular geofence warrant plainly violates the rights enshrined in that Amendment.

II. Findings of Fact and Procedural History

A. Findings of Fact [1]

1. The Robbery at the Call Federal Credit Union

[1] On May 20, 2019, at approximately 4:52 p.m., a bank robbery occurred at the Call Federal Credit Union (the "Bank") in Midlothian, Virginia. The suspect held a firearm over the course of the robbery and took $195,000 from the Bank.

[2] During the robbery, the suspect presented a teller working at the Bank a handwritten note that stated:

> I've been watching you for sometime [sic] now. I got your family as hostage and I know where you live, [i]f you or your coworker alert the cops or anyone your family and you are going to be hurt. I got my boys on the lookout out ***906** side [sic]. The first cop car they see am going to start hurting everyone in sight, hand over all the cash, I need at least 100k and nobody will get hurt and your family will be set free. Think smartly everyone['s] safety is depending and you and your coworker[']s action so I hope they don't try nothing stupid.

(ECF No. 54-1, at 6.) [2] The teller told the suspect that she did not have access to that amount of money, and the suspect then displayed a silver and black firearm. While openly holding the gun, the suspect directed the teller, other Bank employees, and the Bank customers to move to the center of the lobby and get on the floor. The suspect then led these individuals behind the teller counter to an area that contained the Bank's safe. Once behind the counter, the suspect forced the Bank's manager to open the safe and place $195,000 into a bag he brought with him. After acquiring the money, the suspect left the Bank on foot, "towards an adjacent business, west of the [B]ank." (ECF No. 54-1, at 6.)

During its investigation, law enforcement obtained the instant Geofence Warrant (hereinafter "Geofence Warrant" or "Warrant")—a novel application of search technology whose use has grown exponentially in recent years. Google produced certain location information pursuant to the Warrant, which led the police to Okello Chatrie. Chatrie was eventually charged with two crimes related to the robbery. [3] He then filed a Motion to Suppress the Geofence Warrant that forms the basis of this Opinion.

2. The Record Presented to the Court by the Parties

There is a relative dearth of case law addressing geofence warrants.[4] In this case, the parties, especially the defense, pursued a thorough and deep record. This Court was aided by Amicus Google's provision of detailed information, including in-person ***907** testimony regarding the company's acquisition, retention, and use of users' location data. In what may be a first, Google filed an Amicus Brief.[5] Mr. Marlo McGriff, a Location History Manager at Google since 2016, submitted three declarations over the course of this matter. Ms. Sarah Rodriguez, a Team Lead for Legal Investigations Specialists ("LIS")[6] at Google since 2018, provided one declaration. During a hearing on March 4–5, 2021, (one of many in this case), the Court heard live testimony from both Mr. McGriff and Ms. Rodriguez.[7]

The parties to this case also brought their own experts. Spencer McInvaille, an expert in digital forensic examinations, forensics, and cellular location testified for the defense, and FBI Special Agent Jeremy D'Errico, a part of the cellular analysis survey team ("CAST") spoke for the Government. Multiple rounds of briefing occurred before, during, and after the hearings held by the Court.

In order to establish as thorough a record as possible with respect to this new technology, the Court will first discuss Google's location services, as well as Google's typical response to geofence warrants.[8]

3. Google's Collection and Production of Location Data

a. Google's Suite of Location Services

Google collects detailed location data on "numerous tens of millions" of its users. (ECF No. 96-1, at ¶ 13; ECF No. 201, at 205.) It acquires and stores this data through one of at least three services: (1) Location History, (2) Web and App Activity ("WAA"), and (3) Google Location Accuracy ("GLA"). Google only searches Location History when it receives a geofence warrant.

i. Location History

Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing *location* data. Google developed Location History to allow users to view their Location History data through its "Timeline" feature, a depiction of a user's collected Location History points over time. (ECF No. 96-1, at ¶ 5; *see* ECF No. 202, at 79.) According to Google, this permits Google account holders to "choose to keep track of locations they have visited while in possession" of their mobile device. (ECF No. 96-1, at ¶ 4.) Importantly, Location History also supports Google's advertising revenue.[9] For instance, McGriff testified that ***908** Location History data serves Google's advertising business by providing "store visit conversions" or "ads measurement" to businesses based on user location. (ECF 201, at 196–97.) Without identifying any individual user, this "store conversion" data can follow a particular ad campaign and identify "how many users who saw a particular ad campaign actually went to one of those stores." (ECF No. 201, at 197.) Google's "radius targeting" also allows—again without identifying any user—"a business to target ads to users that are within a certain distance of that business." (ECF No. 201, at 198.)

Location History is powerful: it has the potential to draw from Global Positioning System ("GPS") information, Bluetooth beacons, cell phone location information from nearby cellular towers, Internet Protocol ("IP") address information, and the signal strength of nearby Wi-Fi networks. According to Agent D'Errico, Location History logs a device's location, on average, every two minutes.[10] Indeed, Location History even allows Google to "estimat[e] ... where a device is in terms of elevation." (ECF No. 202, at 95.) McGriff testified that this capability helps locate someone in an emergency, or try to "determine if you are on the second [or first] floor of the mall" if the Google Maps directory has launched to help a user navigate indoors. (ECF No. 202, at 95–96.)

Google stores this data in a repository known as the "Sensorvault" and associates each data point with a unique user account. (ECF No. 201, at 130.) The Sensorvault contains a substantial amount of information. McGriff testified that the Sensorvault assigns each device a unique device ID—as opposed to a personally identifiable Google ID—and receives and stores *all* location history data in the Sensorvault to be used in ads marketing. Google then builds aggregate models within the Sensorvault with data that is transformed so that it no longer looks like user data, and then uses the data to, for instance, assist decision-making in Google Maps. As another example, Google uses this data to depict whether certain locations are busy during particular hours. Both McGriff and Rodriguez declared that, to identify

users within the relevant timeframe of a geofence, Google has to compare *all* the data in the Sensorvault in order to identify users within the relevant timeframe of a geofence. (ECF No. 96-1, at ¶ 23 ("Google must search across *all* [Location History] data," and "run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant."); ECF No. 96-2, at ¶ 7 ("Google must conduct the search across *all* [Location History] data.").) Clearly, however, Google can alter the data back to identify users in response to a geofence warrant.

Still, Location history is off by default. A user can initiate, or opt into, Location History either at the "Settings" Level, or when installing applications such as Google Assistant, Google Maps, or Google Photos. Although the specific software pathway each user sees at any given moment can differ based on numerous factors, McGriff acknowledged that it was "possible that a user would have seen the option" to opt ***909** into Location History multiple times across multiple apps. (ECF No. 202, at 77–78.) For instance, Google may prompt the user to enable Location History first in Google Maps, then again when he or she opens Google Photos and Google Assistant for the first time. [11]

Once a user opts into Location History, Google is "always collecting" data and storing *all* of that data in its vast Sensorvault, even "if the person is not doing anything at all with [his or her] phone." (ECF No. 201, at 114–15; *see* ECF No. 201, at 115 ("Once enabled, [Google is] now collecting [the user's] location history all the time.").) Even if a user enables Location History through an application and later deletes that app, Location History will "still collect[ ]" data on the user because Location History is tied to an individual's Google *account*, not to a *specific app.* (ECF No. 201, at 123–24.) Thus, after a user opts into the service, Location History tracks a user's location across every *app* and every *device* associated with the user's account. Approximately one-third of all active Google users have Location History enabled on their accounts.

In certain circumstances, Google can estimate a device's location down to three meters. Location History cannot, however, pinpoint an individual's location with absolute precision. Instead, Google *estimates* a phone's coordinates. When Google, through Location History, reports a device's estimated location by placing a point on a map, it also depicts around that point a "confidence interval"—a circle of varying sizes—which indicates Google's confidence in its estimation. (ECF No. 201, at 38, 212; ECF No. 202, at 253–54.) The smaller the circle around a phone's estimated location, the more confident Google is in that phone's exact location, and *vice versa.* In general, "Google aims to accurately capture roughly 68 percent of users" within its confidence intervals. (ECF No. 201, at 213.) "[I]n other words, there[is] a 68 percent likelihood that a user is somewhere inside" the confidence interval. (ECF No. 201, at 213.)

ii. Web and App Activity

Web and App Activity collects a wider variety of information than Location History. If a user opts into WAA and has authorized all other requisite device permissions, WAA collects certain data points when a user *affirmatively engages* in certain activities. [12] For example, when a user performs a Google search, Google may, through WAA, keep a record of that search so that it can "automatically suggest[ ]" that search to the user at a later time. (ECF No. 96-1, at ¶ 16.) Google maintains that WAA allows a user to "experience faster searches and more helpful app and content recommendations." (ECF No. 96-1, at ¶ 16.) "Some of [the data obtained through WAA] can include location information, although the source of the location information will vary depending on the activity, the device, and the user's other settings." (ECF No. 96-1, at ¶ 16.) Location History "and WAA are separate services that store data in separate databases." (ECF No. 96-1, at ¶ 16.) That is, "WAA data is not used to calculate the locations that are stored in [Location History], and completing a search across [Location History] data does not search or ***910** draw on WAA data in any way." (ECF No. 96-1, at ¶ 16.)

iii. Google Location Accuracy

Lastly, Google Location Accuracy—only available on Android devices [13]—allows a user's phone to draw in location data from sources other than GPS information. "If a user has the GLA setting on, the Android[device's] location services will use additional inputs, including Wi-Fi access points, mobile networks, and sensors[ ] to estimate the device's location." (ECF No. 96-1, at ¶ 17.) Thus, "the device 's location information that is sent to and stored in [Location History] ... may be calculated using not only GPS-sourced data, but also [more detailed] WiFi-or cell-sourced data from the GLA database." (ECF No. 96-1, at ¶ 17.) "In other words, GLA data might be used by the device to calculate a [more

precise] location data point that is then stored in [Location History].” (ECF No. 96-1, at ¶ 17.) Like WAA, Google generally stores GLA data separate from Location History information.

Again, as a general matter, Google appears to draw only from Location History to produce records for geofence requests, as WAA and GLA do not collect enough data points to pinpoint “devices within a certain period of time within a certain radius.” (ECF No. 202, at 138; *see* ECF No. 201, at 211; ECF No. 96-1, at ¶¶ 20–22.) In keeping with this principle, here, Google only produced to law enforcement information from its Location History database.

b. Enabling Location History

The Court reports its understanding of the software pathways necessary to enable Location History based on two sets of sources. All sources agree that Chatrie enabled his Location History on July 9, 2018. However, even with input from two knowledgeable witnesses, the record as to how users can and do—and how Chatrie in particular could and did—enable Location History is not definitive on this record.

First, Defense Expert Spencer McInvaille testified in Court using a video of a device employing what was likely the same software used by Chatrie's phone to demonstrate how one might activate Location History through the Google account setup or through an app such as Google Maps. (Jan. 21 Hr'g Def. Ex. 4 (“Opt-In Video”).) McInvaille also offered a written report explaining how Chatrie may have enabled location history. In that report, McInvaille reported that Chatrie most likely enabled LH using Google Assistant, and that it was enabled on July 9, 2018.

Second, Google Location History Product Manager Marlo McGriff filed three declarations that explain how Google collects, stores, and turns over Location History data. He also testified in person during the March 4–5 Suppression Hearing. In his second declaration, McGriff concedes that McInvaille's video exhibit depicts largely accurate pathways to enable Location History. But McGriff states that McInvaille's video is incomplete. McGriff notes that “[b]y 2017 at the latest, it was not possible for a user to unable [Location History] solely by tapping on ‘YES, I'M IN’ as depicted on the final screen in the McInvaille Video.” (ECF No. 110-1, at ¶ 7.) Instead, “a user who tapped on ‘YES, I'M IN’ ... would be presented with a second opt-in screen” described above. (ECF No. 110-1, at ¶ 7.) McGriff presents the Court with the exact text of the second opt-in screen in his Third Declaration. [14] (ECF ***911** No. 147, at ¶¶ 7–8; *see* ECF No. 147, at ¶ 10 (“The text quoted in ¶¶ 7–8 is the same text that [Chatrie] would have seen on July 9, 2018.”).

No expert could say *exactly* which software pathway Chatrie would have seen when he enabled Location History, nor could Google determine which app he used to turn the service on. Google does, however, accept that Chatrie would have seen the informational text in Part II.A.3.b.ii (“Through an App”) in *some* form.

i. Through Phone Setup

As mentioned, a user must affirmatively enable Location History before Google uses the service to log the user's whereabouts. Google first allows users to enable Location History during the initial Google account setup process. After a new user connects the phone to the internet, agrees to the phone manufacturer's terms and conditions, and inputs the necessary information to create a Google account, the interface displays Google's terms of service. (*See* ECF No. 110-1, at ¶ 5 (acknowledging that the Opt-In Video exhibit was accurate but incomplete).) To move past this screen, the user must scroll through a summary of Google's privacy terms until the user reaches the bottom of the page. This page “does [not] ... say anything about [L]ocation [H]istory.” (ECF No. 81, at 51.) Near the bottom, the screen displays blue text that reads, “MORE OPTIONS,” with a downward-facing arrow next to the text. (Opt-In Video 3:00.) If the user taps on “MORE OPTIONS,” the interface displays additional information about Google's location services. (ECF No. 81, at 51.) This additional information informs the user that WAA and GLA are enabled by default. Although Location History is *not* enabled by default, the user can opt into it from this screen by checking a box.

ii. Through an App

If a user does not enable Location History while setting up his or her Google account, Google will also prompt the user to turn the service on as soon as he or she sets up an app “that has [Location History]-powered features.” (ECF No. 110-1, at ¶ 5; *accord* ECF No. 96-1, at ¶¶ 3–6; ECF No. 201, at 221; ECF No. 202, at 8–9.) Such apps include Google Maps, Google Photos, and Google Assistant. When a user opens one of these

apps for the first time, the phone immediately directs the user to a bright blue screen that reads: "Get the most from Google Maps." (Opt-In Video 4:36.) This screen informs the user that "Google needs to periodically store [his or her] location to improve route recommendations, search suggestions, and more." (Opt-In Video 4:36.) Below that, the interface offers the user the option to "LEARN MORE." (Opt-In Video 4:36.) If the user taps "LEARN MORE," the page redirects to "[a]ll of [Google's] terms and conditions"—but these terms and conditions include no information specifically tailored to location information. (ECF No. 81, at 57.)

Back at the initial blue page, the user can either select "YES, I'M IN" or "SKIP." (Opt-In Video 4:36.) As of July 2018, once the user selects "YES, I'M IN," the interface redirects the user to another page that displays the following text:

> **Location History**
>
> Saves where you go with your devices v [15]
>
> ***912** This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

(ECF No. 147, at ¶ 7 (bold in original).) Next to "Location History: Saves where you go with your devices," the interface includes an "expansion arrow," depicted in the above text with a downward-facing caret. (ECF No. 147, at ¶ 8.) If a user "tap[s] on [this] expansion arrow," the interface "present[s the user] with additional information about" Location History. (ECF No. 147, at ¶ 8.) The screen then reads:

> **Location History**
>
> Saves where you go with your devices
>
> Location History saves where you go with your devices. To save this data, Google regularly obtains location data from your devices. This data is saved even when you aren't using a specific Google service, like Google Maps or Search.
>
> If you use your device without an internet connection, your data may be saved to your account once you return online.
>
> Not all Google services save this data to your account.
>
> This data helps Google give you more personalized experiences across Google services, like a map of where you've been, tips about your commute, recommendations based on places you've visited, and useful ads, both on and off Google.
>
> This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com.
>
> NO THANKS TURN ON

(ECF No. 147, at ¶ 8 (bold in original).) If the user selects "TURN ON"—either in the original screen or this expanded version—Location History is enabled. (ECF No. 147, at ¶ 9.) Importantly, a user need not interface with or employ the expansion arrow to enable Location History. In other words, a user could activate the service without knowing any of the further details of the service as explained in the above expanded version.

As noted, Chatrie enabled Location History on his device on July 9, 2018 at 12:09 a.m. Eastern Standard Time, and he appears to have done so through Google Assistant.

c. "Pausing" and Trying to Delete Location History

After a user opts in, he or she has two mechanisms to manage Google's collection and retention of his or her Location History data: "pausing" the service, or deleting the information it collected.

i. Pausing

As Google Location History Product Manager Marlo McGriff explained, when a user "*pauses*" his or her Location History, it merely "halts the collection of future data;" *it does not delete* information Google has already obtained. (ECF No. 202, at 84.) And deleting an app through which the user enabled Location History will not pause the service.

A user may pause Location History on an Android device in one of three locations. First, the user can pause it "through the settings on any particular app that uses Location History." (ECF No. 202, at 63.) Second, he or she can pause it by navigating "through the device level settings." (ECF No. 202, at 63.) Finally, the user can log into myactivity.google.com and change his or her location settings. For each of these options, "a user [must] actively,

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

intentionally ***913** navigate" through each interface. (ECF No. 202, at 64.)

When a user attempts to pause Location History, the device will present a pop-up screen containing text called the "pause copy." (Mar. 4–5 Hr'g Def. Ex. 27, at 23.) The pause copy warns users that pausing Location History will "limit[ ] functionality of some Google products over time, such as Google Maps and Google Now." (Mar. 4–5 Hr'g Def. Ex. 27, at 23; *accord* ECF No. 202, at 66.) Yet the record suggests that apps such as Google Assistant *will* continue to function with Location History paused. For instance, McInvaille noted that, despite prompts from Google to initiate Location History because apps like Google Assistant "depen[d] on these settings in order to work correctly," the user does not "need Location History for [Google Assistant] to work." (ECF. No. 201, at 111, 113.)

The pause copy also does not specifically detail how app functionality might be limited. Nor does Google inform users of the fact that the app will, indeed, continue to function without Location History enabled, either when setting up the application or when displaying the pause copy. McGriff confirmed that when a user "pauses" the service, it halts only the collection of future data, and it does not (if a user has opted in) pause other location services such as Web & App Activity. (ECF No. 202, at 84, 90.)

ii. Trying to Delete

In 2018, when Chatrie enabled his Location History, a user had only one option to *delete* his or her Location History: by visiting myactivity.google.com and viewing his or her Timeline. Through the Timeline, a user "can review, edit, or delete [his or] her [Location History data] at will." (ECF No. 96-1, at ¶ 15.) But in response to an article from the Associated Press criticizing Google's acquisition of location data, one Google employee apparently remarked through an email: "The current [User Interface as of August 13, 2018] *feels* like it is designed to make things *possible*, yet *difficult* enough that people won't figure ... out" how to turn Location History off. [16] (Mar. 4–5 Hr'g Def. Ex. 30, at 6 (emphasis added).) Whether the substance of this remark is true or not, the sentiment it expresses is certainly not inconsistent with the record before the Court.

The effort to clarify this interface obviously is ongoing at Google. [17] In May 2019, ***914** McGriff formally heralded the "autodelete" controls that made it easier for users to manage their data. (*See* Mar. 4–5 Hr'g Def. Ex. 46.) And in December of 2019, McGriff introduced, on behalf of Google, "Incognito mode" and "Bulk delete in Timeline." (*See* Mar. 4–5 Hr'g Def. Ex. 47.)

d. Google's Process in Answering a Geofence Warrant

Geofence warrants represent "a novel but rapidly growing [investigatory] technique." (ECF No. 59-1, at 8.) When law enforcement seeks a geofence warrant from Google, it (1) identifies a geographic area (also known as the "geofence," often a circle with a specified radius), (2) identifies a certain span of time, and (3) requests Location History data for all users who were within that area during that time. (*See* ECF No. 96-2, at ¶ 4.) The requested time windows for these warrants "might span a few minutes or a few hours." (ECF No. 96-2, at ¶ 4.)

In recent years, the number of geofence warrants received by Google has increased exponentially. Google received its first in 2016. After that, Google "observed over a 1,500% increase in the number of geofence requests it received in 2018 compared to 2017; and the rate ... increased over 500% from 2018 to 2019." (ECF No. 59-1, at 8.) In 2019, Google received "around 9,000 total geofence requests." [18] And Google now reports that geofence warrants comprise more than twenty-five percent of *all* warrants it receives in the United States. Google, *Supplemental Information on Geofence Warrants in the United States* (last visited Mar. 1, 2022), https://bit.ly/3***o***7Znqc.

Google began to take issue with certain early geofence warrants because the requests were too broad. As related by Legal Investigations Specialist Rodriguez, the warrants "sought [Location History] data that would identify *all* Google users who were in a geographical area in a given time frame." (ECF No. 96-2, at ¶ 5 (emphasis added).) Thus, in 2018, Google held both internal discussions with its counsel and external discussions with law enforcement agencies, including the Computer Crime and Intellectual Property Section of the United States Department of Justice ("CCIPS"), to develop internal procedures on how to respond to geofence warrants. "To ensure privacy protections for Google users, ... Google instituted a policy of objecting to any warrant that failed to include de[-]identification and narrowing measures." (ECF No. 96-2, at ¶ 5.) Seemingly developed as a result of Google's collaboration with CCIPS,

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

this de-identification and narrowing "protocol typically ... entails a three-step process." (ECF No. 96-2, at ¶ 5; *see* ECF No. 202, at 553.) As noted earlier, the Court draws its understanding of this process from an amalgam of in-person testimony and a declaration submitted by current Google Tooling and Programs Lead and former Legal Specialist Sarah Rodriguez.

i. Step 1

First, at Step 1, law enforcement receives a warrant "compelling Google to ***915** disclose a *de-identified* list of all Google user[s]" whose Location History data indicates were within the geofence during a specified timeframe. (ECF No. 96-2, at ¶ 6 (emphasis added).) In response to the warrant, Google must "search ... *all* [Location History] data to identify users" whose devices were present within the geofence during the defined timeframe. (ECF No. 96-2, at ¶ 7; ECF No. 96-1, at ¶ 23.) "Google does not know which users may have ... saved [Location History] data before conducting th[is] search." (ECF No. 96-2, at ¶ 7.)

Rodriguez stated that, as part of this first step, Google provides the Government with responsive user records identified in the Sensorvault. Google deems a record "responsive" if a user's estimated location (*i.e.*, the stored coordinates of the phone in Location History) falls within the boundaries of the geofence. (ECF No. 96-1, at ¶ 25.) Rodriguez confirmed that, for every device whose "stored latitude/longitude coordinates fall within the radius described in the warrant," Google turns over a " 'production version' of the [users'] data." (ECF No. 96-2, at ¶ 8.) This production version "includes a [de-identified] device number, [19] the latitude/longitude coordinates and timestamp of the stored [Location History] information, the map's [confidence interval], and the source of the stored [Location History]," (*i.e.*, "whether the location was generated via Wi-Fi, GPS, or a cell tower"). (ECF No. 96-2, at ¶ 8.)

According to Rodriguez, the sizes and timeframes of geofences "vary considerably from one request to another." (ECF No. 96-2, at ¶ 8.) Because Google produces *all* location points captured within the geofence over the timeframe, "[t]he volume of data produced at [Step 1] depends on the size and nature of the geographic area and length of time covered by the geofence request." (ECF No. 96-2, at ¶ 8.) Google does not impose specific, objective restraints on the size of the geofence, the length of the relevant timeframe, or the number of users for which it will produce data.

Indeed, Google places significant discretion on the LIS employee who initially reviews a particular geofence warrant. This "specialist" will first process and review the warrant. (ECF No. 202, at 178–79.) If the specialist believes the warrant "needs further review"—for example, if the geofence seems too large or the timeframe too long—he or she may first "engage with [the requesting] law enforcement officer to collect more information about the investigation." (ECF No. 202, at 179, 182.) From there, the specialist will "consult with [Google's] legal counsel." (ECF No. 202, at 179.) If Google's counsel objects to the warrant, Google may have a "conversation" with law enforcement to alleviate Google's concerns, or it may "require law enforcement to obtain an amended or a newly-issued warrant that addresses the issue." (ECF No. 202, at 187.) Assuming law enforcement eventually assuages Google's concerns with the ***916** warrant, Google then provides the Government with the de-identified geofence data.

ii. Step 2

Second, according to Rodriguez, at Step 2, the Government "reviews the de[-]identified [data] to determine the [Sensorvault] device numbers of interest." (ECF No. 96-1, at ¶ 10.) If law enforcement needs "additional de[-]identified location information for a [certain] device" to "determine whether that device is actually relevant to the investigation," law enforcement, at this step, "can compel Google to provide additional ... location coordinates *beyond* the time and geographic scope of the original request." [20] (ECF No. 96-2, at ¶ 10 (emphasis added).) These additional location points "can assist law enforcement in eliminating devices" from the investigation that were, for example, "not in the target location for enough time to be of interest, [or] were moving through the target location in a manner inconsistent with other evidence." [21] (ECF No. 96-2, at ¶ 11.) Notably, Google imposes "no geographical limits" on this Step 2 data. (ECF No. 202, at 184.) Thus, if a user's location fell within the geofence at Step 1, law enforcement can obtain *all* location points for identified users over an expanded timeframe at Step 2. This means that, at Step 2, no geographic barrier confines the information searched.

Google does, however, typically require law enforcement to narrow the number of users for which it requests

Step 2 data so that the Government cannot not simply seek geographically unrestricted data for *all* users within the geofence. Google has no firm policy as to precisely *when* a Step 2 request is sufficiently narrow. But if law enforcement requests "a lower number of devices from St[ep] 1 to St[ep] 2," this, to some extent, demonstrates to Google that law enforcement has tailored the data it seeks. (ECF No. 202, at 190.) Again, assuming Google has no further objections to law enforcement's Step 2 request, Google provides law enforcement with de-identified but geographically unrestricted data.

iii. Step 3

Finally, at Step 3, drawing from the de-identified data Google has produced so far, "the [G]overnment can compel Google ... to provide *account-identifying information"* for the users "the [G]overnment determines are relevant to the investigation." (ECF No. 96-2, at ¶ 12 (emphasis added).) [22] This "account-identifying information" includes the name and email address associated with the account. (ECF No. 96-2, at ¶ 12; ECF No. 202, at 192.) Google seems to prefer that law enforcement request Step 3 data on fewer users than requested in Step 2, although it is "[p]ossibl[e]" that Google would approve a Step 3 request that is not narrowed after Step 2 at all. (ECF No. 202, at 194.)

4. The Instant Geofence Warrant and Its Justifications

a. Det. Hylton's Investigation [23]

When Det. Hylton responded to the scene of the bank robbery on May 20, ***917** 2019, he "interviewed witnesses" and "reviewed surveillance camera video from ... the Call Federal Credit Union Bank." (ECF No. 202, at 330.) Through this initial investigation, he "learned that [the] suspect had come from the southwestern corner of the Journey Christian Church [the 'Church'], ... a building adjacent and to the east of the Call Federal Credit Union, at approximately 4:50 in the afternoon." (ECF No. 202, at 330–31.) He also learned of the core facts that underlie this case—that the suspect walked into the Bank wearing a fisherman's hat and traffic vest, presented the teller with a note demanding $100,000, forced the manager at gunpoint to open the Bank's vault, took $195,000, and may have left in a blue Buick Lacrosse. Critically, through security footage, Det. Hylton observed that when the suspect first walked into Bank, he was "holding what appeared to be ... a cell phone to the side of his face." (ECF No. 202, at 331.) To Det. Hylton, this use of a phone suggested "that [the suspect] could have possibly been speaking with a coconspirator." (ECF No. 202, at 333.)

After Det. Hylton completed his on-site investigation, he pursued at least two other leads. First, a purportedly estranged romantic partner called the police and told them that she "kn[e]w who did th[e] robbery," and that the suspect was her "ex-boyfriend." (ECF No. 202, at 334.) Law enforcement found this ex-boyfriend, interviewed him, examined his cell phone, and ultimately determined that he was not the suspect. Next, an employee at another branch of the Bank alerted the police about an individual who drove a blue Buick Lacrosse and wore a traffic vest. Det. Hylton ultimately determined that this individual was likewise not the suspect.

Having unearthed no further leads from his investigation, Det. Hylton then turned to geofence technology. He had sought three other geofence warrants in the past. Before seeking those warrants, he had consulted with prosecutors, who approved them. Magistrates—including one federal magistrate judge—approved all three as well. Those warrants were, according to Det. Hylton, "mostly similar" to the one at bar. (ECF No. 202, at 328; *compare* Mar. 4–5 Hr'g Def. Ex. 18 ("Prior Federal Geofence Warrant") and Mar. 4–5 Hr'g Def. Ex. 19 ("Prior State Geofence Warrant") *with* ECF No. 54-1.) Indeed, all but one adopted a roughly 150-meter radius, although a "few of them had more locations because [there were] more robberies to investigate." (ECF No. 202, at 328; *see* Prior Federal Geofence Warrant; Prior State Geofence Warrant.)

On June 14, 2019, roughly three weeks after the robbery, Det. Hylton applied for and obtained the instant Geofence Warrant from Chesterfield County Magistrate David Bishop.

b. Magistrate Bishop

Chatrie contests the sufficiency of Magistrate Bishop's qualifications. Although the Court will address that issue more fully later in this Opinion, the Court briefly notes that Chesterfield County Magistrate "David Bishop graduated from Pensacola Christian College with a Bachelor's of Science in Criminal Justice in May 2016." [24] ***918** (ECF No. 156, at 1.) Around two years later, on June 12, 2018, the Executive Secretary of the Supreme Court of

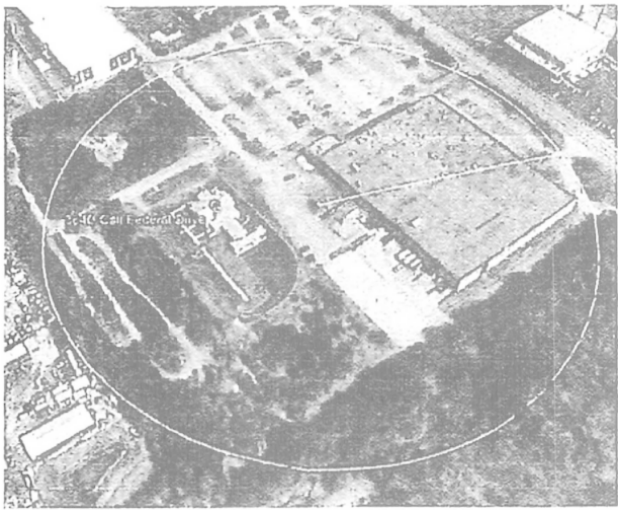
Virginia appointed Bishop as a magistrate. Magistrate Bishop completed his statutorily required probationary period on March 12, 2019. He was released for service on October 24, 2018.

Three months after Magistrate Bishop finished his probationary period, Det. Hylton presented Magistrate Bishop with the instant Geofence Warrant. When Magistrate Bishop reviewed the Warrant, he asked no questions of Det. Hylton, nor did he "seek to modify anything in the affidavit." (ECF No. 202, at 362.) Based on Det. Hylton's understanding, Magistrate Bishop simply "read [the Warrant] and signed it."[25] (ECF No. 202, at 362.) The record suggests that this was the first geofence warrant Magistrate Bishop had signed.

c. The Instant Geofence Warrant

The Warrant drew a geofence with a 150-meter radius—with a *diameter* of 300 meters, longer than three football fields—in an urban environment which included the Bank and the nearby Journey Christian Church.[26] All told, the geofence encompassed 17.5 acres. The eastern side of the geofence abutted but did not include Price Club Boulevard. The southern side encompassed a wooded area behind the Bank. The northern side encircled the Church's parking lot, and the western side captured a wooded area to the west of the Bank. The Warrant included the following photograph of the area with the geofence superimposed over it:

***919**



The Warrant sought location data for every device present within the geofence from 4:20 p.m. to 5:20 p.m. on the day of the robbery. In keeping with Google's established approach, the Geofence Warrant described a three-step process by which law enforcement would "attempt to narrow down" the list of users for which the Government would obtain the most invasive information. (ECF No. 54-1, at 4.)

At Step 1, "Google w[ould] provide 'anonymized information' regarding the Accounts that are associated with a device that was inside the described geographical area" from 4:20 p.m. to 5:20 p.m. (ECF No. 54-1, at 4.) At Step 2, "Law enforcement w[ould] return a list [of accounts] that they ha[d] attempted to narrow down." (ECF No. 54-1, at 4.) Google would then "produce contextual data points with points of travel outside of the geographical area." (ECF No. 54-1, at 4.) During Step 2, the warrant expanded the timeframe to include thirty minutes before and thirty minutes after the initial hour-long window, so that the Step 2 window was two hours long in total. (ECF No. 54-1, at 4.) Finally, at Step 3, after Government review, Google would "provide identifying account information/CSI[27] for the accounts requested" by law enforcement. (ECF No. 54-1, at 4–5.)

***920** In explaining why "Google [should] provide Geo[f]encing data," Det. Hylton noted in the warrant's accompanying affidavit that:

> when people act in concert with one another to commit a crime, they frequently utilize cellular telephones and other such electronic devices, to communicate with each other through WiFi, Bluetooth, GPS, voice calls, text messages, social media accounts, applications, emails, and/or cell towers in the area of the [crime].

(ECF No. 54-1, at 6.) Specifically, he noted that when reviewing the Bank's surveillance footage, he observed that the perpetrator "had a cell phone in his right hand and appeared to be speaking with someone on the device." (ECF No. 54-1, at 6.) He further explained that:

> Google has ... developed a proprietary operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android

> operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.
>
> Based on [his] training and experience, [he has learned] that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled.

ECF No. 54-1, at 7.) Therefore, he explained, "the requested data/information would have been captured by Google during the requested time." (ECF No. 54-1, at 6.) Det. Hylton noted several ways law enforcement could use this information. For example, "location data ... may tend to identify potential witnesses and/or suspects." (ECF No. 54-1, at 7.) In turn, this geographic and timeline information may tend to "inculpat[e] or exculpate[e] persons of interest." (ECF No. 54-1, at 7.)

Inexplicably, on June 19, 2019—*the day before he sent the Warrant to Google*—Det. Hylton submitted his return for the Warrant to the Chesterfield County Circuit Court. A search warrant return "notifies the Court when [an officer] *execute*[*s*] a search warrant," and the officer "report[s] back to the Court what items [he or she] gathered during the search." (ECF No. 202, at 366-68 (emphasis added).) In the return, he stated that he had executed the warrant on June 14, 2019. Yet he had not yet sent the Warrant to Google. Moreover, in describing the items *already seized* under the Warrant—again, he had not yet executed it—Det. Hylton wrote for what would be a sizable amount of precise location information on at least nineteen device users: "Data." (Mar. 4–5 Hr'g Gov't Ex. 2, at 9; *see* ECF No. 202, at 367, 369); *see also* *United States v. Williams*, 592 F.3d 511, 520 (4th Cir. 2010) ("While the [Fourth Amendment's] protection cannot demand perfection, any tolerance of imperfection does not give officers free reign to ransack and take what they like." (citation and quotation marks omitted)).

5. Google Receives the Geofence Warrant

The next day, on June 20, 2019, Det. Hylton sent Google the Warrant that Magistrate Bishop had approved. Pursuant to Step 1, Google produced anonymized Location History data for all accounts associated with phones present within the geofence from 4:20 p.m. to 5:20 p.m.—nineteen users in total.[28] Associated with these nineteen users were 210 individual location points, along with the confidence ***921** interval for each point. In this case, law enforcement ran this information through a program to produce a visual representation of the data. *See* Part II.A.6.a, *infra.*

A few days after Google provided him the Step 1 information, Det. Hylton emailed Google. The record then strongly suggests that he did not "attempt to narrow down" the list of devices for which he requested further data. In contravention to Google's policy, and without consulting Magistrate Bishop, Det. Hylton requested "additional location data" (Step 2 data) *and* "subscriber information" (Step 3 data) "for *all* 19 device numbers produced in [S]tep 1." (ECF No. 48-1, at 1; *accord* ECF No. 96-2, at ¶ 15; ECF No. 202, at 195, 345.) He noted that, because "the sought Google devices [were] fairly low in number," he requested Step 2 and 3 data for *all* nineteen users "in an effort to rule out possible co-conspirators." (ECF No. 48-1, at 1; *see* ECF No. 202, at 195.) He admitted, however, that "device numbers 1–9 may fit the more likely profile of [the] parties involved." (ECF No. 48-1.) Six days after sending the email, Det. Hylton called Google and left two voicemails seeking a response.

A Google specialist then called Det. Hylton. As described by Rodriguez, the LIS "explained the issues" with Det. Hylton's request—namely, that the request "did not appear to follow the three sequential steps or the narrowing required by the search warrant." (ECF No. 96-2, at ¶ 16; *see* Mar. 4–5 Hr'g Tr. 189, 197.) "Det. Hylton asked ... what information would be produced in [S]tep 2 and ... [S]tep 3." (ECF No. 96-2, at ¶ 16.) The Google specialist explained the nature of the data to be turned over during these steps and emphasized to Det. Hylton "the importance of [S]tep 2 in narrowing." (ECF No. 96-2, at ¶ 16; *see* ECF No. 202, at 197.) The specialist, however, does not appear to have provided Det. Hylton with any "specific directive[s] ... about how much [Det. Hylton] had to narrow" his request. (ECF No. 202, at 197.) On July 9, 2019, Det. Hylton emailed Google, requesting Step 2 data on the *nine* users identified in his prior email. Google then provided him that information in the same format as Step 1 data had been returned. It does not appear that Det. Hylton explained to Google precisely why he requested Step 2 data for these nine particular accounts. Neither Det. Hylton nor Google consulted with a magistrate or judge before Google disclosed this data.

"On or about July 10, 2019, and July 11, 2019, Google received emails from [Det.] Hylton requesting [Step 3]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

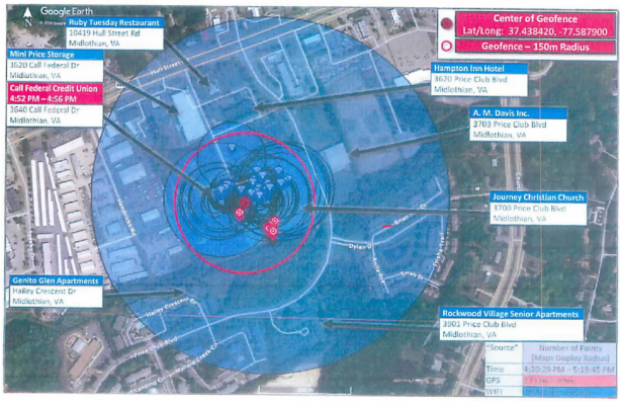
information ... on [three] device numbers." (ECF No. 96-2, at ¶ 19.) Google provided him with this information—"the account subscriber information associated with the 3 device numbers"—on July 11. (ECF No. 96-2, at ¶ 20.) Again, it is not apparent from the record whether Det. Hylton demonstrated to Google why he requested Step 3 data for these three accounts, nor did he seek the magistrate's approval before obtaining the data.

Finally, "[o]n or about July 12, 2019," Det. Hylton emailed Google "requesting *additional* device or phone number information that could be associated with one of the accounts" for which Google had produced Step 3 data. (ECF No. 96-2, at ¶ 21 (emphasis added).) This would have been an unauthorized Step 4. A Legal Investigations ***922** Specialist called Det. Hylton, that day and told him that "no further information was produced under" the Geofence Warrant. (ECF No. 96-2, at ¶ 21.)

6. Data Derived from the Warrant

a. Law Enforcement's Demonstrative

Upon receipt of the geofence data, law enforcement "imported [the Step 1 information] into mapping software" so that law enforcement could visualize the data points. (Mar. 4–5 Hr'g Gov. Ex. 1, at 15.) That program rendered the following depiction:



The visualization, created by Agent D'Errico, plots each point's confidence interval—the area in which Google is 68 percent confident a given individual is located—with a blue shaded circle.

Here, the largest confidence interval for a user located within the geofence had a radius of roughly 387 meters (longer than four football fields)—more than twice as large as the original geofence.[29] Thus, the Geofence Warrant *could* have captured the location of someone who was hundreds of feet outside the geofence. Within this confidence interval—in addition to the Bank and the Church—are several buildings (with an unknown number of floors), including ***923** a Ruby Tuesday restaurant, a Hampton Inn Hotel, several units of the Genito Glen apartment complex, a self-storage business, a senior living facility, two busy streets (Hull Street and Price Club Boulevard), and what appear to be several residences near the southeast edge of the confidence interval. Near the time of the robbery, the individual whose account produced this large confidence interval could have been present at any of these locations instead of within the geofence.

Indeed, given that Google returns locations via these estimated location points, both McInvaille and D'Errico confirmed geofences can return both false positives (someone who is not in the geofence reported as being there) and false negatives (someone in the geofence not reported). Chatrie created a video based on the returns of this geofence warrant suggesting that a false positive was returned here.

b. The Three Paths Video

Chatrie's video depicting the movement of three phones was based on the data obtained through the Warrant at Step 2. At the March 4–5 Suppression Hearing, Chatrie introduced a video that plotted the locations of three anonymous individuals whose location data Google turned over at Step 2—"Mr. Blue," "Mr. Green," and "Ms. Yellow." (ECF No. 201, at 63, 67; *see* Mar. 4–5 Hr'g Def. Ex. 5 ("Three Paths Video").)

At the beginning of the two-hour, geographically unlimited, window for which the Government requested Step 2 location data, a cluster of location points for Mr. Blue appeared at a nearby apartment complex. At 4:34 p.m., Mr. Blue seemed to leave the apartment complex, and at 4:35 p.m., Mr. Blue's location estimate appeared inside the geofence, roughly seventeen minutes before the robbery occurred. However, at 4:36 p.m.—twenty-seven seconds later—Mr. Blue appeared outside the geofence on Price Club Boulevard, and by 4:37 p.m., Mr. Blue appeared to be driving down Hull Street. Mr. Blue then drove south and stopped at another residence—clustering location data for five minutes—and eventually drove back toward the original apartment complex, where he remained for the rest of the two-hour window. Because Mr.

Blue appeared within the geofence for such a brief period of time—and because he appeared within the fence just as he appeared to drive on a nearby street—Defense Expert Mclnvaille testified that Mr. Blue may have been a "false positive"—he may not have actually stepped foot within the geofence. (ECF No. 201, at 43–44, 65.)

Mr. Green's location points initially clustered at a hospital for a period of about thirty-five minutes. Eventually, Mr. Green drove south along Old Courthouse Road, ultimately appearing inside the geofence at 4:41 p.m. Around two minutes later—and nine minutes before the robbery—Mr. Green's estimated location appeared in a residential neighborhood, clustering around one home for the remainder of the two-hour window.

Finally, Ms. Yellow clustered location points at a house from 3:51 p.m. to 4:11 p.m. At 4:18 p.m., she clustered several points near a school, and by 4:26 p.m., she appeared to drive toward the Bank. At 4:31 p.m., she first appeared in the geofence, her location estimate surfacing inside the Bank. She reported two more location points inside the Bank, and by 4:36—eighteen minutes before the robbery—appeared to be driving away from the Bank. She drove south, arrived at the house from which she started, and remained there for the rest of the two-hour window.

Defense Expert McInvaille testified that he was able to access publicly available ***924** information such as tax records related to the homes in which Mr. Blue, Mr. Green, and Ms. Yellow appeared to spend significant time. He explained that these records, in conjunction with other publicly available information such as social media accounts, would have allowed him to determine these individuals' likely identities with only a few data points. Law enforcement would, of course, have similar or enhanced research capabilities to identify users based on these "de-identified" location points.

* * *

Ultimately, the Step 3 information law enforcement obtained led the authorities to Chatrie.

B. Procedural History

On September 17, 2019, a grand jury indicted Chatrie on two counts: (1) Forced Accompaniment During Armed Credit Union Robbery, in violation of 18 U.S.C. §§ 2113(a), (d), and (e); and, (2) Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A). The police issued a warrant, and a magistrate judge signed a Petition and Order for Writ of Habeas Corpus ad Prosequendum ordering that Chatrie, then an inmate at Riverside Regional Jail, appear in the United States District Court for the Eastern District of Virginia to answer for the charges.

On October 1, 2019, Chatrie appeared before the magistrate judge and waived his right to a detention hearing. The magistrate judge ordered Chatrie detained pending trial. On that same day, Chatrie appeared for an arraignment and pleaded not guilty to the charged offenses.

On October 29, 2019, Chatrie filed the instant Geofence Motion to Suppress. (ECF No. 29.) The United States responded, (ECF No. 41), and Chatrie replied, (ECF No. 48). On December 23, 2019, the Court granted Google leave to file an amicus brief. (ECF No. 73.) In response to Chatrie's Federal Rule of Civil Procedure 17(c) subpoenas, Google also filed a total of four declarations by two Google employees: three by Marlo McGriff, and (2) one by Sarah Rodriguez. (ECF Nos. 96-1, 96-2, 110-1, [30] 147.)

On November 9, 2020, around one week before the scheduled Suppression Hearing, Google filed a Motion for Leave to Present Remote Testimony. On November 11, 2020, Chatrie responded in opposition. In this response, Chatrie argued that "[i]n person testimony from the Google employees [was] critical to the Court's resolution of Mr. Chatrie's geofence warrant," and that "Google's continued intrusion into this case warrants a finding from this Court that the Google witnesses are hostile/adverse witnesses." (ECF No. 166, at 1, 6.) After the Court held a status conference on the Motion for Leave to Present Remote Testimony, Chatrie filed a Motion to Continue the November 17, 2020 hearing, seeking to continue the hearing to a time when Google would be able to attend in person. On December 18, 2020, the Court granted Chatrie's Motion to Continue and scheduled the Suppression Hearing for March 4, 2021.

***925** Considering the novel and complex questions of law at issue, the Court allowed the parties to provide supplemental briefing on discovery provided by Google and the March 4-5, 2021 Suppression Hearing. Among others, witnesses from Google—McGriff and Rodriguez—provided the Court with a relatively exhaustive picture of Google's typical response to geofence warrants. Now, after careful consideration of the issues and with the aid of the parties' thorough briefing, the Court concludes that, although this warrant is invalid

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

for lack of particularized probable cause, the Court cannot suppress the resulting evidence because the *Leon* good faith exception applies.

III. Analysis

Chatrie seeks to suppress evidence obtained from the June 14, 2019 Geofence Warrant that covered 70,686 square meters of land around the Bank, located in a busy part of the Richmond metro area. Despite the Court's concerns about the validity of this warrant and the adoption of unsupervised geofence warrants more broadly, the Court will deny Chatrie's Motion to Suppress because the officers sought the warrant in good faith.

A. The Court Will Briefly Address Fourth Amendment Standing

Because the Court will independently deny Chatrie's motion to suppress by considering the validity of the Geofence Warrant, the Court "need not wade into the murky waters of standing," *i.e.*, whether Chatrie has a reasonable expectation of privacy in the data sought by the warrant. *United States v. James*, No. 18cr216, 2018 WL 6566000, at *4 (D. Minn. Nov. 26, 2018); *see* *Byrd v. United States*, —— U.S. ——, 138 S. Ct. 1518, 1530, 200 L.Ed.2d 805 (2018) (Fourth Amendment standing "is not a jurisdictional question and hence need not be addressed before addressing other aspects of the merits of a Fourth Amendment claim.").

Nonetheless, the Court notes its deep concern (underlying both Fourth Amendment standing, and the third-party doctrine discussed below) that current Fourth Amendment doctrine may be materially lagging behind technological innovations. As Fourth Amendment law develops in a slow drip, "technology [continues to] enhance[ ] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes." *Carpenter v. United States*, —— U.S. ——, 138 S. Ct. 2206, 2214, 201 L.Ed.2d 507 (2018). Relevant here, although *law enforcement* limited the warrant's window to two hours, Google—despite efforts to constrain law enforcement access to its data—retains constant, near-exact location information for each user who opts in. *See* Part II.A.3.a, *supra.* The Government thus has an almost unlimited pool from which to seek location data, and ' "[w]hoever the suspect turns out to be,' they have 'effectively been tailed' " since they enabled Location History. *Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (en banc) (quoting *Carpenter*, 138 S. Ct. at 2218).

Indeed, the " 'retrospective quality of [geofence] data' enables police to 'retrace a person's whereabouts,' " and "[p]olice need not even know in advance whether they want to follow a particular individual, or when." *Id.* at 342 (quoting *Carpenter*, 138 S. Ct. at 2218). Until recently, the ease with which law enforcement might access such precise and essentially real-time location data was unimaginable. And it is this expansive, detailed, and retrospective nature of Google location data that is unlike, for example, surveillance footage, and that perhaps causes such data to "cross[ ] the line from merely augmenting [law enforcement's ***926** investigative capabilities] to impermissibly enhancing" them. *Id.* at 341.

What is more, the Court is disturbed that individuals other than criminal defendants caught within expansive geofences may have no functional way to assert their own privacy rights. Consider, for example, a geofence encompassing a bank, a church, a nearby residence, and a hotel. Ordinarily, a criminal perpetrator would not have a reasonable expectation of privacy in his or her activities within or outside the publicly accessible bank. *See* *United States v. Knotts*, 460 U.S. 276, 281, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). He or she thus may not be able to establish Fourth Amendment standing to challenge a time-limited acquisition of his location data at the bank.

But the individual in his or her residence likely *would* have a heightened expectation of privacy. *Silverman v. United States*, 365 U.S. 505, 511, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961) ("At the very core [of the Fourth Amendment] stands the right of a [person] to retreat into his [or her] own home and there be free form unreasonable government intrusion."). Yet because that individual would not have been alerted that law enforcement obtained his or her private location information, and because the criminal defendant could not assert that individual's privacy rights in his or her criminal case, *United States v. Rumley*, 588 F.3d 202, 206 n.2 (4th Cir. 2009), that innocent individual would seemingly have

no realistic method to assert his or her own privacy rights tangled within the warrant. Geofence warrants thus present the marked potential to implicate a "right without a remedy." *Hawkins v. Barney's Lessee*, 30 U.S. 457, 463, 5 Pet. 457, 8 L.Ed. 190 (1831) ("There can be no right without a remedy to secure it.").

As this Court sees it, analysis of geofences does not fit neatly within the Supreme Court's existing "reasonable expectation of privacy" doctrine as it relates to technology. That run of cases primarily deals with *deep*, but perhaps not *wide*, intrusions into privacy. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (considering the validity of using thermal imaging on one's home); *United States v. Jones*, 565 U.S. 400, 402-03, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (construing "the attachment of a [GPS] tracking device to an individual's vehicle" for twenty-eight days); *Carpenter*, 138 S. Ct. at 2217 n.3 (considering whether "accessing seven days of [an individual's cell site location information] constitutes a Fourth Amendment search").

At base, these matters are best left to legislatures. *See* Zach Whittaker, *A Bill to Ban Geofence and Keyword Search Warrants in New York Gains Traction*, TechCrunch (Jan. 13, 2022), https://tcm.ch/35mLHkP (discussing a recently introduced New York bill that would ban the use of geofence warrants statewide). This case has arisen because no extant legislation prevents Google or its competitors from collecting and using this vast amount of data. And, as discussed below, despite its ongoing efforts to improve, Google appears to do so under the guise of consent few people understand how to disable. Even with consent, it seems clear that most Google users do not know how the consent flow to control their collection of data works, nor do they know Google is logging their location 240 times a day. It is not within this Court's purview to decide such issues, but it urges legislative action. Thoughtful legislation could not only protect the privacy of citizens, but also could relieve companies of the burden to police ***927** law enforcement requests for the data they lawfully have.

B. Because the Government Lacked Particularized Probable Cause as to Every Google User in the Geofence, the Warrant Violates the Fourth Amendment

At base, this particular Geofence Warrant is invalid. The Fourth Circuit has clearly articulated that warrants, like this one, that authorize the search of every person within a particular area must establish probable cause to search every one of those persons. Here, however, the warrant lacked any semblance of such particularized probable cause to search each of its nineteen targets, and the magistrate thus lacked a substantial basis to conclude that the requisite probable cause existed. And to the extent the Government would argue that Steps 2 and 3 cure the warrant's defects as to probable cause, such an argument is unavailing here. The Government itself contends that law enforcement demonstrated probable cause to obtain *all* the data sought without any narrowing measures (*i.e.*, de-anonymized and geographically unlimited data from everyone within the geofence). In any event, Steps 2 and 3—undertaken with no judicial review whatsoever—improperly provided law enforcement and Google with unbridled discretion to decide which accounts will be subject to further intrusions. These steps therefore cannot buttress the rest of the warrant, as they fail independently under the Fourth Amendment's particularity prong.

1. Legal Standard: The Warrant Requirement

[3] **[4]** The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Stated another way, the Fourth Amendment requires that a warrant (1) be supported by probable cause; (2) particularly describe the place to be searched and the things to be seized; and, (3) be issued by a neutral, disinterested magistrate.[31] *Dalia v. United States*, 441 U.S. 238, 255, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979) (internal quotations and citations omitted). If a warrant is invalid, the proper remedy in a criminal action is "ordinarily" to suppress the evidence derived from it. *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018).

a. Probable Cause

[5] **[6]** **[7]** **[8]** **[9]** **[10]** Whether probable cause for a search exists is a "practical, common-sense" question, asking whether "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 103 S.Ct. 2317,

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

76 L.Ed.2d 527 (1983). It requires only "the kind of fair probability on which reasonable and prudent people, not legal technicians," would rely. *United States v. Jones*, 952 F.3d 153, 158 (4th Cir. 2020) (citing *Florida v. Harris*, 568 U.S. 237, 244, 133 S.Ct. 1050, 185 L.Ed.2d 61 (2013)). Officers must present sufficient information to the magistrate judge[32] to allow him or her to exercise independent judgment. *Gates*, 462 U.S. at 239, 103 S.Ct. 2317. The magistrate cannot simply ratify the bare conclusions of others. *Id.* "When reviewing the probable cause supporting a warrant, a reviewing ***928** court must consider only the information presented to the magistrate who issued the warrant." *United States v. Wilhelm*, 80 F.3d 116, 118 (4th Cir. 1996) (citations omitted). "[T]he duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2004).

[11] **[12]** More specifically, a warrant must be "no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) (quoting *United States v. Zimmerman*, 277 F.3d 426, 432 (3d Cir. 2002)). Indeed, the United States Court of Appeals for the Fourth Circuit has established that warrants that authorize the search of "all persons on [a] premise[s]" must show probable cause "to believe that *all* persons on the premises at the time of the search are involved in the criminal activity." *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004) (emphasis added) (second alteration in original), *overturned on other grounds by* *Pearson v. Callahan*, 555 U.S. 223, 129 S. Ct. 808, 172 L.Ed.2d 565 (2009). In other words, these warrants must demonstrate "good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant in the criminal activity." *Owens*, 372 F.3d at 276 (internal quotation marks omitted).

[13] **[14]** At base, probable cause demands that law enforcement possess "a reasonable ground for belief of guilt ... *particularized* with respect to the person to be searched or seized." *Maryland v. Pringle*, 540 U.S. 366, 124 S. Ct. 795, 800, 157 L.Ed.2d 769 (2003) (emphasis added); *see* *Ybarra v. Illinois*, 444 U.S. 85, 91, 100 S.Ct. 338, 62 L.Ed.2d 238 (1979) ("Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person.") A "person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338.

b. Particularity

[15] **[16]** **[17]** A warrant must also be sufficiently "particular[ ]." *Hurwitz*, 459 F.3d at 470. Thus, a warrant must "confine the executing [officers'] discretion by allowing them to seize only evidence of a particular crime." *United States v. Cobb*, 970 F.3d 319, 328 (4th Cir. 2020), as amended (Aug. 17, 2020) (quoting *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986)). The warrant must therefore "identif[y] the items to be seized by their relation to designated crimes," and the "description of the items [must] leave[ ] nothing to the discretion of the officer executing the warrant." *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (citation omitted). "So long as the warrant describes the items to be seized with enough specificity that the executing officer is able to distinguish between those items which are to be seized and those that are not ... the particularity standard is met." *United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020) (internal citations and quotations omitted).[33]

*929 2. The Geofence Warrant Fails to Establish Particularized Probable Cause to Search Every Google User Within the Geofence

[18] Although cloaked by the complexities of novel technology, when stripped of those complexities, this *particular* Geofence Warrant lacks sufficient probable cause.[34] The United States Supreme Court has explained that warrants must establish probable cause that is "particularized with respect to the person to be searched or seized." *Pringle*, 124 S. Ct. at 800. This warrant did no such thing. It first sought location information for *all* Google account owners who entered the geofence over the span of an hour.[35] For those Google accounts, the warrant further sought "contextual data points with points of travel outside of the" Geofence for yet another hour—and those data points retained *no* geographical restriction. (ECF No. 54-1, at 4.)

Astoundingly, the Government claims that law enforcement established probable cause to obtain *all* information (Steps 1, 2, and 3) from *all* users within the geofence without any narrowing measures.[36] Yet the warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals.

Law enforcement attempted to justify the warrant by claiming that such a sweeping search "may [have] tend[ed] to identify potential witnesses and/or suspects." (ECF No. 54-1, at 7.) Even if this Court were to assume that a warrant would be justified on the grounds that a search would yield *witnesses* (some of whom had already been interviewed) instead of perpetrators, the Geofence Warrant is completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime. *Cf.* *Owens*, 372 F.3d at 276. To be sure, a fair probability may have existed that the Geofence Warrant would generate the *suspect's* location information.[37] ***930** However, the warrant, on its face, also swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny.

Indeed, it is difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing. Law enforcement knew only that the perpetrator "had a cell phone in his right hand and appeared to be speaking with someone on the device." (ECF No. 54-1, at 6.) After the police failed to located the suspect via reviewing camera footage, speaking with witnesses, and pursuing two leads, law enforcement simply drew a circle with a 150-meter radius that encompassed the Bank, the entirety of the Church, and the Church's parking lot.[38] The Government then requested location information for *every device* within that area. *See* *Carpenter*, 138 S. Ct. 2206, 2216 (2018) (describing cell phone location information as "encyclopedic").

What is more, in one instance, this Geofence Warrant captured location data for a user who may not have been *remotely* close enough to the Bank to participate in or witness the robbery. Because the radius of one of the users' confidence intervals stretched to around 387 meters, the Geofence Warrant might have reported that user's location data to the Government, notwithstanding the fact that he may have simply been present in any number of nearby locations. For example, that person may have been dining inside the Ruby Tuesday restaurant nearby. The person may have been staying at the Hampton Inn Hotel, just north of the Bank. Or, he or she could have been inside his or her own home in the Genito Glen apartment complex or the nearby senior living facility. He or she may have been moving furniture into the nearby self-storage business. Indeed, the person may have been simply driving along Hull Street or Price Club Boulevard. Yet the Government obtained the person's location data just the same. The Government claims that footage depicting the perpetrator holding a phone to his ear—and nothing else—justified this sweeping warrant. That, however, is simply not "[ ]reasonable." U.S. Const. amend. IV.

To further underscore the breadth of this search, Chatrie's expert Spencer McInvaille pointed out a likely "false positive" from the warrant—"Mr. Blue." Mclnvaille testified that this "false positive" individual may not have ever stepped within the geofence—he may have simply driven "outside of the original geofence" on a nearby road, but could have nonetheless appeared "as if [he] were inside the geofence." (ECF No. 201, at 43–44, 65.) Because Google's location estimate for that person could have been "incorrect," Google may have *thought* the person had stepped foot in the target area. (ECF No. 201, at 43–44.) The Government therefore obtained ***931** two hours of unrestricted location data for an individual who perhaps had only driven within the outer vicinity of the crime scene.[39]

[19] This Geofence Warrant therefore suffers from the same probable cause defect as that at issue in *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020). In that case, the Government sought "to erect three geofences." *Id.* 732. Two encompassed the same location during different timeframes, and the other captured a second location. *Id.* Each geofence lasted for forty-five minutes. *Id.* The court remarked that "the proposed warrant would admittedly capture the device IDs ... for all who entered the geofences, which surround locations as to which there is no reason to believe that anyone – other than the Unknown Subject – entering those locations is involved in the subject offense or in any other crime." *Id.* at 752. There, just as here, the warrant provided the Government "unlimited discretion to obtain from Google the device IDs ... of anyone whose Google-connected devices traversed the geofences (including their vaguely defined margins of error), based on nothing more than the 'propinquity' of these persons to the Unknown

Subject at or near the time" of the criminal activity. *Id.* at 753. As that court (and the Supreme Court in *Ybarra*) recognized—and as this Court now concludes—the Fourth Amendment's probable cause requirement demands more than "mere propinquity" to a crime. *Id.* at 752; *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338.

Despite the Government's reliance on *United States v. McLamb*, that case is inapposite. There, the Fourth Circuit upheld a warrant that allowed law enforcement to obtain identifying information of "any user entering a username and password into" an internet-based dark website where users could download or upload child pornography. *United States v. McLamb*, 880 F.3d 685, 689 (4th Cir. 2018). But there, a user's "mere propinquity" to the website *did* necessarily establish probable cause: any user visiting the site likely participated in the criminal conduct of viewing or sharing child pornography. *Id.* Here, on the other hand, a Google user's proximity to the bank robbery does not necessarily suggest that the user participated in the crime. *McLamb* therefore does not inform this case. [40]

***932** Nor does the Government's reliance on *United States v. James* persuade. The *James* court considered a warrant to collect cell tower information (so-called "tower dumps") to determine whether "a particular cellular phone number (ostensibly held by the robber) could be identified during the timeframes of each of the respective robberies." 2018 WL 6566000, at * 1. Law enforcement sought the cell tower data based on the notion that a cell phone number present at the location and time of all six robberies created sufficient probable cause that the number belonged to the robber. *Id.* Ultimately, the court concluded that "there was a fair probability that data from the cellular towers" would contain identifying information about the perpetrator and that therefore the warrants sufficed to allege probable cause. *Id.* at *4. As another court has noted however, *James* did not account for whether probable cause existed to search through the *other* individuals' location information. *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 751; *see also* *id.* at 752 (distinguishing another tower dump decision from the geofence context because the court discussing the tower dump "stopped the analysis once the court found probable cause in the 'nexus' between the offense and *all* the requested cell phone records, without analyzing whether probable cause existed to obtain all of those records." (quoting *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769 (S.D. Tex. 2013)). *James* therefore stopped short of considering whether "particularized" probable cause existed, and it is precisely that lack of narrowly-tailored probable cause that is fatal to this Geofence Warrant. [41]

The Court cautions that it declines to consider today whether a geofence warrant may *ever* satisfy the Fourth Amendment's strictures. *See* *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 361–62 (N.D. Ill. 2020) ("[I]t is nearly impossible to pinpoint a search where only the perpetrator's privacy interests are implicated."). Consider, for example, one of the few other federal court opinions to address a geofence warrant—*In re Search of Information That Is Stored at the Premises Controlled by Google LLC*, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021) [hereinafter "DDC Opinion"]. There, law enforcement devised a two-step process to narrow the list of individuals whose data they would obtain. *Id.* at *5–6. At Step 1, Google would identify all accounts who entered the geofence within the relevant time periods. *Id.* For each of ***933** these accounts, Google would turn over only anonymized data. *Id.*

The Government would then review that data, identify likely suspects based on the "mov[ement]" of the users' devices through the geofence, and, crucially, identify to the *court* the devices the Government believed belonged to the perpetrator. *Id.* The *court* could then, at its discretion, order Google to disclose to the Government personally identifying information for devices that belonged to likely suspects. *Id.* In essence, to obtain a warrant authorizing disclosure of de-anonymized data, the Government was required to demonstrate that location data for a *particular* user or set of users would provide evidence of the crime. And crucially, the warrant left ultimate discretion as to which users' information to disclose to the reviewing court, not to Google or law enforcement.

In certain situations, then, law enforcement likely *could* develop initial probable cause to acquire from Google *only* anonymous data from devices within a narrowly

circumscribed geofence at Step 1. *See* *Hurwitz*, 459 F.3d at 473 (a warrant must be "no broader than the probable cause on which it is based"). From there, officers likely could use that narrow, anonymous information to develop probable cause particularized to specific users. Importantly, officers likely could then present that particularized information to a magistrate or magistrate judge to acquire successively broader and more invasive information. Although the *instant* warrant is invalid, where law enforcement establishes such narrow, particularized probable cause through a series of steps with a court's authorization in between, a geofence warrant may be constitutional. [42]

[20] At bottom however, particularized probable cause "cannot be undercut or avoided by simply pointing to the fact that coincidentally there exists probable cause to search or seize another or to search the premises where the person may happen to be." *Ybarra*, 444 U.S. at 91, 100 S.Ct. 338. The Court finds unpersuasive the United States' inverted probable cause argument—that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby. In essence, the Government's argument rests on precisely the same "mere propinquity to others" rationale the Supreme Court has already rejected as an appropriate basis for a warrant. *Id.* This warrant therefore cannot stand.

3. This Geofence Warrant's Three-Step Process Does Not Cure Its Defects

[21] **[22]** To the extent the Government would attempt to argue in the alternative ***934** that this warrant's three-step process cures any defects with the warrant's particularized probable cause, such an argument is unavailing. [43] Even if this narrowing process cured any of the warrant's shortcomings as to particularized probable cause, this process cannot independently buttress the warrant for an entirely separate reason: clear lack of particularity. Warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In other words, "[a] warrant that meets the particularity requirement leaves the executing officer with no discretion as what to seize." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 754 (N.D. Ill. 2020) (citing *Stanford v. Texas*, 379 U.S. 476, 485, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965)). But Steps 2 and 3 of this warrant leave the executing officer with *unbridled* discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users.

This warrant, for instance, contains no language objectively identifying *which* accounts for which officers would obtain further identifying information. Nor does the warrant provide objective guardrails by which officers could *determine* which accounts would be subject to further scrutiny. Nor does the warrant even simply limit the *number* of devices for which agents could obtain identifying information. Instead, the warrant provided law enforcement unchecked discretion to seize more intrusive and personal data with each round of requests—without ever needing to return to a neutral and detached magistrate for approval.

The facts here underscore the breadth of discretion law enforcement possessed under this warrant. [44] After receiving anonymized information on the nineteen targeted users at Step 1, Det. Hylton requested the additional location information (Step 2) and subscriber information (Step 3) "for all 19 device numbers produced in [S]tep 1." (ECF No. 96-2, at ¶ 15.) In response, a Google specialist "called Detective Hylton and explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant." [45] (ECF No. 96-2, at ¶ 16.) During that call, "[t]he LIS specialist also explained the importance of [S]tep 2 in narrowing." (ECF No. 96-2, at ¶ 16.) Det. Hylton eventually narrowed his requests. Yet he did not specify to Google why he was choosing these particular users.

[23] *Google's* insistence on narrowing the list does not render this warrant sufficiently particular. For one thing, this warrant's clear text does not specifically allow Google to limit the group of accounts that would be subject to further scrutiny. (*See* ECF No. 54-1, at 4–5 (noting only that ***935** Google "shall produce" further information).) But even if it did, Fourth Amendment discretion must be confined to the signing magistrate, not the executing officers or a third party. *United States v. Chadwick*, 433 U.S. 1, 9, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977) ("The judicial warrant has a significant role to play in that it provides the detached scrutiny of a neutral magistrate ...."), *abrogated on other grounds by* *California v. Acevedo*, 500 U.S. 565, 111 S.Ct. 1982, 114

L.Ed.2d 619 (1991). Stated plainly, Steps 2 and 3 "put[ ] no limit on the [G]overnment's discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences." *In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 754. These Steps accordingly fail to provide the executing officer with clear standards from which he or she could "reasonably ... ascertain and identify ... the place to be searched [or] the items to be seized." *Blakeney*, 949 F.3d at 861. The Government therefore cannot rely on Steps 2 and 3 to supply this warrant with particularized probable cause, as these steps independently fail under the Fourth Amendment's particularity requirement.

> it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [because] [t]his approach is ill suited to the digital age.... I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.

4. The Third-Party Doctrine

[24] Lastly, the Court simply cannot determine whether Chatrie "voluntarily" agreed to disclose his Location History data based on this murky, indeterminate record. But the Court expresses its skepticism about the application of the third-party doctrine to geofence technology. Under this doctrine, "a person [generally] has no legitimate expectation of privacy in information he [or she] voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). However, in *Carpenter v. United States*, the Supreme Court refined this principle and held than an individual *does* possess an expectation of privacy in seven days of cell-site location information collected by a wireless carrier. 138 S. Ct. at 2217 & n.3. Here, the Government argues that Chatrie cannot claim a reasonable expectation of privacy in his Location History data because (1) he "voluntarily disclosed" the information to Google; and, (2) the two hours of location data sought here do not implicate the same privacy concerns as the seven days obtained in *Carpenter*. (ECF No. 41, at 11; *see* ECF No. 41, at 9–13.)

The Court thinks otherwise. Common sense underscores Supreme Court Justice Sonia Sotomayor's observation in *United States v. Jones* about "voluntary" collection of electronic information unbeknownst to the subject of the warrant. As to the third-party doctrine, Justice Sotomayor observed that:

Jones, 565 U.S. at 417–18, 132 S.Ct. 945 (Sotomayor, J., concurring). At base, the topic is complex. And considering the messiness of the current record as to how and when Chatrie "gave consent," the Court cannot—and need not—reach a firm decision on the issue. But the Court remains unconvinced that the third-party doctrine would render hollow Chatrie's expectation of privacy in his data, even for "just" two hours. Google Location History information—perhaps even more so than ***936** the cell-site location information at issue in *Carpenter*—is "detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct. at 2216; *see id.* at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."). Although, unlike in *Carpenter*, Chatrie apparently took some affirmative steps to enable location history, those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day.

This is especially so given the limited and partially hidden warnings provided by Google. In the Google Assistant set-up process, the device likely provided Chatrie a single pop-up screen informing him that "[t]his data may be saved and used in any Google service where [he was] signed in to give [him] more personalized experiences," and that he "can see [his] data, delete it and change [his] settings at account.google.com." (ECF No. 147, at ¶ 7; *see* ECF No. 96-1, at ¶ 7; ECF No. 201, at 102; ECF No. 202, at 21.) However, the consent flow did not detail, for example, how

frequently Google would record Chatrie's location (every two to six minutes); the amount of data Location History collects (essentially *all* location information); that even if he "stopped" location tracking it was only "paused," meaning Google retained in its Sensorvault all his past movements; or, how precise Location History can be (*i.e.*, down to twenty or so meters).[46] (ECF No. 201, at 122, 136; ECF No. 202, at 71.)

While the Court recognizes that Google puts forth a consistent effort to ensure its users are informed about its use of their data, a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting "YES, I'M IN" at midnight while setting up Google Assistant, even if some text offered warning along the way. The record here makes plain that these "descriptive texts" are less than pellucid. Although the Court cannot reach a final decision on the issue today based on the current record here, Chatrie likely could not have, in a "meaningful sense, ... voluntarily 'assumed the risk' of turning over a comprehensive dossier of his physical movements" to law enforcement. *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745, 99 S.Ct. 2577); *see* *id.* at 2217 ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere.").

C. Because Det. Hylton Consulted with Government Attorneys in the Face of Novel Technology and Obtained Similar Warrants in the Past, and Because the Warrant Was Not Otherwise "So Facially Deficient," the Good-Faith Exception Applies

Despite the warrant's defects, the Court ultimately cannot find that excluding the instant evidence would serve to deter future improper law enforcement conduct. This is particularly so in light of rapidly advancing technology and lack of judicial guidance on this novel investigatory technique, and where, as here, prosecutors and magistrates approved three similar warrants.

*937 1. Legal Standard

[25] **[26]** The exclusionary rule "is neither 'a personal constitutional right' nor is it 'designed to redress the injury occasioned by an unconstitutional search.' " *United States v. Manafort*, 323 F. Supp. 3d 795, 805 (E.D. Va. 2018) (quoting *Davis v. United States*, 564 U.S. 229, 236, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011)). Rather, the exclusionary rule "is a prudential doctrine created ... to compel respect for" constitutional rights. *Davis*, 564 U.S. at 236–37, 131 S.Ct. 2419 (2011). "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *McLamb*, 880 F.3d at 690 (internal quotation marks and citation omitted). Where suppression would not produce deterrent benefits, the exclusionary rule does not apply. *United States v. Leon*, 468 U.S. 897, 909, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).

[27] **[28]** For that reason, evidence obtained pursuant to a search warrant issued by a neutral magistrate need not be excluded if the officer's reliance on the warrant was "objectively reasonable." *Id.* at 922–23, 104 S.Ct. 3405. Generally, the fact that a neutral magistrate has issued a warrant "suffices to establish" that a law enforcement officer has "acted in good faith in conducting the search." *Id.* at 922, 104 S.Ct. 3405. Therefore, searches carried out pursuant to a warrant "rarely require any deep inquiry into reasonableness." *Id.*

[29] **[30]** The Fourth Circuit has nonetheless set out four categories of cases in which the good-faith exception will not apply:

> (1) if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) if the issuing magistrate wholly abandoned his [or her] judicial role[;] ... (3) if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the warrant is so facially deficient —*i.e.*, in failing to particularize the place to be searched or the things to be seized-that the executing officers

> cannot reasonably presume it to be valid.

United States v. Doyle, 650 F.3d 460, 467 (4th Cir. 2011) (internal quotation marks and citations omitted). When considering a motion to suppress the fruits of a novel investigative technique, courts generally decline to hold a warrant "facially deficient where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant." *McLamb*, 880 F.3d at 691. Further, "consultation [with Government attorneys prior to seeking a warrant] is a relevant consideration in determining whether the warrant was facially deficient." *United States v. Matthews*, 12 F.4th 647, 657 (7th Cir. 2021).

2. Because Det. Hylton Relied on the Approval of Prior Warrants in the Face of Novel Technology, the Good-Faith Exception Applies

a. Det. Hylton

[31] Despite the warrant failing under Fourth Amendment scrutiny, the *Leon* good faith exception shields the resulting evidence from suppression. The warrant lacked particularized probable cause, but it was not *"so* lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Leon*, 468 U.S. at 923, 104 S.Ct. 3405 (emphasis added). This is particularly so because "the legality of [this] investigative technique [was] unclear," and Det. Hylton ***938** sought "advice from counsel before applying for the warrant." *McLamb*, 880 F.3d at 691. When Det. Hylton applied for the Geofence Warrant, no court had yet ruled on the legality of such a technique. And as this Court's preceding analysis demonstrates, the permissibility of geofence warrants is a complex topic, requiring a detailed, nuanced understanding and application of Fourth Amendment principles, which police officers are not and cannot be expected to possess. *See* Part III.B.2, *supra*. [47]

[32] In the face of this legal uncertainty, Det. Hylton relied on his past experience seeking geofence warrants—he had sought three before applying for this one. Magistrates and prosecutors had approved all three. *See Matthews*, 12 F.4th at 656 (noting the "general principle that attorney involvement supports a finding of good faith"). Det. Hylton testified that these prior warrants were "mostly similar" to the one at bar—all but one incorporated a roughly 150-meter radius, although a "few of them had more locations because of the more robberies to investigate." (ECF No. 202, at 328.) Even accounting for his miscues, in light of the complexities of this case, Det. Hylton's prior acquisition of three similar warrants, and his consultation with Government attorneys before obtaining those warrants, the Court cannot say that Det. Hylton's reliance on the instant warrant was objectively unreasonable. *See McLamb*, 880 F.3d at 691. While magistrate approval and consultation with the prosecution alone cannot and should not mechanically trigger the good-faith exception, exclusion here likely would not "meaningfully deter" improper law enforcement conduct. *Herring v. United States*, 555 U.S. 135, 144, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009). [48]

b. Magistrate Bishop

[33] Nor can this Court conclude that Magistrate Bishop wholly abandoned his role as a detached magistrate as Chatrie argues. *See Doyle*, 650 F.3d at 470. This exception to good faith primarily looks to whether the magistrate "overstep[ped] his [or her] judicial responsibilities and compromise[d] his judicial neutrality," *United States v. Gary*, 420 F. Supp. 2d 470, 486 (E.D. Va. 2006) (quoting *United States v. Servance*, 394 F.3d 222, 231 (4th Cir. 2005), *vacated on other grounds by Servance v. United States*, 544 U.S. 1047, 125 S.Ct. 2308, 161 L.Ed.2d 1086 (2005)), by, for example, actively participating in an investigation, *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 327, 99 S.Ct. 2319, 60 L.Ed.2d 920 (1979); retaining a pecuniary interest in issuing the warrant, *Connally v. Georgia*, 429 U.S. 245, 249–51, 97 S.Ct. 546, 50 L.Ed.2d 444 (1977) (per curiam); "rubber stamp[ing]" a warrant that contained a "bare bones" affidavit, *Wilhelm*, 80 F.3d at 121 (4th Cir. 1996); or, failing to make an independent assessment as to the validity of the warrant, *United States v. McKneely*, 810 F. Supp. 1537, 1547 (D. Utah 1993), *rev'd on other grounds by United States v. McKneely*, 6 F.3d 1447 (10th Cir. 1993).

Chatrie has, perhaps, shown that Magistrate Bishop *should have* considered the implications of the Warrant more carefully. But ultimately, he has "produced no evidence to show that the magistrate did not ***939** read the affidavit or that he read it so cursorily as to have wholly abandoned his neutral and detached role." *Gary*, 420 F. Supp. 2d at 487; (*see* ECF No. 202, at 361-62 (noting that the magistrate reviewed the warrant for around fifteen or thirty minutes).) Nor did he "suggest that the magistrate acted in a partisan manner or aligned himself with the police. Consequently, ... the second *[Leon* exception] does not bar application of the good-faith exception." *Gary*, 420 F. Supp. 2d at 487. Chatrie further argues that "[t]he magistrate's utter lack of concern regarding the obvious flaws in the warrant constituted a complete abandonment of his role as ... neutral arbiter." (ECF No. 205, at 41.) But the Fourth Circuit has instructed that such "an allegation that a search warrant application contained grossly insufficient information is best analyzed under the third *Leon* exception." *United States v. Wellman*, 663 F.3d 224, 229 (4th Cir. 2011). And for the reasons explained above, that exception does not warrant suppression either.

Finally, the Court must address Chatrie's challenge to Magistrate Bishop's qualifications. Chatrie contends that Magistrate Bishop did not possess the requisite statutory qualifications to make the instant probable cause determination. The Court first observes that, in Virginia, any United States citizen who is a resident of the Commonwealth is eligible to be appointed as a magistrate with certain limitations not relevant here. Va. Code § 19.2-37. To qualify today, a magistrate need only have "a bachelor's degree from an accredited institution of higher education." Va. Code § 19.2-37(B). And "[a] person initially appointed as a magistrate prior to July 1, 2008, who continues in office without a break in service is *not* required to have a bachelor's degree from an accredited institution of higher education." Va. Code § 19.2-37(B) (emphasis added). No law degree is required. Indeed, "[n]o person appointed as a magistrate on or after July 1, 2008, *may* engage in the practice of law." Va. Code § 19.2-37(F) (emphasis added).

Magistrate Bishop graduated from Pensacola Christian College with a Bachelor of Science Degree in Criminal Justice in May of 2016. He was appointed as a Virginia magistrate roughly two years later in June 2018, began certification school in July 2018, and was formally appointed and "released for independent service on October 24, 2018." (ECF No. 156, at ¶ 3.) His nine-month probationary period pursuant to Virginia Code § 19.2-38 ended on March 12, 2019. In other words, Magistrate Bishop had been serving as a non-probationary magistrate just *three months* before he signed this sweeping and powerfully intrusive Geofence Warrant on June 14. And he had graduated from college just three years earlier.

Chatrie does not rest on Magistrate Bishop's lack of a law degree. He instead avers that Magistrate Bishop's undergraduate degree was not sufficiently "accredited" under Virginia law. (ECF No. 135, at 6–9.) As noted, Pensacola Christian College does not appear to be officially licensed in Florida. (*See* Ex. B 24, ECF No. 135-2 ("Pensacola Christian College operates in the state of Florida as an independent institution of higher learning that is exempt from state commission oversight as per Florida statutes.").) Further, it does not appear to be accredited by a regional higher-education accrediting agency. *See, e.g.*, Southern Association of Colleges and Schools Commission on Colleges, *Accredited and Candidate List January 2022* (last visited Mar. 1, 2022), https://bit.ly/3cb3ICF. Yet the Transnational Association of Christian Colleges and Schools ***940** ("TRACS")[49] accredited the college in 2013. *Pensacola Christian College*, TRACS (last visited Mar. 1, 2022), https://bit.ly/3C22S5j.

Chatrie contends that the TRACS accreditation means little, as "[t]he most widely respected agencies are regional [accrediting] bodies," while "national accrediting agencies are significantly less prestigious." (ECF No. 135, at 7.) He points out that elsewhere, the Virginia Code and Virginia Administrative Code specify that certain professionals receive degrees accredited by specific agencies (typically distinguishing between regional and national entities), and that professionals with similar levels of expertise are typically required to obtain a degree from a regionally accredited school. *See*Va. Code § 54.1-4400; 18 Va. Admin. Code 115-40-22, 160-40-280. If the Court is to read anything into this, however, it is precisely the opposite conclusion from Chatrie's. The notion that Virginia lawmakers narrow the permissive group of accrediting agencies *elsewhere* merely signals that the lawmakers know how to limit the pool of accrediting bodies but chose not to do so here. *Cf Alexis v. Barr*, 960 F.3d 722, 735 n.1 (5th Cir. 2020) (Dennis, J., dissenting) (noting that where a statute defined a term more specifically in one place but not the other, lawmakers had "intentionally omitted" that more specific definition in

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

the other usage). Under Virginia Code § 19.2-37 then, Magistrate Bishop's degree likely suffices.

[34] To the extent Chatrie also attacks Magistrate Bishop's decision because he "would have had, at most, only a few months of experience evaluating warrant applications on his own when he signed the geofence warrant," that argument cannot prevail given Virginia's statutory scheme. (ECF No. 135, at 9.) Virginia magistrates must complete a training program, pass a certification examination, and serve a nine-month probationary period before hearing cases without supervision. Va. Code § 19.2-38. Magistrate Bishop had done this, and he had been certified by the Commonwealth of Virginia's Office of Executive Secretary. As a general principle, "[s]tates are entitled to some flexibility and leeway in their designation of magistrates, so long as all are neutral and detached and capable of the probable-cause determination required of them." *Shadwick v. City of Tampa*, 407 U.S. 345, 354, 92 S.Ct. 2119, 32 L.Ed.2d 783 (1972). In the ordinary course then, Virginia sufficiently trains its magistrates to determine probable cause.

Frankly, however, it is not clear to the Court that *any* person just three years out of college should be burdened with the responsibility of approving or rejecting a warrant of this complexity and magnitude. The Court certainly does not impute any bad faith or improper action by Magistrate Bishop (or the Commonwealth). This case has shown, however, the myriad ways that geofencing instigates a massive intrusion into individual rights, and it does so without notice to potentially thousands of persons with phones within it. It seems less than evident that all law enforcement officers have a clear understanding of the invasive scope of these warrants either. Nor do most magistrates, with or without a law degree. Ultimately, it is for the General Assembly to review or change its magistrate practice given this new technology, and one hopes they would.

In any event, even if Magistrate Bishop's degree or lack of experience did not ***941** qualify him to make this consequential finding, the good faith exception would still apply. The Fourth Circuit recently concluded in *McLamb* that the good faith exception is not categorically inapplicable even if the instant "warrant ... reache[s] beyond the boundaries of a magistrate judge's jurisdiction" where suppression would not "produce an appreciable deterrence on law enforcement." 880 F.3d at 691 (internal quotation marks omitted). The Court finds that suppression based on a technical defect of the magistrate's credentials would not serve to deter improper law enforcement conduct. In a typical investigation, officers simply cannot be required to consult a magistrate's resume before approaching that magistrate to obtain a warrant.

IV. Conclusion

Despite the Court finding good faith here, the Court nonetheless strongly cautions that this exception may not carry the day in the future. This Court will not simply rubber stamp geofence warrants. If the Government is to continue to employ these warrants, it must take care to establish particularized probable cause. As the legal landscape confronts newly developed technology and further illuminates Fourth Amendment rights in the face of geofence practices, future geofence warrants may require additional efforts to seek court approval in between Steps, or to limit the geographic and temporal information sought. But in light of the complex legal issues that lead to this Court's conclusion, the Court cannot say that Det. Hylton's reliance on the Geofence Warrant was objectively unreasonable. Accordingly, the *Leon* good faith exception applies, and the Court will deny Chatrie's motion to suppress evidence obtained as a result of the Geofence Warrant.

For the foregoing reasons, the Court will deny the Motion to Suppress. (ECF No. 29.) An appropriate Order shall issue.

All Citations

590 F.Supp.3d 901

Footnotes

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

1 A "presumption of validity" exists "with respect to the affidavit supporting the search warrant." *Franks v. Delaware*, 438 U.S. 154, 171, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978). Because Chatrie does not allege that the statements in the affidavits supporting the search warrants are untrue statements, but instead says that these statements do not provide enough information or that they do not contain the proper information to support the search warrants, the Court in part makes its findings of fact based on the statements made in the affidavits. *Id.* (describing the circumstances in which the Court must hold an evidentiary hearing on a defendant's motion to suppress).

2 The Court employs the pagination assigned by the CM/ECF docketing system for citations to the parties' submissions. Where a document was not filed through CM/ECF (for example, an exhibit introduced at a hearing), the Court will cite to the pages that would have been assigned through CM/ECF had they been filed through the system.

In addition, the Court acknowledges that its findings of fact differ between this Memorandum Opinion and a later issued Memorandum Opinion addressing the validity of four other warrants. In that Opinion, the warrants set forth a lengthier, more detailed narrative explaining the officers' investigatory steps than the instant Geofence Warrant. In determining the validity of a warrant, the "magistrate [or magistrate judge], and a reviewing court, will restrict their inquiries on probable cause to the facts set forth in the four corners of the officers' sworn affidavit." *United States v. Lipscomb*, 386 F. Supp. 3d 680, 684 (E.D. Va. 2019). Thus, because the facts in the Geofence Warrant differ from those set out in the four other warrants, the Court's findings of fact accordingly differ as well.

3 More precisely, (1) Forced Accompaniment During Armed Credit Union Robbery, in violation of 18 U.S.C. §§ 2113(a), (d), and (e); and, (2) Using, Carrying, or Brandishing a Firearm During and in Relation to a Crime of Violence, in violation of 18 U.S.C. § 924(c)(1)(A).

4 Specifically, this Court has identified only five other federal opinions on the subject, but all assessed the validity of the warrants *before* they were issued: *In re Search of Information That is Stored at the Premises Controlled by Google LLC*, No. 21sc3217, 2021 WL 6196136 (D.D.C. Dec. 30, 2021); *In re Search of Information that is Stored at the Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153 (D. Kan. 2021); *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730 (N.D. Ill. 2020); and, *In re Search of Information Stored at Premises Controlled by Google*, No. 20M297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).

5 Among other things, Google argued in its brief that Location History is not a business record, but is a journal stored primarily for the user's benefit and is controlled by the user. Google states that LH information "can often reveal a user's location and movements with a much higher degree of precision than [Cell Site Location Information]." (ECF No. 59-1, at 8.) Google argues that a geofence is certainly a " 'search' within the meaning of the Fourth Amendment," because "[u]sers have a reasonable expectation of privacy in the LH information, which the government can use to retrospectively reconstruct a person's movements in granular detail." (ECF No. 59-1, at 9.)

6 Legal Investigations Specialists are the Google employees who receive warrants and send the returns.

7 This testimony was delayed at the request of defense counsel during an extensive period of time because the COVID pandemic prevented live testimony.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

8 Other companies such as Amazon and Apple invariably retain users' location data as well. But Google, whose services function across Apple *and* Android devices (as opposed to Apple Maps for example, which functions only on iPhones), seems to be subject to more geofence requests than other companies.

9 Using 10K filings from Google's parent company Alphabet, FBI Agent D'Errico noted that Google's advertising revenue constituted 85.4% and 83.9% of its *entire* revenue in 2018 and 2019, respectively.

10 Defense Expert McInvaille evaluated a sample set of data and found that, for that data, Location History logged a device's location every six minutes. Under McInvaille's estimate, a user's movement is logged 240 times a day. D'Errico's estimate would raise that to 720 times a day. And Google Expert McGriff confirmed that Location History can track a user "hundreds" of times a day. (ECF No. 202, at 159.)

11 In a highly critical 2018 evaluation of tracking through Location History and Web & App Activity, the Norwegian Consumer Council (funded by the Norwegian government) characterized this as one of an identifiable set of problematic practices, dubbing it "repeated nudging" to encourage a user to enable the app. (Mar. 4–5 Hr'g Def. Ex. 27, at 28.)

12 This stands in contrast to Location History, which constantly and *passively* logs a user's location.

13 At the time of the robbery, Chatrie used an Android device.

14 McGriff complicated this seemingly straightforward proposition by acknowledging that any "device that has been sitting on a shelf for three years [would use start up language] dated to when it was baked into the device." (ECF No. 202, at 18.)

15 Although the testimony is unclear on the matter, prior to 2018, this line appears to have read: "[C]reates a private map of where you go with your signed in devices." (ECF No. 201, at 266.) Google changed this language in response to European regulation.

16 On May 11, 2018, two Senators launched an investigation into Google's acquisition of location data. During the March 4–5 Suppression Hearing, Chatrie tried to suggest that this investigation—in conjunction with a critical article from news website Quartz—*caused* Google to issue an update to its privacy policy on May 25, 2018. Google's expert McGriff testified credibly, however, that the investigation and policy changes were unrelated, because "there[was] no way Google updated its privacy policy in two weeks." (ECF No. 201, at 259.)

17 Since 2018, Google has added another feature to increase user control over Location History data. It now allows a user to set an "auto delete function" that limits how long Location History information remains with Google. (Mar. 4–5 Hr'g Def. Ex. 46, at 2.) The auto delete function now enables a user to "[c]hoose a time limit" for how long he or she wants Google to save activity data and "any data older than that will be automatically deleted from [the] account on an ongoing basis." (Mar. 4–5 Hr'g Def. Ex. 46, at 2.) McGriff testified that Google has also now developed a practice whereby Google sends monthly or annual emails about how to change settings. Google has no record that these emails were ever sent to Chatrie.

Still, concern about the user interface seemed to persist over time. Chatrie presented what purported to be emails from Google employees (garnered for other litigation) noting the confusing nature of various location products. One, in April 2019, reads: "Speaking as a user, WTF? More specifically I **thought** I had location tracking turned off on my phone. However the location toggle in the quick settings was on. So our messaging around this is enough to confuse a privacy focused Google-[software engineer]. That's not good." (Mar. 4–5 Hr'g Def. Ex. 37, at 5). The Norwegian report called this phenomenon "[d]eceptive click-flow." (Mar. 4–5 Hr'g Def. Ex. 27, at 27).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

18 To clarify, a geofence *request* is not identical to a geofence *warrant.* "[I]n some cases, law enforcement is[not] aware that [it] need[s] to submit a warrant" to obtain Location History. (ECF No. 202, at 173.) Google still considers this communication from law enforcement a "geofence request," even when not accompanied by a warrant. (ECF No. 202, at 173.)

19 When responding to geofence warrants, Google:

> de[-]identifies the data produced to the [G]overnment at this [first] step by removing the [user's distinct] Google Account ID ..., leaving only a device number that is used only in the Location History database. This device number is only used for distinguishing devices reporting [Location History] to a user's account ...

(ECF No. 96-2, at ¶ 9.) Unlike a Google Account ID, a Location History device number does not by itself identify which account is associated with certain location points. However, as discussed in Part II.A.6.b ("The Three Paths Video"), *infra*, piecing together an "anonymous" user's location data could reveal that user's identity.

20 At Step 2, for law enforcement to expand the timeframe from which to obtain Location History data, Google generally requires that the warrant explicitly expand that timeframe *in the warrant's text.* Otherwise, Google will object to that request.

21 If law enforcement requests this additional data, it must typically do so within sixty days.

22 Law enforcement has sixty days from the time Google turns over Step 2 data to request Step 3 information.

23 Although the subsequent warrants evaluated in a separate Opinion, explain officers' investigatory efforts to identify a suspect beyond reviewing security camera footage, the Geofence Warrant contains no information about those efforts. Because the Geofence Warrant does not expressly incorporate these subsequent warrants—and indeed, it could not have because officers obtained them after drafting the Geofence Warrant —the Court will consider only the following facts in its analysis. *See* *United States v. Hurwitz*, 459 F.3d 463, 470 (4th Cir. 2006) (requiring that a warrant either incorporate a supporting document by reference or attach the document to warrant itself in order for a court to read the document alongside the warrant).

24 The Virginia Code imposes one educational requirement on the Commonwealth's magistrates: they must possess a bachelor's degree "from an accredited institution of higher education." Va. Code § 19.2-37. The Code does not further define what qualifies as an "accredited institution" for the purpose of magistrates. Chatrie disputes whether Magistrate Bishop's alma mater, Pensacola Christian College, is sufficiently "accredited" under the Virginia Code. (ECF No. 135, at 6–9.) The Court will speak to this later in the Opinion.

25 Det. Hylton did note, however, that because Magistrate Bishop did not read the Warrant in front of him, Magistrate Bishop "*could* have consulted with someone" about it. (ECF No. 202, at 362 (emphasis added).)

26 Thus, the total area of the geofence is 70,686 square meters—about three and a half times the *footprint* of a New York city block. Michael Kolomatsky, *How Big Is an Acre, Anyway?* N.Y. Times (July 26, 2018), https://nyti.ms/345CjS7. Of course, this portion of suburban Richmond, Virginia does not have the density (or height) comparable to that of seven New York City blocks.

27 The warrant included in the definition of "identifying account information/CSI" the following:

> user name and subscriber information to include date of birth if available, account type and account number, email addresses associated with the account, electronic devices associated with the account and their identifying make, model and other identifying numbers, telephone numbers associated with the account

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> including telephone numbers used to set up the account, verify the account or to receive assistance with the account, and Google Voice phones numbers associated with the account.
>
> (ECF No. 54-1, at 4.)

28 Google provides this information in a table, sorted into seven columns: "Device ID," "Date," "Time," "Latitude," "Longitude," "Source," and "Maps [Confidence Interval]." (*See, e.g.*, Mar. 4–5 Hr'g Def. Ex. 3, at 7.) Google LIS Rodriguez testified that the Device ID is not an identifier for "any other specific Google account." (ECF No. 202, at 176.) It is not cross-referenced by Google outside of Location History, but if an individual device were responsive to two different geofence warrants, the ID would be the same in both. Law enforcement does not return this information to Google nor, in this case, did it return the data to the Chesterfield County Court.

29 The Court acknowledges that as a matter of fact, it is unlikely that this user would have been located far outside the geofence. As FBI Agent D'Errico testified during the March 4-5 Suppression Hearing, this user first reported a location point within the geofence with a confidence interval of around 84 meters. The next location point, reported only thirty seconds later, was the point with the 387-meter confidence interval—but the user's reported location was in exactly the same spot as the prior point. It is thus unlikely that the user would have traveled from an area in or near the geofence to a location significantly outside of it within thirty seconds. FBI Agent D'Errico did note, however, that these location points were "indicative ... that the device [was] moving," and that "for some reason, ... a new center coordinate was not obtained by that phone." (ECF No. 202, at 255.) Nevertheless, the notion that geofences *can* capture information from users who are not even in the vicinity of the relevant area troubles the Court and evinces how broad a sweep these warrants may have.

30 On June 17, 2020, Google sought leave to file a Supplemental Declaration of Marlo McGriff (the "Motion for Leave"). The Court granted the Motion for Leave over Chatrie's objection. Given the close proximity in time, the Court continued the then-scheduled July 2, 2020 geofence hearing. The Court found that "the ends of justice [were] best served by granting a short continuance" because "the Geofence Motion to Suppress presents substantial issues of first impression that require the Court to consider a full and accurate record concerning the technology at issue." (ECF No. 115, at 4.) The Court continued the hearing to November 17, 2020.

31 Because this third prong intersects with the Court's good faith analysis, the Court discusses it more fully in Part III.C.2, *infra.*

32 In the federal system, the magistrates who review and sign search warrants are judges who must have law degrees. This is not necessarily the case in state judicial systems.

33 The Framers included the particularity requirement to "end the practice, abhorred by the colonists, of issuing general warrants," which authorized officers to carry out an "exploratory rummaging in a person's belongings." *United States v. Dargan*, 738 F.3d 643, 647 (4th Cir. 2013) (internal citation and quotations omitted). Such "general warrants" placed "the liberty of every [person] in the hands of every petty officer" and were therefore denounced as "the worst instrument of arbitrary power." *Stanford v. Texas*, 379 U.S. 476, 481, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965).

34 In considering whether the Geofence Warrant is valid, the Court assumes for the sake of analysis that the Government's collection of data here is a "search." *See In re Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d at 736 (noting that by obtaining a warrant and arguing for the validity of that warrant, "the [G]overnment is treating its proposed capture of information as a search"). Indeed, this is the position Google advances in its amicus brief.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

35 To be clear, the Court sees individuals from whose accounts the Government obtained data as functional subjects of the search, even though the warrant authorized officers to obtain data only from Google's servers. In the same way that users' devices generate IP address information and typically share that information with a third party, so too do users' phones generate Location History data and share that information with Google. *See, e.g.*, *United States v. Broy*, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. 2016) (treating the defendant's IP address as if it is were defendant's property that he disclosed to a third party).

In other words, regardless of which entity's files the Government looked through, the users ultimately retain at least some joint interest in the location data their phones generate. As discussed in Part III.B.4, *infra*, however, because the Court ultimately finds that Det. Hylton acted in good faith, whether these individuals have an expectation of *privacy* in that data must be decided another day. *Cf, e.g.*, *Broy*, 209 F. Supp. 3d at 1053 (finding no reasonable expectation of privacy because the defendant disclosed his IP address to a third party).

36 Instead, it appears that law enforcement implemented narrowing measures in this Warrant at the behest of Google. (*See* ECF No. 202, at 275–76 (discussing "go bys," template documents that outline "specific information that [Google] need[s] in order to process the search warrant").)

37 For instance, Det. Hylton stated in his affidavit that: (1) surveillance tapes revealed that the suspect used a phone; (2) in the officer's "training and experience, when people act in concert ... they frequently utilize cellular telephones;" (3) Google "provides electronic communication services to subscribers, including email services;" (4) Google "has also developed a proprietary operating system for mobile devices, including cellular phones, known as Android;" and, (5) studies show that "91% of American adults own a cellular phone with 56% being smartphones." (ECF No. 54-1, at 6–7.)

38 The Government has made passing references to "several [additional] pieces of evidence" that might have guided the contours of the Geofence Warrant. (*E.g.*, ECF No. 202, at 272.) But neither the warrant nor its supporting affidavit referred to this evidence. It is therefore irrelevant to the validity of the warrant. *See* *Groh v. Ramirez*, 540 U.S. 551, 557–58, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004) (declining to consider material contained in a warrant's *application* where the warrant did not incorporate the application by reference).

39 The fact that data points obtained during Steps 1 and 2 are anonymized when Google reports them does not completely quell this Court's concerns about the invasiveness of this warrant. Even "anonymized" location data—from innocent people—can reveal astonishing glimpses into individuals' private lives when the Government collects data across even a one or two hour period. As noted above, during the March hearing, McInvaille identified three anonymous accounts captured within the geofence—"Mr. Blue," "Mr. Green," and "Ms. Yellow." (ECF No. 201, at 63–71.)

McInvaille testified that, using two hours of only "anonymized" data obtained through the warrant, he could observe each account's reported location, track each account to his or her home, and pinpoint each account's personal identity using publicly available resources even without any Step 3 information. *See* Herbert B. Dixon Jr., *Your Cell Phone is a Spy!*, Am. Bar Ass'n (July 29, 2020), https://bit.ly/3nRuCVq ("Although user data are anonymized, users' identities can nonetheless be determined by following their movements back to their homes and other places.").

40 But one can readily imagine other instances when one's "mere propinquity" to a location, as in *McLamb*, likely *would* provide probable cause to obtain location data for each individual within a geofence. This would *not* necessarily involve improper use of location data. For example, the FBI appears to have employed geofence technology to locate participants in the January 6 Capitol riots. Mark Harris, *How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob*, Wired (Sept. 30, 2021), https://bit.ly/3HktvWU. In that

situation, one's presence within the Capitol *would* perhaps, by itself, provide probable cause that an individual was present without permission and was therefore committing a crime.

41 Throughout this litigation, the parties—and Google—drew or resisted analogies to tower dumps. As explained above, however, the lead tower dump cases like *James* do not persuade this Court. Those decisions either decide that individuals' proximity to certain towers *alone* creates probable cause to search them, or altogether neglect to consider such particularity concerns. *James*, 2018 WL 6566000, at *4; *see also* *United States v. James*, 3 F.4th 1102, 1106 (8th Cir. 2021) (affirming the district court's adoption of the magistrate judge's original opinion on the same grounds). Indeed, the Eighth Circuit in *James* expressly warned that in holding valid the warrants at issue—which connected a robber to a *series* of crimes—was *not* holding "that it is now fair game to search the records from 'cell phone towers near the location of *every* crime.' " *Id.* at 1106. The Court similarly concludes here that the commission of a single crime—by itself, and with no narrowing measures or guardrails—is not sufficient to search geofence records "near the location of *every* crime." *Id.*

42 The warrant in the DDC Opinion differed in additional ways. For instance, that warrant appears to have sought only location data that fell *within* the geofence across time periods notably shorter than the geofence at bar. *See* DDC Op. at *12 ("[T]he geofence only provides cell phone user's whereabouts in a single area for a handful of minutes on the days in question, not the sum-total of their daily movements."). Here, by contrast, the Government sought two hours of location data *not* bound within the geofence. *Cf.* DDC Op. *12 ("[T]he warrant does not seek location data for days or even hours to track the whereabouts of the perpetrators, but rather location data that is tailored and specific to the time of the [alleged crimes] only." (second alteration in original) (quotation marks and citation omitted)).

In addition to restricting officers' discretion when selecting which accounts for which to obtain personally identifying information, limiting the pool of data returned to only location points *within* the geofence helps assuage this Court's concerns with respect to particularized probable cause, and, more broadly, concerns that broad swaths of anonymous data can be used to pinpoint numerous individuals' identities.

43 The Court recognizes that the Government primarily argues that it possessed probable cause to obtain *all* data sought regardless of the three-step process.

44 The facts also raise a concern about how even good faith effort by law enforcement can impinge upon constitutional boundaries through a lack of understanding as to what this warrant actually produces and how it does so. While all performed in good faith—especially given this novel and complex process—Det. Hylton returned the warrant before it was served, improperly requested Step 2 and 3 information simultaneously, failed at first to narrow his request at Step 2, and incorrectly tried to add a Step 4 to the process. While the Google LIS allowed only what was permitted under the warrant (which Det. Hylton did not resist), Fourth Amendment protections should not be left in the hands of a private actor.

45 Det. Hylton received this remonstration despite having executed three geofence warrants prior to this one.

46 As Google's expert Mario McGriff testified, Location History also allows Google to estimate a device's *elevation.* Thus, if New York City law enforcement obtained a geofence warrant with a roughly 150-meter radius (similar in size to the one at issue here) that encircled the Empire State Building, even if it were not fully precise, the police might be able to obtain location data for many thousands of people.

47 The Court therefore rejects Chatrie's argument that "one who had even a rudimentary understanding of the Fourth Amendment's particularity and breadth requirements" would know that this warrant was insufficient. (ECF No. 205, at 42.)

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

48 This is particularly so because Det. Hylton's "consultation with [G]ovemment attorneys [in the face of untested investigatory techniques] is precisely what *Leon's* 'good faith' expects of law enforcement." *McLamb*, 880 F.3d at 691.

49 TRACS is a national agency recognized by the Council for Higher Education Accreditation and the United States Department of Education. *CHEA-and USDE-Recognized Accrediting Organizations*, CHEA (last visited Mar. 1, 2022), https://bit.ly/3***o***g0sLw.

End of Document © 2022 Thomson Reuters. No claim to original U.S. Government Works.

KeyCite Yellow Flag - Negative Treatment
Disagreed With by People v. Mendez, N.Y.Sup., October 13, 2021

690 F.3d 226
United States Court of Appeals,
Fourth Circuit.

UNITED STATES of America, Plaintiff–Appellee,
v.
Earl Whittley DAVIS, a/k/a Baby Earl, a/k/a E, Defendant–Appellant.

No. 09–4890.
|
Argued: Dec. 9, 2011.
|
Decided: Aug. 16, 2012.

Synopsis

Background: Following denial of his motion to suppress, 657 F.Supp.2d 630, defendant was convicted in the United States District Court for the District of Maryland, Roger W. Titus, J., of Hobbs Act robbery, possession and discharge of firearm in furtherance of crime of violence, possession and discharge of firearm in furtherance of crime of violence resulting in death, and carjacking, and he appealed.

Holdings: The Court of Appeals, Agee, Circuit Judge, held that:

[1] officer's seizure of defendant's clothing fell within scope of plain view exception to warrant requirement;

[2] extraction of DNA sample from defendant's clothing and creation of his DNA profile constituted "search";

[3] extraction of defendant's DNA sample from his clothing and creation of his DNA profile for testing in murder investigation constituted unreasonable searches;

[4] use of defendant's DNA profile to identify him as perpetrator fell within scope of good faith exception to exclusionary rule; and

[5] court did not abuse its discretion in excluding expert testimony regarding lineup procedure and unreliability of eyewitness testimony.

Affirmed.

Davis, Circuit Judge, dissented and filed opinion.

West Headnotes (18)

[1] Searches and Seizures Plain View from Lawful Vantage Point

Plain view doctrine is not exception to warrant requirement for Fourth Amendment search. U.S.C.A. Const.Amend. 4.

30 Cases that cite this headnote

[2] Criminal Law Review De Novo
Criminal Law Evidence wrongfully obtained

Court of Appeals reviews factual findings underlying motion to suppress for clear error and district court's legal determinations de novo.

26 Cases that cite this headnote

[3] Criminal Law Reception of evidence

When suppression motion has been denied, Court of Appeals reviews evidence in light most favorable to government.

23 Cases that cite this headnote

[4] Searches and Seizures Plain View from Lawful Vantage Point

For plain view exception to warrant rule to apply, government must show that: (1) officer was lawfully in place from which object could be viewed; (2) officer had lawful right of access to seized items; and (3) items' incriminating character was immediately apparent. U.S.C.A. Const.Amend. 4.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

26 Cases that cite this headnote

[5] **Searches and Seizures** Plain View from Lawful Vantage Point

Police officer had lawful access to shooting victim's bloody clothing from his hospital room, and thus officer's seizure of clothing fell within scope of plain view exception to warrant requirement, even though clothes were in bag, and not immediately visible, where officer was in room lawfully, bag containing clothing was in plain view, officer was aware of hospital's policy of placing patient's clothing in bag on shelf under his bed, officer could see that victim had been shot in his upper right thigh and was no longer wearing pants or underwear, and it was nearly certain that victim's pants would contain blood and bullet hole, and would thus be incriminating evidence in shooter's prosecution. U.S.C.A. Const.Amend. 4.

29 Cases that cite this headnote

[6] **Searches and Seizures** Circumstances Affecting Validity of Warrantless Search, in General

Otherwise lawful seizure of physical evidence does not become illegal merely because non-perpetrator's DNA may be on that evidence. U.S.C.A. Const.Amend. 4.

[7] **Searches and Seizures** Expectation of privacy

Fourth Amendment's protections are activated only when state conducts search or seizure in area in which there is constitutionally protected reasonable expectation of privacy. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

[8] **Searches and Seizures** Fourth Amendment and reasonableness in general

Fourth Amendment does not prohibit all searches, only those that are unreasonable. U.S.C.A. Const.Amend. 4.

8 Cases that cite this headnote

[9] **Searches and Seizures** Taking samples of blood, or other physical specimens; handwriting exemplars

Analysis required to obtain DNA profile generally qualifies as "search," for Fourth Amendment purposes, because individual retains legitimate expectation of privacy in information obtained from testing, even when there is no issue concerning collection of DNA sample. U.S.C.A. Const.Amend. 4.

7 Cases that cite this headnote

[10] **Searches and Seizures** Expectation of privacy

Person who is solely crime victim does not lose all reasonable expectation of privacy in his or her DNA material simply because it has come into lawful possession of police, even if victim is later arrested. U.S.C.A. Const.Amend. 4.

3 Cases that cite this headnote

[11] **Searches and Seizures** Taking samples of blood, or other physical specimens; handwriting exemplars

Extraction of DNA sample from crime victim's clothing and creation of his DNA profile constituted "search" for Fourth Amendment purposes, even though police lawfully obtained clothing, and victim was later arrested in connection with another incident. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

[12] **Searches and Seizures** Emergencies and Exigent Circumstances; Opportunity to Obtain Warrant

"Special needs doctrine" allows warrantless searches where Fourth Amendment intrusion serves special governmental needs, beyond normal need for law enforcement, and when balancing individual's privacy expectations against government's interests leads to

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

determination that it is impractical to require warrant or some level of individualized suspicion in particular context. U.S.C.A. Const.Amend. 4.

2 Cases that cite this headnote

[13] **Searches and Seizures** Samples and tests; identification procedures

Reasonableness of police department's testing and retention of crime victim's DNA profile was properly analyzed under totality of circumstances test, rather than pursuant to special needs doctrine, where victim was aware that police had retained clothing containing his blood in connection with criminal investigation, yet did nothing to retrieve clothing or otherwise claim ownership in it. U.S.C.A. Const.Amend. 4.

[14] **Searches and Seizures** Samples and tests; identification procedures

Police department's extraction of defendant's DNA sample from his clothing and creation of his DNA profile for testing in murder investigation constituted unreasonable searches under Fourth Amendment, even though police had lawfully obtained defendant's bloody clothing from hospital after he had been shot in unrelated incident, and did not obtain DNA sample from his person, where defendant was free citizen and had never been convicted of felony at time DNA searches were conducted, and defendant's DNA was specifically sought as result of police suspicions that he was involved in murder, and based on some quantum of proof amounting to less than probable cause. U.S.C.A. Const.Amend. 4.

14 Cases that cite this headnote

[15] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

Police department's use of defendant's DNA profile to identify him as perpetrator of armed robbery and murder fell within scope of good faith exception to exclusionary rule, even if extraction, testing, and retention of defendant's DNA profile violated Fourth Amendment, where clothing containing defendant's blood was lawfully within department's custody, officers knew of clothing's existence because of defendant's arrest on drug charges when he left hospital, it appeared that analyst who entered defendant's DNA profile into database was not aware that sample was obtained while defendant was crime victim, and there was no evidence that improper retention of DNA profiles in similar circumstances was systemic or recurring problem. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

[16] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

In assessing applicability of good faith exception to exclusionary rule, courts must weigh deterrent effect of applying rule against cost to society. U.S.C.A. Const.Amend. 4.

9 Cases that cite this headnote

[17] **Criminal Law** Reception and Admissibility of Evidence

Criminal Law Admissibility

Court of Appeals reviews district court's evidentiary rulings, including rulings on admissibility of expert testimony, for abuse of discretion.

3 Cases that cite this headnote

[18] **Criminal Law** Eyewitnesses

District court did not abuse its discretion in armed robbery prosecution in excluding expert testimony regarding lineup procedure and unreliability of eyewitness testimony, where jurors using common sense and their faculties of observation were capable of judging credibility of eyewitness's identification, probative value of expert's testimony was low, points that would have been made by expert were made by defense counsel on cross-examination, and there was overwhelming evidence of guilt. Fed.Rules Evid.Rule 403, 28 U.S.C.A.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

4 Cases that cite this headnote

Attorneys and Law Firms

***228 ARGUED:** Paresh S. Patel, Office of the Federal Public Defender, Greenbelt, Maryland, for Appellant. Deborah A. Johnston, Office of the United States Attorney, Greenbelt, Maryland, for Appellee. **ON BRIEF:** James Wyda, Federal Public Defender, Baltimore, Maryland, for Appellant. Rod J. Rosenstein, United States Attorney, Baltimore, Maryland, Emily N. Glatfelter, Assistant United States Attorney, Office of the United States Attorney, Greenbelt, Maryland, for Appellee.

Before AGEE, DAVIS, and KEENAN, Circuit Judges.

Affirmed by published opinion. Judge AGEE wrote the majority opinion, in which Judge KEENAN joined. Judge DAVIS wrote a dissenting opinion.

OPINION

AGEE, Circuit Judge:

A jury convicted Earl Whittley Davis of various federal offenses arising from a course of conduct that included the armed robbery and murder during that robbery of an armored car employee, Jason Schwindler, as well as a subsequent carjacking. [1] On appeal, Davis challenges the ***229** use of DNA evidence against him at trial, and also argues that the district court erred in excluding expert testimony proffered by Davis in an attempt to undermine an eyewitness identification of him. For the reasons set forth below, we affirm the judgment of the district court.

I.

All of Davis' convictions arose from the same brief course of events occurring in Prince George's County, Maryland. The district court accurately summarized the facts as follows:

> On August 6, 2004, shortly before 1:00 p.m., Jason Schwindler, an armored car employee, picked up a bank deposit from a local business and took it to a nearby BB & T bank in Hyattsville, Maryland. As Schwindler walked up to the bank entrance, two [gunmen] exited a Jeep Cherokee and began shooting at Schwindler, killing him. When their escape in the Jeep was thwarted by the armored truck driver, the assailants carjacked a bank customer and fled in her vehicle[, a Pontiac Grand Am, which] was later recovered.

United States v. Davis, 657 F.Supp.2d 630, 635 (D.Md.2009).

After the murder, officers from the Prince George's County Police Department ("PGCPD") responded to the scene and collected numerous items of evidence, including a baseball cap worn by one of the shooters, two firearms, ammunition, and the steering wheel covers from the Jeep Cherokee and the Grand Am. After swabbing and analyzing the items for DNA, the profiles of the major contributors to the DNA found in the ball cap and on the triggers and grips of the recovered firearms were entered into the local Combined DNA Index System ("CODIS") database. [2] A search of the local database led to a "cold hit" between the DNA recovered at the Schwindler murder scene and Davis' DNA profile, which was already present in the local database.

Based on the "cold hit," officers obtained a search warrant to obtain a sample of Davis' DNA directly from him, which again matched the evidence from the Schwindler murder scene. Evidence of this second match was introduced at trial in this case.

Prior to trial, Davis filed a motion to suppress the use of all DNA evidence against him, arguing that his DNA profile had been obtained by police and entered into the local PGCPD DNA database in violation of his Fourth Amendment rights. The district court held an evidentiary hearing, but declined to rule on the motion to suppress immediately, instructing the parties to continue preparing for trial. After a jury found Davis guilty of the charges, the district court issued a lengthy written order denying the motion to suppress. *Davis,* 657 F.Supp.2d 630–67. Davis was sentenced by the district court

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

on September 18, 2009 to a term of life imprisonment plus 420 months. [3]

Davis noted a timely appeal, and we have jurisdiction pursuant to 28 U.S.C. § 1291.

***230** II.

Background and Proceedings Below

On August 29, 2000, almost four years before the Schwindler murder, Davis arrived at Howard County General Hospital with a gunshot wound to his leg. He claimed to be a robbery victim and reported that he had been shot by the purported robber. Hospital personnel called the police, as Maryland law required, and Patrol Officer Joseph King of the Howard County, Maryland, Police Department ("HCPD") responded to the call. [4] Officer King found Davis lying on a bed in the emergency room. He was conscious, sitting up, and able to converse with Officer King at the time. Davis' pants and boxer shorts had been removed by hospital personnel and placed in a plastic hospital bag, which was stored on a shelf beneath the bed. Officer King observed Davis' gunshot wound and secured Davis' pants and boxer shorts as evidence of the reported shooting. He did so without express permission from Davis (although Davis saw him take the clothing) and without a warrant. He then gave those items to his colleague, Detective Steven Lampe, who placed them in the HCPD "property room," to be held as evidence in the prosecution of Davis' assailant.

At the suppression hearing, Officer King testified that he could not recall exactly what the bag looked like containing Davis' clothes, and neither could Detective Lampe, except that the bag was "plastic." (J.A. 166.) Officer King testified, however, that he had "responded to the hospital on numerous calls," that he knew it was the hospital's "practice to secure any property" taken from a patient and that the hospital placed that "[c]lothing from a victim ... under [the patient's] bed." (J.A. 147.) He also testified that he did not need "permission from anyone in the hospital to access" the bag. (J.A. 150.)

No one was ever charged in the August 2000 shooting of Davis, and neither his clothing nor the blood on it were ever tested in connection with that shooting. Davis was not contacted or advised that the shooting investigation was no longer being pursued by the HCPD, nor was he offered the opportunity to retrieve his clothing. Instead, Davis' clothes, containing his DNA material, [5] were simply retained by the HCPD.

In order to give a more complete picture of later events, we note certain additional facts concerning Davis' hospital stay. First, although Davis had given a false name and false driver's license upon his admission to the hospital, police later learned his true identity through fingerprinting analysis. Additionally, from the beginning of their questioning of Davis, Officer King and Detective Lampe believed Davis was being uncooperative so they conducted further investigation. That investigation led to the discovery of marijuana in the vehicle in which Davis had arrived at the hospital, as well as several other potentially incriminating items, such as a t-shirt and a ball cap that said "FBI," a handheld radio, leg shackles, gloves, and a mask. As a result, Davis was arrested on drug charges upon his ***231** release from the hospital, but those charges were later dropped.

The government does not dispute that Davis' clothing was seized initially because it was evidence of a crime in which he was a victim. The clothing was logged into the HCPD property room, however, on the same sheet with the marijuana found in the car and the false ID card Davis had presented. It also was Davis' arrest record on the drug offense that later led the PGCPD to inquire and learn about the existence of the seized clothing. *Davis,* 657 F.Supp.2d at 634–35 (noting that in April 2004, Lampe "was contacted by members of [PGCPD], who asked him questions about the arrest of Earl Davis in 2000."). When the clothing was later checked out to the PGCPD for testing in a subsequent murder investigation, however, the form indicated that the clothes and blood were from the victim of a shooting. In effect, then, Davis had a "dual status" throughout the events in this case—he was both victim and arrestee—a fact which becomes important when analyzing his Fourth Amendment claims.

In June 2001, an individual named Michael Neal was murdered in Prince George's County. In April 2004, a PGCPD homicide detective investigating the Neal murder, Detective K. Jernigan, learned that Davis had previously been arrested in Howard County and that the HCPD had Davis' clothes. The PGCPD suspected Davis was involved in the Neal murder. [6] As a result, they requested and obtained Davis' clothing, without a warrant, from the HCPD.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

In June 2004, the PGCPD extracted Davis' DNA from the blood stains on Davis' pants, again without a warrant, and created a DNA profile from the test results. That DNA was compared to an unknown DNA sample recovered from the scene of the Neal homicide, but there was no match. Despite the fact that Davis' DNA profile excluded him as the source of the evidentiary sample from the Neal murder, the PGCPD nonetheless retained his DNA profile, and approximately one week later, included it in their local DNA database.

At a hearing before a Maryland state court in its Schwindler murder prosecution, [7] which is part of the record before us, the DNA analyst for the PGCPD, Julie Kempton, testified concerning the extraction of Davis' profile and its entry into the local database. She testified that she was told by a detective that the boxer shorts were taken "from a suspect, from a hospital emergency room where he had been brought in [she] believe[d] for a shooting[.]" (Supp. J.A. 93.) She further testified that her testing ultimately excluded Davis' profile as a match in the Neal homicide. (Supp. J.A. 93–94.) She also testified that she knew that, at the state level of the CODIS database, a suspect's profile should be deleted if the court ordered expungement based on a vacated conviction. The record does not disclose any ***232** other information as to why the profile was retained, whether that was a common policy or practice, or whether it violated any local rule, regulation, policy, or practice to do so. [8]

As noted earlier, in the course of the investigation of the robbery and murder of Mr. Schwindler, when the DNA profile recovered from the Schwindler crime scene was entered into the PGCPD DNA database, a "cold hit" resulted with the DNA sample that had been lifted from Davis' clothing. The PGCPD then secured a search warrant to obtain a DNA sample directly from Davis. That subsequent DNA profile of Davis also matched the DNA samples from the Schwindler crime scene.

Evidence of the match between the known sample obtained via the search warrant and the crime scene evidence was introduced at Davis' trial. Specifically, DNA analyst Sarah Chenoweth testified that Davis' DNA matched DNA profiles from the baseball cap and both cars' steering wheel covers, and testified as to the infinitesimally small probabilities that the DNA on those items came from any person other than Davis. [9]

Davis moved to suppress the DNA evidence against him, arguing that it was obtained in violation of the Fourth Amendment. In a lengthy order denying suppression, the district court addressed each of Davis' challenges. The court concluded that Davis' Fourth Amendment rights were violated only when his DNA profile was retained in the local DNA database, after Davis' profile did not match the DNA sample from the Neal murder, but found no other violations. As to the retention of Davis' profile, the court concluded that the "good faith" exception should be applied and thus the application of the exclusionary rule was not warranted.

III.

Davis' Challenge to the DNA Evidence

Davis alleges three separate Fourth Amendment violations regarding the collection and retention of his DNA. Specifically, Davis asserts that each of the following actions by police constituted a Fourth Amendment violation: (1) the seizure of his clothing from the hospital room and its subsequent search; (2) the extraction of his DNA profile and testing in connection with the Neal murder investigation; and (3) the retention of his DNA profile in the local DNA database. [10]

[1] For the reasons discussed below, we agree with the district court that no Fourth Amendment violation occurred in the seizure of the bag containing Davis' clothing at the hospital. We also agree that any subsequent "search" of the bag was not unlawful because its contents were a foregone conclusion, based in part on Officer King's uncontradicted testimony that he saw "a bag underneath of [Davis'] hospital bed that contained clothing." [11] We further determine that there was a ***233** Fourth Amendment violation when the PGCPD extracted Davis' DNA profile from his clothing and tested it as part of the Neal murder investigation. We assume, without deciding, that there was a separate Fourth Amendment violation in retaining Davis' DNA profile in the local CODIS database. Finally, we conclude that the "good faith exception" to the exclusionary rule applies here to both violations and thus the DNA evidence was not required to be excluded.

[2] **[3]** We review the factual findings underlying a motion to suppress for clear error and the district court's legal determinations de novo. *Ornelas v. United States,* 517 U.S. 690, 699, 116 S.Ct. 1657, 134 L.Ed.2d 911 (1996);

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

United States v. Rusher, 966 F.2d 868, 873 (4th Cir.1992). When a suppression motion has been denied, this Court reviews the evidence in the light most favorable to the government. *United States v. Seidman,* 156 F.3d 542, 547 (4th Cir.1998).

A.

The Seizure of Davis' Clothing in His Hospital Room

Davis first argues that the seizure of his clothing from his hospital room constituted a warrantless seizure that was not justified by any exception to the warrant requirement. The government contends that both the seizure and the subsequent search of the bag containing the clothing were justified by the "plain view" exception, as the district court concluded. [12]

[4] **[5]** For the plain view exception to the warrant rule to apply, the government must show that: (1) the officer was lawfully in a place from which the object could be viewed; (2) the officer had a "lawful right of access" to the seized items; and (3) the incriminating character of the items was immediately apparent. *See* *United States v. Jackson,* 131 F.3d 1105, 1109 (4th Cir.1997). Davis concedes that Officer King was lawfully in the hospital room and thus that the government has satisfied the first requirement, but argues that the government failed to satisfy the latter two requirements. We disagree.

As to the second requirement, Davis contends that, even though Officer King was in the room lawfully, he did not have lawful access to the bag of clothing. The case most heavily relied upon by Davis, ***234** *United States v. Neely,* 345 F.3d 366 (5th Cir.2003), is inapposite. In *Neely,* the Fifth Circuit held the plain view doctrine did not allow the seizure of the patient's clothing, because the clothing at issue was not in open view but in the hospital property storage room, and required permission from hospital personnel to retrieve it. *Id.* at 368, 371. Notably, the hospital patient in *Neely* was the suspect in a criminal investigation, not the victim of a crime like Davis. *Id.* at 367–68.

Neely aside, we have no difficulty finding that there was lawful access to the clothing here. As suggested in *Horton v. California,* 496 U.S. 128, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990), the lawful access requirement is intended to clarify that police may not enter a premises to make a warrantless seizure, even if they could otherwise see (from a lawful vantage point) that there was contraband in plain sight. *Id.* at 137 & n. 7, 110 S.Ct. 2301 (describing the second requirement and explaining that even if "[i]ncontrovertible testimony of the senses" establishes that an object in plain view is contraband, "the police may not enter and make a warrantless seizure"); *see also* *Boone v. Spurgess,* 385 F.3d 923, 928 (6th Cir.2004) (the "lawful right of access" requirement "is meant to guard against warrantless entry onto premises whenever contraband is viewed from off the premises in the absence of exigent circumstances"; thus, while "lawfully positioned" "refers to where the officer stands when she sees the item," "lawful right of access" refers "to where she must be to retrieve the item"). The example given by the government in this case is apt, *i.e.,* the analysis of the first and second prongs might be different if "the officer were lawfully present outside a building, peering through a window into a room in which he would not be lawfully present." (Appellee's Br. 32 n. 8.) Here, however, there is no dispute that Officer King was lawfully present in the hospital room, and he thus had lawful access in the ordinary course of his investigation to the bag of clothing which could be evidence against Davis' assailant. [13] *See* *Washington v. Chrisman,* 455 U.S. 1, 8, 102 S.Ct. 812, 70 L.Ed.2d 778 (1982) ("when a police officer, for unrelated but entirely legitimate reasons, obtains lawful access to an individual's area of privacy ...[,] the Fourth Amendment does not prohibit seizure of evidence of criminal conduct found in these circumstances."); *see also infra* at 237–38 (discussing cases permitting seizure of blood-stained clothing in plain view).

The third prong of the plain view doctrine is less readily resolved. Nonetheless, having carefully reviewed the district court's ruling on this point, we find no clear error in its factual findings, nor any error in its legal conclusions.

Davis' primary argument is that while the bag may have been in plain view, the clothes were not. Thus, he contends that both the seizure and any subsequent search of the bag violated his constitutional rights. The seizure implicated Davis' possessory interest in his clothing, and any subsequent search implicated his privacy interest. *See* ***235** *Texas v. Brown,* 460 U.S. 730, 747, 103 S.Ct. 1535, 75 L.Ed.2d

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

502 (1983) (Stevens, J., concurring in the judgment). As Davis' arguments on this issue acknowledge, under the facts here, the two concepts overlap. Specifically, the seizure of the bag was warranted under the plain view exception only if it was immediately apparent that it contained incriminating evidence. Here, that would require it be immediately apparent that the bag contained evidence of a crime, *i.e.,* Davis' clothing possessing blood, trace evidence, and/or a bullet hole. Similarly, the subsequent search of the bag (whether to identify or examine its contents), was warranted if it was a foregone conclusion that the bag contained the clothing, which was evidence of a crime.

As to both the seizure of the bag and any subsequent search of the bag, the district court's reliance on *United States v. Williams,* 41 F.3d 192 (4th Cir.1994) was appropriate. In *Williams,* officers had properly seized five packages, which consisted of a brown, opaque material wrapped in heavy cellophane. *Id.* at 197–98. The defendant challenged the subsequent warrantless search, in which a police officer removed the cellophane wrapping from one of the packages, poked a hole in the opaque material surrounding its contents, removed a small quantity of white powder and field tested the powder, which tested positive for cocaine. *Id.* at 194.

The *Williams* Court explained that a search of such a container is permissible under the plain view doctrine when "the contents of a seized container are a foregone conclusion." *Id.* at 197. That is, "when a container is not closed, or transparent, or when its distinctive configuration proclaims its contents, the container supports no reasonable expectation of privacy and the contents can be said to be in plain view." *Id.* (citations omitted). *Williams* clearly stated that, "[i]n determining whether the contents of a container are a foregone conclusion, the circumstances under which an officer finds the container may add to the apparent nature of its contents." *Id.* (citing *Blair v. United States,* 665 F.2d 500, 507 (4th Cir.1981)).

Williams also quite plainly allows the experience of the officer to be taken into account when determining whether a container's contents are a "foregone conclusion." *Id.* at 198. There, the Court relied on the testimony of the police officer that, based on his ten years of experience, packages wrapped in this manner contained narcotics, to support the Court's holding that the contents of the container were a "foregone conclusion." *Id.* at 194, 198. The Court also noted that the other items found in the suitcase with the wrapped packages (towels, dirty blankets, and a shirt with a cigarette burn) were unusual for a traveler, in that they did not contain clothing or other items a person normally carries when traveling across the country. *Id.* Thus, in conducting this inquiry, we consider both the circumstances under which the container here was found and Officer King's knowledge about this particular hospital's practices and procedures and his experience in responding to the hospital bedsides of gunshot victims in this particular hospital. [14]

Here, Officer King testified, without contradiction or challenge, that when he entered the curtained-off area where he was told Davis would be, he saw Davis on a hospital bed and observed "a bag underneath of the hospital bed that contained ***236** clothing." (J.A. 140.) He did not testify that he walked into the area and saw what he *thought* might be a bag of clothing under the bed. Drawing the inferences from the facts in the government's favor, as we must, *see Seidman,* 156 F.3d at 547, that testimony fairly supports an inference that Officer King could see the clothing through the bag or that the bag was partially open, revealing clothing. Nothing in the record contradicts such a conclusion. Because the officers were not asked whether the bag was open or closed and could not recall precisely what the bag looked like, however, we do not know for certain "whether the bag was open or closed, or whether it was transparent, opaque or somewhere in-between," *Davis,* 657 F.Supp.2d at 638. [15] What is clear from this record is that Officer King expressed no doubt he observed "a bag ... that contained clothing." (J.A. 140.) Thus, we disagree with the dissent's contention that Officer King's testimony was equivocal, or that his testimony fails to rise to the level of certainty required in *Williams. See post* at 274–75. [16]

Officer King also testified that it was the practice and procedure of the hospital to place a patient's clothing in a bag on the shelf under his bed. He further could visibly see that Davis had been shot in his upper right thigh, and that Davis was no longer wearing pants or underwear. Instead, while Davis was wearing clothing on his upper body, his lower body was exposed, except for his genital area, which was covered by a sheet. (*See* Supp. J.A. 73 (picture of Davis in hospital bed); J.A. 141 (testimony of Officer King that picture accurately depicted what Davis was wearing)).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

We agree with the district court that "the totality of the circumstances, taking into account [Officer] King's experience with the hospital's practices regarding patients' property, the appearance of the Defendant at the time [Officer] King spoke with him, and the obvious fact that the Defendant had been shot in an area of the body usually covered by clothing" support the determination that it was a foregone conclusion the bag under Davis' hospital bed contained the clothing he wore when he was shot.

Davis alternatively contends that even if it had been a virtual certainty that the bag contained Davis' clothing, the incriminating nature of those clothes was not "immediately apparent." We have little trouble, however, in concluding that Davis' pants almost certainly would contain both blood and a bullet hole, [17] and would thus ***237** be incriminating evidence in the prosecution of the shooter. Such a conclusion is based on the circumstances, Davis' appearance, and the location of his bullet wound. As noted by the district court, moreover, Davis has provided no authority to support imposing a requirement that the evidence be incriminating against the person from whom it is seized. *Davis,* 657 F.Supp.2d at 640. As the district court reasoned:

> [The defendant's failure to provide any authority] may be due to the unique situation presented by the facts of this case; very rarely will a victim from whom evidence is seized later become a criminal defendant with standing and reason to challenge the previous seizure. As a matter of first impression, however, it would seem unwise and overly restrictive to require police to know who will be incriminated by an item in plain view before they are able to seize it and investigate further.
>
> *Id.*

Indeed, Supreme Court cases and authority from other circuits explain that an item need not itself be contraband before it has an "incriminating nature," but instead, an item need only be evidence of a crime. *Texas v. Brown,* 460 U.S. 730, 742, 103 S.Ct. 1535, 75 L.Ed.2d 502 (1983) (Rehnquist, J., plurality opinion) (discussing plain view doctrine and whether items may be "contraband or stolen property or *useful as evidence of a crime* ") (emphasis added); *United States v. Smith,* 459 F.3d 1276, 1293 (11th Cir.2006) ("the scope of the 'plain view' doctrine extends to the seizure of items that, while not contraband themselves, may be used as evidence against a defendant"); *United States v. Rodriguez,* 601 F.3d 402, 407 (5th Cir.2010) ("The incriminating nature of an item is 'immediately apparent' if the officers have 'probable cause' to believe that the item is either *evidence of a crime* or contraband.") (emphasis added and citation omitted); *United States v. Chipps,* 410 F.3d 438, 443 (8th Cir.2005) (warrantless seizure of a sweatshirt on the ground outside a house where there had been a reported assault was justified by the plain view doctrine, since "the incriminating nature of a bloody sweatshirt at the site of a potential assault was obvious" and the officer "had a legal right to access the shirt —it was right in front of him on the ground"); *Chavis v. Wainwright,* 488 F.2d 1077, 1078 (5th Cir.1973) (clothing in plastic hospital bag was properly seized from stabbing victim in hospital without a warrant as evidence of an assault, despite fact that victim told police he did not want to prosecute his assailant girlfriend). [18] Here, like the bloody clothing in *Chipps* and in *Chavis,* the pants with a bullet hole, which would be clear evidence a shooting occurred ***238** and might reasonably provide scientific evidence related to the gun caliber, distance, etc., is evidence of a crime and hence, has an immediately apparent "incriminating nature." [19]

For all of the foregoing reasons, we conclude that the plain view doctrine justified both the warrantless seizure and the subsequent search of the bag containing the clothing under Davis' hospital bed.

Before turning to the issues surrounding the extraction and testing of Davis' DNA, we respond briefly to two points raised by the dissent regarding the seizure and search of the clothing and our application of *Williams.* First, the dissent argues *Williams* is distinguishable on the grounds that the district court here considered *only* extrinsic evidence, while the *Williams* court considered such extrinsic evidence in addition to the physical appearance and character of the container. Relatedly, the dissent further states, without citation to authority, that "[n]arcotics packaging is so readily recognizable as to rise to the level of the archetypal kit of burglar tools or a gun case," while the bag here was not ***239** "distinctive in any way." *Post* at 274–75, 275. We disagree.

The dissent's assertions that drug packaging is "readily recognizable" as such while a bag containing a hospital patient's clothing is not, is true only if the contextual evidence

present in *Williams* is being taken into account, *i.e.,* the fact that the packaging was in a suitcase with very few other items one would suspect to find in a traveler's luggage, and the contextual evidence here is ignored, *i.e.,* that the bag was underneath a gunshot victim's hospital bed. But *Williams* expressly permits us to consider the context and circumstances of the specific case, as well as the experience of the officer. Here, those factors compel the conclusion that the bag under Davis' bed contained his clothing. [20]

Second, the dissent suggests an inconsistency between our upholding the seizure of Davis' clothing at the hospital (which obviously contained his DNA), but concluding that he had a reasonable expectation of privacy in his DNA such that its later use violated his Fourth Amendment rights. *See post* at 275–76 (it is "curious, to say the least, to reason as does the majority that Davis retained, for several years after the bag was seized at the hospital, a reasonable expectation of privacy in the character of his DNA molecules, but that he lacked any reasonable expectation of privacy in the presence of those molecules in his blood while they were embedded in his clothing" while at the hospital). This perceived inconsistency is based on a misunderstanding of our holding.

We do not hold that Davis had no expectation of privacy in his DNA while it was on his clothing at the hospital. What we conclude is that the seizure and search of the bag containing Davis' clothing were permitted under the plain view doctrine because his clothing was evidence of a crime and was in plain view, as applied in *Williams*. *See infra* at 244 ("while Davis may not have had any expectation of privacy in the outward appearance of the clothing once it was in police custody, we nevertheless must consider ... whether Davis retained a reasonable expectation of privacy in his DNA on the clothing or in the DNA profile obtained from it.")

[6] Davis always had an expectation of privacy in his DNA, but that expectation of privacy was not implicated merely by an effort to identify, describe and catalogue his clothing as evidence of a reported crime, rather than testing anything found on it. It was not until the police sought to obtain a DNA profile from his blood that his privacy interest in his DNA was implicated. As we explain, the search of his DNA did not occur until the police extracted and tested his DNA in conjunction with the Neal murder. *See infra* at Section III.B.2. The dissent's perceived "inconsistency" in our holdings does not exist. [21]

***240** B.

The Extraction and Testing of Davis' DNA Profile for Use in the Neal Murder Investigation, and the Retention of Davis' DNA Profile

Having concluded that the HCPD lawfully obtained the clothing that contained Davis' DNA material, we now turn to Davis' contention that the PGCPD violated the Fourth Amendment by extracting his DNA from the blood on that clothing and testing it for use in the Neal murder investigation, as well as in retaining his profile in their local DNA database.

1.

General Fourth Amendment Principles

The general issue of a person's reasonable expectation of privacy in his DNA is a developing and unsettled area of the law, one that has not yet been addressed by the Supreme Court. The relative recency of the technology, especially when coupled with its potential power, is no doubt part of the reason why there is uncertainty over the degree of privacy persons can reasonably expect to have in their DNA. *Cf. Dist. Attorney's Office for the Third Judicial Dist. v. Osborne,* 557 U.S. 52, 129 S.Ct. 2308, 2316, 174 L.Ed.2d 38 (2009) ("Modern DNA testing can provide powerful new evidence unlike anything known before ... DNA testing has exonerated wrongly convicted people, and has confirmed the convictions of many others."); *Jones v. Murray,* 962 F.2d 302, 307 (4th Cir.1992) (describing DNA as a "dramatic new tool for the law enforcement effort to match suspects and criminal conduct"). [22]

***241** **[7]** The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. However, the protections of the Fourth Amendment are activated only when the state conducts a search or seizure in an area in which there is a "constitutionally protected reasonable expectation

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

of privacy." *New York v. Class,* 475 U.S. 106, 112, 106 S.Ct. 960, 89 L.Ed.2d 81 (1986) (citation omitted). When there is no reasonable expectation of privacy, the Fourth Amendment is not implicated.[23] *See, e.g., United States v. Dionisio,* 410 U.S. 1, 14, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973) (no reasonable expectation of privacy in one's voice); *United States v. Mara,* 410 U.S. 19, 21, 93 S.Ct. 774, 35 L.Ed.2d 99 (1973) (no reasonable expectation of privacy in one's handwriting); *California v. Greenwood,* 486 U.S. 35, 37, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988) (same as to trash left by the curb). A search or seizure for Fourth Amendment purposes does not occur, therefore, when a person lacks a reasonable expectation of privacy in the material examined. *United States v. Breza,* 308 F.3d 430, 433 (4th Cir.2002) (citing *Illinois v. Andreas,* 463 U.S. 765, 771, 103 S.Ct. 3319, 77 L.Ed.2d 1003 (1983)).

[8] Even if a search has occurred without a warrant and without individualized suspicion, a Fourth Amendment violation does not necessarily occur. The Fourth Amendment does not prohibit all searches, only those that are unreasonable. *Skinner v. Ry. Labor Execs.' Ass'n,* 489 U.S. 602, 619, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989) ("the Fourth Amendment does not proscribe all searches and seizures, but only those that are unreasonable"); *Terry v. Ohio,* 392 U.S. 1, 9, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968) ("[W]hat the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures.") (quoting *Elkins v. United States,* 364 U.S. 206, 222, 80 S.Ct. 1437, 4 L.Ed.2d 1669 (1960)). And "[a]lthough as a general matter, warrantless searches 'are *per se* unreasonable under the Fourth Amendment,' there are 'a few specifically established ***242** and well-delineated exceptions' to that general rule." *City of Ontario, Ca. v. Quon,* —— U.S. ——, 130 S.Ct. 2619, 2630, 177 L.Ed.2d 216 (2010) (quoting *Katz v. United States,* 389 U.S. 347, 357, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)); *Nat'l Treasury Employees Union v. Von Raab,* 489 U.S. 656, 665, 109 S.Ct. 1384, 103 L.Ed.2d 685 (1989) ("neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance").

2.

Whether Extraction and Testing of Davis' DNA Profile for Use in the Neal Murder Investigation, or its Later Retention, Constituted Searches?

We first consider the threshold question whether a search occurred when the PGCPD extracted and tested Davis' DNA for use in the Neal murder investigation, or when the PGCPD retained Davis' DNA profile in CODIS. Our analysis turns on the question whether Davis had a reasonable expectation of privacy in his clothing and the blood and DNA it contained, once it was in the lawful custody of the HCPD.

The government argues that there was no search or seizure here, relying primarily on *United States v. Edwards,* 415 U.S. 800, 94 S.Ct. 1234, 39 L.Ed.2d 771 (1974), for the proposition that Davis lacked any reasonable expectation of privacy in his clothes or DNA after they were lawfully seized by police.[24] In *Edwards,* the defendant was arrested and charged with an attempted break-in at approximately 11:00 p.m., taken to the local jail and placed in a cell. 415 U.S. at 801, 94 S.Ct. 1234. Investigation at the scene revealed that the attempted entry had been made through a wooden window and that paint chips had been left on the window sill and wire mesh. *Id.* at 801–02, 94 S.Ct. 1234. The next morning (approximately ten hours after his arrest), Edwards was given a change of clothing and his clothing was then taken from him and held as evidence. *Id.* at 802, 94 S.Ct. 1234. Examination of the clothing revealed paint chips matching the samples taken from the window. *Id.* The evidence of the matching paint chips was later introduced at trial, over Edwards' objection. *Id.* The Sixth Circuit reversed, finding the seizure of the clothing, carried out after "the mechanics of [Edwards'] arrest" had been completed, violated the Fourth Amendment. *Id.*

The Supreme Court reversed the Sixth Circuit, holding that the warrantless seizure of the clothing was constitutional. The Supreme Court first noted that warrantless searches are permitted incident to custodial arrests, and that they can legally be conducted later when the accused arrives at the place of detention. ***243** *Id.* at 802–03, 94 S.Ct. 1234. "Nor is there any doubt that clothing or other belongings may

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

be seized upon arrival of the accused at the place of detention and later subjected to laboratory analysis or that the test results are admissible at trial." *Id.* at 803–04, 94 S.Ct. 1234.

The government reads *Edwards* to stand for the proposition that once the police have lawful custody of evidence, like Davis' clothing here, further scientific examination conducted on it by that particular police department or by any other law enforcement body does not first require that a search warrant be obtained. (*See* Appellee's Br. 46.) As a result, the government argues, Davis did not have a reasonable expectation of privacy in the DNA contained in his clothing because it had been lawfully seized by the HCPD. The government accordingly contends that the PGCPD did not violate the Fourth Amendment when the PGCPD later obtained Davis' clothing and extracted the DNA at issue.

The Court in *Edwards,* however, did not adopt the categorical rule advanced by the government:

> In upholding this search and seizure, *we do not conclude that the Warrant Clause of the Fourth Amendment is never applicable to postarrest seizures of the effects of an arrestee.* But we do think that the Court of Appeals for the First Circuit captured the essence of situations like this when it said in *United States v. DeLeo,* 422 F.2d 487, 493 (1970) (footnote omitted): "While the legal arrest of a person should not destroy the privacy of his premises, it does—for at least a reasonable time and to a reasonable extent—take his own privacy out of the realm of protection from police interest in weapons, means of escape, and *evidence.*"

415 U.S. at 808–09, 94 S.Ct. 1234 (footnote omitted and emphasis added); *id.* at 808 n. 9, 94 S.Ct. 1234 ("Holding the Warrant Clause inapplicable in the circumstances present here does not leave law enforcement officials subject to no restraints. This type of police conduct must still be tested by the Fourth Amendment's general proscription against unreasonable searches and seizures.") (internal quotation marks and alteration omitted).

In *Edwards,* the class of person whose item was seized, an arrestee, and the type of item seized, evidence, were material considerations in the Court's analysis. Further, *Edwards* recognized that even an arrestee, who has a diminished expectation of privacy, does not forfeit forever all privacy interests in his effects. Therefore, the *Edwards* decision itself does not support the government's broad categorical assertion that any item in the lawful custody of law enforcement can be subjected to laboratory analysis at any later time and for any purpose related to law enforcement.

[9] Moreover, because the analysis of biological samples, such as those derived from blood, urine, or other bodily fluids, can reveal "physiological data" and a "host of private medical facts," such analyses may "intrude[ ] upon expectations of privacy that society has long recognized as reasonable." *Skinner,* 489 U.S. at 616–17, 109 S.Ct. 1402. Therefore, such analyses often qualify as a search under the Fourth Amendment. *Id.* at 618, 109 S.Ct. 1402 (concluding that "the collection and subsequent analysis of the requisite biological [blood and urine] samples must be deemed Fourth Amendment searches"). Similarly, an analysis required to obtain a DNA profile, like the chemical analysis of blood and urine at issue in *Skinner,* generally qualifies as a search, because an individual retains a legitimate expectation of privacy in ***244** the information obtained from the testing. *See, e.g., United States v. Mitchell,* 652 F.3d 387, 407 (3d Cir.2011) (en banc) (after discussing the Fourth Amendment search that occurs when a DNA sample is collected directly from a person's body, discussing separately "[t]he second 'search' at issue," which was, "of course, the processing of the DNA sample and creation of the DNA profile for CODIS. This search also has the potential to infringe upon privacy interests.").

By contrast, in *Edwards,* the analysis at issue examined paint chips found in the defendant's clothing, which did not implicate the privacy concerns inherent in the use of physiological and medical information obtained from DNA analysis that was addressed in *Skinner. See Edwards,* 415 U.S. at 801–02, 94 S.Ct. 1234. Thus, in the present case, while Davis may not have had any expectation of privacy in the outward appearance of the clothing once it was in police custody, we nevertheless must consider the type of analysis conducted on that clothing to determine whether Davis retained a reasonable expectation of privacy in his DNA on the clothing, or in the DNA profile obtained from it.

The district court concluded that *Edwards* is inapplicable here because, unlike the defendant's clothing in Edwards, Davis' clothing was not seized pursuant to his arrest on the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

drug charges, but was seized before his arrest when his status was that of a reported crime victim. As noted by the district court, to allow the testing and retention of DNA profiles from any evidence lawfully obtained by police could expose a victim of a crime whose blood, or other material from which DNA could be obtained, to having his or her DNA extracted and retained indefinitely in a law enforcement database. The district court reasoned:

> Taken to its logical extreme, the application of *Edwards* and its progeny to the instant case would mean that any citizen whose blood finds its way into lawful police custody as a result of victimization (e.g., child abuse, sexual assault and domestic violence victims, etc.), would then lose any expectation of privacy in the DNA markers in that blood, which could be used against him or her at a later date without the constitutional safeguard that a warrant supported by probable cause first be issued.

Id. at 647. It was on this basis, the distinction between the DNA of a victim and an arrestee, that the district court found *Edwards* inapplicable.

[10] Although we are not faced here with the full range of potential problems identified by the district court, we agree with the district court that a person who is solely a crime victim does not lose all reasonable expectation of privacy in his or her DNA material simply because it has come into the lawful possession of the police. And, although Davis later was arrested, because the police seized his clothing when he was solely a crime victim, we conclude that his later arrest does not eradicate his expectation of privacy in his DNA material.

Our conclusion that Davis' status as a victim materially distinguishes the present case from *Edwards* is supported by our precedent and by decisions of our sister circuits. These decisions, in addressing whether, and under what circumstances, the Constitution allows the collection of DNA samples, uniformly recognize that persons who have not been arrested have a greater privacy interest in their DNA than would persons who have been arrested, such as the arrestee in *Edwards.*

First, our decision in *Jones v. Murray,* 962 F.2d 302 (4th Cir.1992), is instructive. There, we rejected a Fourth Amendment ***245** challenge to a Virginia law that required convicted felons in custody to submit blood samples for DNA analysis. We concluded that the identification of a person arrested upon probable cause "becomes a matter of legitimate state interest and he can hardly claim privacy in it." *Id.* at 306. Additionally, we recognized that "we do not accept even [a] small level of intrusion, [such as fingerprinting] for free persons without Fourth Amendment constraint." *Id.* at 306–07 (citing *Davis v. Mississippi,* 394 U.S. 721, 727, 89 S.Ct. 1394, 22 L.Ed.2d 676 (1969)). Thus, we emphasized that a court's constitutional analysis may differ depending on whether the person is an arrestee or a "free person."

Our sister circuits, in upholding DNA collection statutes against Fourth Amendment challenges, likewise have recognized that the status of an individual whose DNA is sought is material to the issue whether he had a reasonable expectation of privacy in that DNA. In *Mitchell,* for example, the Third Circuit sitting en banc upheld the suspicionless collection of DNA samples from arrestees principally on the basis that the fingerprinting of arrestees did not violate the Fourth Amendment. 652 F.3d at 411 (citing *Hayes v. Florida,* 470 U.S. 811, 813–18, 105 S.Ct. 1643, 84 L.Ed.2d 705 (1985) and *Davis,* 394 U.S. at 727, 89 S.Ct. 1394); *see also* *Mitchell,* 652 F.3d at 402 & n. 13 (collecting authority and noting that "[e]very federal circuit court to have considered [the federal DNA Act and its state law analogues] as applied to an individual who has been convicted and is either incarcerated or on probation, parole, or supervised release has upheld the constitutionality of the challenged statute"). Additionally, in *United States v. Kincade,* 379 F.3d 813 (9th Cir.2004) (en banc), a plurality of the Ninth Circuit held that the federal DNA act requiring the collection of DNA samples from convicted felons was constitutional. *See* 379 F.3d at 835–36 (O'Scannlain, J., plurality opinion) (noting "the obvious and significant distinction between the DNA profiling of law-abiding citizens who are passing through some transient status (*e.g.,* newborns, students, passengers in

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

a car or on a plane) and lawfully adjudicated criminals whose proven conduct substantially heightens the government's interest in monitoring them and quite properly carries lasting consequences that simply do not attach from the simple fact of having been born, or going to public school, or riding in a car"); *see also* *Green v. Berge,* 354 F.3d 675, 678–79 (7th Cir.2004) (rejecting Fourth Amendment challenge to law requiring DNA samples from felons and contrasting felons from persons not otherwise in custody); *id.* at 679–81 (Easterbrook, J., concurring) (constitutional challenges to DNA—collection statutes differ depending on the status of the person whose DNA is being collected, and noting that "[t]his appeal does not present the question whether DNA could be collected forcibly from the general population").

Unlike the cases cited immediately above, however, which concerned parolees, persons on supervised release, convicted felons, or arrestees, the HCPD had possession of Davis' DNA because he was the victim of a crime. Thus, the above cases inferentially provide support for Davis' position, because they all distinguish an arrestee or one convicted of a crime from members of the general public at large.

These cases, however, do not directly answer the question before us, because they involved challenges to the *collection* of DNA samples, and not, as here, a challenge to the extraction of DNA or retention of a DNA profile when the police already had lawful possession of the DNA sample. And, for the same reason, these cases do not eliminate any consideration of *Edwards* in circumstances like these. *But* ***246** *see* *United States v. Weikert,* 504 F.3d 1, 16–17 (1st Cir.2007) (suggesting that "it may be time to reexamine the proposition that an individual no longer has any expectation of privacy in information seized by the government so long as the government has obtained that information lawfully.... In short, there may be a persuasive argument on different facts that an individual retains an expectation of privacy in the future uses of her DNA profile").

Nevertheless, we are persuaded by the Supreme Court's analysis in *Skinner,* as applied in *Mitchell* and other cases in the context of DNA, that the extraction of DNA and the creation of a DNA profile result in a sufficiently separate invasion of privacy that such acts must be considered a separate search under the Fourth Amendment even when there is no issue concerning the collection of the DNA sample. *See* *Mitchell,* 652 F.3d at 407 (citing *United States v. Sczubelek,* 402 F.3d 175, 182 (3d Cir.2005) (citing *Skinner,* 489 U.S. at 616, 109 S.Ct. 1402)).

[11] Based on the foregoing, we conclude that the holding in *Edwards* does not give a law enforcement agency carte blanche to perform DNA extraction and analysis derived from clothing lawfully obtained from the victim of a crime in relation to the investigation of other crimes. Instead, a victim retains a privacy interest in his or her DNA material, even if it is lawfully in police custody. Therefore, we conclude that the extraction of Davis' DNA sample from his clothing and the creation of his DNA profile constituted a search for Fourth Amendment purposes.

We turn to consider whether a separate search occurred when the PGCPD retained Davis' DNA profile in the local CODIS database after the profile did not implicate him in the Neal murder. Our sister circuits do not appear to be uniformly settled on the question whether such entry of a DNA profile into this type of database is a search entitled to Fourth Amendment protection. *Compare, e.g., Boroian v. Mueller,* 616 F.3d 60, 67–68 (1st Cir.2010) (concluding that the retention and later matching of a lawfully obtained DNA profile is not a search for Fourth Amendment purposes and collecting authority for the same) *with* *United States v. Amerson,* 483 F.3d 73, 85 (2d Cir.2007) (in addition to the collection of the DNA sample from a probationer, determining that "[t]here is ... a second and potentially much more serious invasion of privacy occasioned by the DNA Act" because the "analysis and maintenance of [offenders'] information in CODIS ... is, in itself, a significant intrusion") (citation omitted) *and* *Kincade,* 379 F.3d at 841–42 (en banc) (Gould, J., concurring) (suggesting the retention of a lawfully obtained DNA profile once a person has "fully paid his or her debt to society" and "left the penal system" would implicate the person's privacy interest).

These differing conclusions illustrate the fact that at least some courts have concluded that once a DNA profile has been lawfully obtained and entered into CODIS, the retention of that profile and "periodic matching of the profile against other profiles in CODIS for the purpose of identification[,]" is not a search because it does not intrude upon an offender's legitimate expectation of privacy. *Boroian,* 616 F.3d at 67–68 (so holding and citing other authority for the same). [25] Other courts, at ***247** least in principle, have left open the possibility that an unrelated examination after DNA retention

could be a separate search for Fourth Amendment purposes. *See, e.g.,* *Amerson,* 483 F.3d at 85 n. 12.

We need not choose among these competing principles in this case because, as discussed in the next section, we conclude that the extraction and initial testing of Davis' profile was an unreasonable Fourth Amendment search. Accordingly, for purposes of this opinion, we will assume, without deciding, that Davis had a continuing right of privacy in his DNA profile, and that a search occurred in the retention of that profile. We now turn to consider the issue whether the two searches were reasonable.

3.

Whether the Searches Were Reasonable Under the Fourth Amendment?

As noted above, not every warrantless search violates the Fourth Amendment. Instead, a Fourth Amendment violation occurs when a warrantless search is unreasonable. *See* *Skinner,* 489 U.S. at 619, 109 S.Ct. 1402. Courts have employed several different approaches in assessing reasonableness.[26] With regard to searches in which there is an absence of individualized suspicion, the "general Fourth Amendment approach" is to "examine the totality of the circumstances" to determine whether a search is reasonable. *Samson v. California,* 547 U.S. 843, 848, 126 S.Ct. 2193, 165 L.Ed.2d 250 (2006). Under this approach, the reasonableness of a search "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id.* (citation and internal quotation marks omitted).

For example, in *United States v. Knights,* 534 U.S. 112, 122 S.Ct. 587, 151 L.Ed.2d 497 (2001), the Supreme Court applied the totality of the circumstances approach in upholding the search of a probationer's apartment based on the presence of "reasonable suspicion," but in the absence of probable cause. *Id.* at 118, 121, 122 S.Ct. 587. Similarly, in *Samson,* the Court upheld a suspicionless search of a parolee applying the same approach. 547 U.S. at 846, 126 S.Ct. 2193.

***248** **[12]** Courts also have applied a "special needs" analysis in certain circumstances to uphold contested searches. *See* *Griffin v. Wisconsin,* 483 U.S. 868, 107 S.Ct. 3164, 97 L.Ed.2d 709 (1987); *Kincade,* 379 F.3d at 823–832 (en banc) (O'Scannlain, J., plurality opinion) (describing development of the special needs doctrine and various Supreme Court cases utilizing it). The special needs doctrine allows warrantless searches "where a Fourth Amendment intrusion serves *special governmental needs,* beyond the normal need for law enforcement" and "when balancing the individual's privacy expectations against the government's interests leads to the determination that it is 'impractical to require a warrant or some level of individualized suspicion in the particular context.' " *United States v. Rendon,* 607 F.3d 982, 989 (4th Cir.2010) (quoting *Von Raab,* 489 U.S. at 665–66, 109 S.Ct. 1384) (emphasis in *Rendon*).

The district court found here that the special needs doctrine was inapplicable, because "the governmental interest in this case cannot be characterized as anything other than an ordinary interest in law enforcement." *Davis,* 657 F.Supp.2d at 651. Thus, the district court employed the totality of the circumstances test. Applying that test, the district court found the extraction of Davis' DNA in conjunction with the Neal murder investigation was "reasonable." *Id.* at 654.

On appeal, Davis argues that the totality of the circumstances test is not applicable, because it applies only when a person being searched has "substantially diminished privacy rights." (Appellant's Br. 53.) Instead, Davis argues that nothing less than a warrant and probable cause would have allowed the testing and retention of his DNA profile. Davis further argues that, even if the totality of the circumstances test were applicable, the district court applied the test incorrectly. The government also argues that the district court erred in applying the totality of the circumstances test because, in the government's view, *Edwards* resolves the issue against Davis.[27]

[13] We begin this part of our analysis by restating our conclusion that the holding in *Edwards* is not dispositive of the matter under the unique facts before us, and that Davis retained a reasonable expectation of privacy in his DNA profile. We also consider as part of our analysis the fact that Davis' expectation of privacy may have been diminished

to some degree because Davis knew that the police had retained his clothing, yet had taken no action to retrieve his personal effects following his release. Thus, we analyze the reasonableness of the searches here under the "totality of the circumstances test."[28] Our employment of this test is consistent with the decisions of most of our sister circuits, which have applied the test in cases where there was a diminished expectation of privacy. *See* *Mitchell,* 652 F.3d at 403 n. 15 (noting that only the Second and Seventh Circuits have consistently ***249** held that the "special needs" test should apply instead of the totality of the circumstances test in addressing the constitutionality of a DNA indexing statute).

Applying the totality of the circumstances test here requires us to "assess [ ], on the one hand, the degree to which [the search] intrudes upon [Davis'] privacy, and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Knights,* 534 U.S. at 119, 122 S.Ct. 587. When considering the magnitude of the intrusion upon Davis' privacy, we think it very significant that these DNA searches were conducted in 2004, at a time when Davis was a free citizen and had never been convicted of a felony. The PGCPD extracted Davis' DNA from his clothing, created Davis' DNA profile, and checked that profile against evidence on the CODIS database, all while Davis was a free citizen who retained a reasonable privacy interest in his DNA sample and DNA profile, as we have discussed. However, his privacy interest was diminished to a degree by the fact that he knew that the police had retained his bloody clothing, and yet did nothing to retrieve the clothing or otherwise claim ownership in it.

In contrast to many DNA privacy cases, the privacy interest in Davis' bodily integrity was not implicated when police obtained the DNA sample, because it was taken from his clothing, rather than from his person. This too is a factor that we must consider under the totality of the circumstances. *See e.g.,* *Mitchell,* 652 F.3d at 404 (weighing the "minimal" intrusion of privacy caused by DNA sample collection by blood test); *Jones,* 962 F.2d at 307 (weighing "minor intrusion" caused by DNA sample collection by blood test).

We next turn to consider the government's interest in conducting the search. The police, of course, have a strong and important interest in apprehending and prosecuting those who have committed violent crimes, like the Neal murder and the murder of Schwindler in this case. The government also has a legitimate interest in entering and maintaining information in CODIS and in increasing the number of entries in CODIS to improve its efficacy as a crime-solving tool. *See* *Haskell v. Harris,* 669 F.3d 1049, 1062 (9th Cir.2012), *reh'g en banc granted,* 686 F.3d 1121 (2012) (upholding California law requiring police to collect DNA samples from all adult felony arrestees and citing the government's four "key interests": "identifying arrestees, solving past crimes, preventing future crimes, and exonerating the innocent").

In balancing these competing interests to determine the reasonableness of the searches at issue, we are guided by the weighty reasons underlying the warrant requirement: to allow a detached judicial officer to decide "[w]hen the right of privacy must reasonably yield to the right of search," and not "a policeman or Government enforcement agent." *Johnson v. United States,* 333 U.S. 10, 13–14, 68 S.Ct. 367, 92 L.Ed. 436 (1948) (quoted in *Davis,* 657 F.Supp.2d at 653.) The right protected is "a right of personal security against arbitrary intrusions by official power." *Coolidge v. New Hampshire,* 403 U.S. 443, 455, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). The importance of the judge or magistrate in the process is why the exceptions to the warrant requirement are "jealously and carefully drawn." *Id.*

The potential for arbitrary intrusions of one's privacy from warrantless searches in cases involving felons, parolees, or arrestees is mitigated by the fact that officials are required to collect from everyone in that certain group of persons. They cannot selectively choose which persons within a particular group must submit a DNA ***250** sample. *See, e.g.,* *Mitchell,* 652 F.3d at 415 (the search is further rendered reasonable because "there is no room for law enforcement officials to exercise (or abuse) discretion by deciding whether or not to collect a DNA sample"); *Amerson,* 483 F.3d at 82 ("[T]he programmatic nature of the 2004 DNA Act —all felons are required to submit DNA samples, and the uses of those samples are strictly circumscribed—leaves no discretion for law enforcement personnel to decide whether to force an individual to submit to a taking of a DNA sample or how to use the information collected. This lack of discretion removes a significant reason for warrants—to provide a check on the arbitrary use of government power. *See* *Skinner,* 489 U.S. at 621–22, 109 S.Ct. 1402.").

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

[14] In this case, by contrast, Davis' DNA was specifically sought as a result of police suspicions that he was involved in the Neal murder, and based on some quantum of proof amounting to less than probable cause. Indeed, the parties' briefs and the record before us are devoid of any factual basis for concluding that Davis was involved in the Neal murder. Thus, the precise concern that the warrant requirement was designed to alleviate is plainly before us here. That fact alone severely diminishes the reasonableness of the search. Thus, our comparison of the respective interests leads us to conclude that the government's extraction of Davis' DNA sample from his clothing and creation of his DNA profile for testing in the Neal murder investigation constituted unreasonable searches under the Fourth Amendment.

Lastly, we assume, without deciding, that the entry and retention of Davis' profile into the CODIS database under these circumstances was also unreasonable under the Fourth Amendment, because the police only had Davis' DNA profile as a result of a Fourth Amendment violation resulting from the extraction and testing of his DNA profile against the DNA in the Neal investigation.

The conclusion that Fourth Amendment violations occurred does not end our inquiry, however. Instead, as we discuss next, we conclude that the exclusionary rule should not be applied to remedy these violations. [29]

***251** IV.

The "Good Faith" Exception to the Remedy of Suppression

[15] Having determined that there was a Fourth Amendment violation in the extraction and testing of Davis' DNA profile, and having assumed, but not decided, there was a second violation in the retention of his profile, we address whether suppression is the proper remedy. *Leon,* 468 U.S. at 906, 104 S.Ct. 3405 ("Whether the exclusionary sanction is appropriately imposed in a particular case ... is an issue separate from the question whether the Fourth Amendment rights of the party seeking to invoke the rule were violated by police conduct.") (citation and internal quotation marks omitted). As noted, the district court concluded that suppression was not warranted because the "good faith" exception to the exclusionary rule was applicable. For the reasons discussed below, we agree.

The Supreme Court articulated the "good faith" exception to the exclusionary rule in *Leon,* 468 U.S. at 920, 104 S.Ct. 3405. In that case, the Court refused to apply the exclusionary rule where police properly executed a search warrant, but it was later determined the issuing magistrate had erred as the warrant lacked probable cause. *Id.* at 922, 104 S.Ct. 3405. The Supreme Court has also applied the "good faith" exception to warrantless administrative searches performed in good-faith reliance on a statute later declared unconstitutional, *Illinois v. Krull,* 480 U.S. 340, 107 S.Ct. 1160, 94 L.Ed.2d 364 (1987), and to an arrest by police who reasonably relied on erroneous information, entered by a court employee into a court database, that an arrest warrant was outstanding, *Arizona v. Evans,* 514 U.S. 1, 14, 115 S.Ct. 1185, 131 L.Ed.2d 34 (1995).

The Supreme Court's recent decisions applying the exception have broadened its application, and lead us to conclude that the Fourth Amendment violations here should not result in the application of the exclusionary rule. *See* *Herring,* 555 U.S. at 135, 129 S.Ct. 695; *Davis v. United States,* —— U.S. ——, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011).

[16] In both *Herring,* and *Davis,* the Supreme Court emphasized the crucial role that deterrence plays in determining whether to apply the exclusionary rule. Specifically, "the benefits of deterrence must outweigh the costs." *Herring,* 555 U.S. at 141, 129 S.Ct. 695 (citing *Leon,* 468 U.S. at 910, 104 S.Ct. 3405 (1984)). That is, courts must weigh the deterrent effect of applying the rule against the cost to society. The "principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free—something that 'offends basic concepts of the criminal justice system.' " *Id.* at 141, 129 S.Ct. 695 (quoting *Leon,* 468 U.S. at 908, 104 S.Ct. 3405).

In determining the deterrent effect of applying the rule, the *Herring* Court explained that the deterrent effect is higher where law enforcement conduct is more culpable. Thus, " 'an assessment of the flagrancy of the police misconduct constitutes an important step in the calculus' of applying the exclusionary rule." *Id.* at 143, 129 S.Ct. 695 (quoting *Leon,* 468 U.S. at 911, 104 S.Ct. 3405).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

The *Herring* Court explained that the rule should not be applied where excluding the evidence would have little deterrent effect on future constitutional violations by law enforcement officers, and the cost to society of such a rule is high. *Id.* at 147–148, 129 S.Ct. 695 (concluding that "when police mistakes are the result of negligence such as that described here, rather than systemic error or reckless disregard of constitutional requirements, any marginal ***252** deterrence does not 'pay its way' " and the exclusionary rule should not be applied).

In *Herring,* the mistake made by police was that a police department in Dale County, Alabama told the neighboring Coffee County police that the defendant had an outstanding arrest warrant in Dale County. *Id.* at 137–38, 129 S.Ct. 695. In fact, the Dale County arrest warrant had been recalled five months earlier, but had never been deleted from the electronic database. *Id.* at 138, 129 S.Ct. 695. After being given the incorrect information that the warrant was outstanding, a Coffee County police officer detained Herring, and found drugs and a gun on his person. *Id.* Herring sought to exclude the evidence seized from his person. *Id.* at 137, 129 S.Ct. 695.

The majority distinguished the negligent conduct involved in *Herring* from earlier cases where the good faith exception did not apply, calling the error before it the "result of isolated negligence attenuated from the arrest." *Id.* at 137, 129 S.Ct. 695.

More recently, the Supreme Court followed the *Herring* analysis in *Davis,* 131 S.Ct. 2419, where the Court considered "whether to apply [the exclusionary rule] when the police conduct a search in compliance with binding precedent that is later overruled." *Id.* at 2423. The Court ruled that the exclusionary rule should not be applied in those circumstances, "[b]ecause suppression would do nothing to deter police misconduct ... and because it would come at a high cost to both the truth and the public safety." *Id.* In so ruling, the Court again expounded on the balancing test that courts must apply after finding a Fourth Amendment violation: "For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs." *Id.* at 2427 (citing *Herring,* 555 U.S. at 141, 129 S.Ct. 695, and *Leon,* 468 U.S. at 910, 104 S.Ct. 3405). Justice Alito, writing for the Court, elaborated:

> The basic insight of the *Leon* line of cases is that the deterrence benefits of exclusion vary with the culpability of the law enforcement conduct at issue. When the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs. But when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force and exclusion cannot pay its way.

Davis, 131 S.Ct. at 2427–28 (internal citations, quotation marks and brackets omitted).

The *Davis* Court also reviewed the line of "good faith exception" cases, starting with *Leon,* concluding that "in 27 years of practice under *Leon's* good-faith exception, we have 'never applied' the exclusionary rule to suppress evidence obtained as a result of nonculpable, innocent police conduct." *Id.* at 2429 (quoting *Herring,* 555 U.S. at 144, 129 S.Ct. 695.)

Indeed, the *Davis* Court focused on the issue of culpability as the decisive factor in the case before it:

> Under our exclusionary-rule precedents, this acknowledged absence of police culpability dooms Davis' claim. Police practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield "meaningfu[l]" deterrence, and culpable enough to be "worth the price paid by the justice system." *Herring,* 555 U.S. at 144, 129 S.Ct. 695. The conduct of the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> officers here was neither of these things. The officers who conducted the search did not violate Davis's Fourth Amendment rights deliberately, ***253** recklessly, or with gross negligence. *See* *ibid.* Nor does this case involve any "recurring or systemic negligence" on the part of law enforcement. *Ibid.*

Davis, 131 S.Ct. at 2428.

In order to properly apply *Leon,* *Herring*, and *Davis* here, we must focus on the culpability of the actors who committed the violations. The government mistakenly argues that we should focus on the conduct and "good faith" of PGCPD Detective Blazer, who, based on the cold hit, obtained the warrant for Davis' known DNA. It is true that nothing in the record suggests that Detective Blazer engaged in any culpable, or even negligent, conduct. He relied in good faith on the cold hit obtained and followed proper procedures in getting a search warrant based on it. There is nothing to suggest that his conduct was improper or that he had any obligation to look behind the cold hit match to see if there was some earlier constitutional violation.

But the deterrent effect of the exclusionary rule must be judged at the point of the constitutional violation, and the culpability of the actors involved then. The pertinent inquiry is whether we apply the exclusionary rule to keep similar violations from happening again; here, to prevent and deter the warrantless extraction of a victim's DNA from materials lawfully in police custody when he later becomes a suspect and then to deter that DNA profile from being retained. Thus, we look at the culpability of the police officers involved in those decisions, not at Detective Blazer.

As to the first violation, the extraction and testing of Davis' DNA in connection with the Neal murder, we find nothing in the conduct of the PGCPD officers that would warrant exclusion. As an initial matter, the PGCPD officers had no reason to question that Davis' blood was lawfully within HCPD custody and indeed, we have concluded that the clothing was properly in police custody.

Although we do not have detailed testimony before us as to the subjective motivations of the PGCPD officers who obtained the clothing and requested it be tested, the unique facts of this case reflect, at most, isolated negligence. What the officers did here was to obtain clothing that was lawfully in police custody and to test it for evidence. Significantly, the only reason they knew of the clothing's existence was because of Davis' *arrest* on drug charges when he left the hospital in Howard County. Had the clothing been obtained initially because of his arrest (like the other items on the property form), *Edwards* and *Wallace v. State,* 373 Md. 69, 816 A.2d 883 (2003), a Maryland Court of Appeals decision applying *Edwards,* likely would have permitted the testing. Thus, attributing culpability to the officers at this stage would be based on either: (1) their failure to learn, or recognize, that the clothing was in police custody because Davis was a victim, rather than an arrestee; or (2) assuming they did know the clothing had been seized from a crime victim, their failure to recognize that Davis' dual status as victim and arrestee might change the legal analysis set forth in *Edwards* and *Wallace.* This is simply not the type of "flagrant," or "intentional ... patently unconstitutional" conduct that warrants the application of the exclusionary rule. *See* *Herring,* 555 U.S. at 143–44, 129 S.Ct. 695. The conduct of PGCPD officers, in testing the blood contained on otherwise lawfully-seized clothing, does not constitute the type of "deliberate, reckless or grossly negligent" conduct that warrants exclusion. *See* *id.* at 144, 129 S.Ct. 695. As the *Herring* Court explained, "[a]n error that arises from nonrecurring and attenuated negligence is thus far removed ***254** from the core concerns that led us to adopt the rule in the first place." *Id.*

The dissent's mantra of "deliberate and intentional" police conduct at each step in the factual scenarios here, *see post* at 281, does not alter the facts as we have set them forth or the proper analysis to be applied to them. To be sure, the police took the steps that they did deliberately and intentionally in the sense that their actions were not accidental. But for the reasons we explain, one could insert "innocently" or "without knowledge of any constitutional violation," before each of those actions.

Likewise, as to any violation that occurred when the analyst entered Davis' DNA profile into the database after he was not a match in the Neal murder investigation, the record simply does not disclose anything that suggests that this action was anything other than an isolated, negligent incident at best. There is nothing, first of all, to show that the analyst here knew or should have known entering the data would violate the Fourth Amendment. Indeed, the many court decisions (including this Court's decision in *Jones*), that

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

have considered challenges to the use of DNA evidence have uniformly upheld statutes and other laws allowing the collection and testing of DNA evidence.

Additionally, while the paperwork accompanying Davis' clothing indicated that it came from a victim's clothing (J.A. 164, Supp. J.A. 76), it is not at all clear that the analyst actually knew anything other than that the evidence came from a "suspect in a shooting." (Supp. J.A. 93.) Similar to *Leon* and *Herring,* where officers relied on records from others in law enforcement, the PGCPD officers were relying on the fact that the HCPD had lawfully obtained the evidence. Indeed, while we rejected the government's broad construction of *Edwards* based on the fact that Davis was a victim when police seized his clothing, courts have repeatedly held, in broad terms, that evidence lawfully seized by one police agency may be given to another, even for a different purpose and even for additional testing. [30]

So, while we have determined for purposes of this opinion that *Edwards* did not allow the testing because Davis, as a victim, retained an objectively reasonable expectation of privacy in his DNA, that does not mean that the PGCPD officers and DNA analyst were not acting in a good faith belief that they had authority to do ***255** that testing under *Edwards* and similar cases.

Additionally, there is no evidence before this Court that the retention of a DNA profile in circumstances like that of Davis, is a systemic or recurring problem. The dissent disagrees, relying heavily on what it describes as an "admission" of the government at oral argument that the constitutionally violative conduct here was "clearly systemic." *See post* at 279. In our view, that reliance is misplaced. At oral argument, in response to questioning, counsel for the government briefly set forth the basic PGCPD policy or practice that the analyst was following. [31] Specifically, counsel explained that if a piece of evidence was analyzed for DNA evidence and a DNA profile was obtained from it, or if a DNA profile was obtained from a "known sample," then those DNA profiles were uploaded into the local CODIS database.

From this, our dissenting colleague assumes that evidence tainted by antecedent constitutional violations would also be uploaded to the database. But while it is possible to imagine, given the policy as articulated, that DNA evidence obtained by an illegal search or pursuant to an illegal arrest might end up in CODIS, there is no testimony before us as to whether that actually happened in any other instance. Indeed, defense counsel conceded at oral argument that the evidentiary record before this Court does not contain a single other example of a person's DNA being placed into the PGCPD local CODIS database without a proper constitutional basis. Any conclusion to that effect is purely speculative.

Moreover, as we have repeatedly made clear, our finding of a constitutional violation in this case was based on the specific and unusual facts of this case. Here, the police properly seized a piece of evidence from a victim in one crime, but then unconstitutionally used DNA evidence extracted from that evidence in investigating an unrelated crime in which the original victim was a suspect. They did so without consent from the victim and without obtaining a warrant, and thus we have found a violation. But a change in any one of those facts might have rendered the inclusion of Davis' DNA in CODIS constitutionally permissible. For example, had the clothing been taken from Davis as part of an inventory search at the time of his arrest for the present crime, as was the clothing in *Edwards,* rather than seized from him when he was a victim of a different crime, the result likely would have been different. Similarly, had the police obtained a search warrant to extract Davis' DNA from his pants and test it in conjunction with the Neal murder, the result likely would have been different. [32] So, the mere fact that other victims' DNA might be present in the database does not mean there were other constitutional violations.

Likewise, there is no evidence before us that the analyst acted with knowledge that ***256** she should not retain the profile. [33] Like the conduct at issue in *Herring* and in *Davis,* then, the conduct here stands in stark contrast to the cases in which the exclusionary rule has been applied, described by the *Herring* Court as "patently unconstitutional" conduct. *See* *Herring,* 555 U.S. at 143, 129 S.Ct. 695. Moreover, given the evolving and unsettled law governing DNA searches and seizures (as amplified by the district court's lengthy decision in this case, the briefs on appeal, and the lack of controlling Fourth Circuit or Supreme Court precedent), the conduct of the officers entering and retaining Davis' DNA profile can hardly be characterized as brazen or reckless.

We also note that Congress and the Maryland legislature, through their imposition of fines and criminal penalties for

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

failures to comply with their respective DNA statutes, already provide a deterrent effect against similar and future potential misuses of DNA information. Md.Code Ann. Pub. Safety § 2–512 (providing penalties for persons who misuse, disclose, or fail to destroy certain DNA records as required by the Maryland Act); 42 U.S.C. §§ 14135e(c), 14132(c) (same as to federal DNA act). This factor, too, militates in favor of judicial restraint in exercising the remedy of suppression, which exacts a "costly toll upon truth-seeking and law enforcement objectives." *Cf. Herring,* 555 U.S. at 141, 129 S.Ct. 695 (citation omitted); *see also Osborne,* 557 U.S. 52, 129 S.Ct. at 2312 (describing the response of the federal government and the states in regulating DNA testing as "prompt and considered").

In short, the obtaining and testing of Davis' DNA from his bloody clothing, and the subsequent inclusion of his DNA profile in the database were, at best, "isolated negligence attenuated from the arrest" [for the Schwindler murder]. *See Herring,* 555 U.S. at 137, 129 S.Ct. 695. We have no proof before us showing that victims' DNA profiles or individuals cleared of suspicion in an investigation are routinely entered into the local database by PGCPD, or have been entered into the database in any other instance. There is nothing in the record to suggest that the acts here are likely to reoccur. Moreover, the particularly unusual facts of this case—where a victim, with a dual status as an arrestee, later becomes a suspect in an unrelated crime, and there is DNA evidence available as a result of the crime in which the person was a victim—diminish further the likelihood of reoccurrence. The price to society of application of the exclusionary rule here, especially since the DNA evidence against Davis was compelling, would be to allow a person convicted of a deliberate murder to go free. The deterrent effect, if any, would be minimal, especially considering the lack of culpable conduct on the part of the police. Exclusion, therefore, would not "pay its way." *See Davis,* 131 S.Ct. at 2428. [34]

***257** For the foregoing reasons, the good faith exception to the exclusionary rule applies and we affirm the district court's denial of Davis' motion to suppress.

V.

[17] **[18]** Davis' second and final contention is that the district court erred in excluding the testimony of his proffered expert, Dr. Jeffrey Neuschatz. We review a district court's evidentiary rulings, including rulings on the admissibility of expert testimony, for abuse of discretion. *Gen. Elec. Co. v. Joiner,* 522 U.S. 136, 141–42, 118 S.Ct. 512, 139 L.Ed.2d 508 (1997); *United States v. Barsanti,* 943 F.2d 428, 432 (4th Cir.1991) (decision whether to admit expert testimony "will not be reversed absent a clear abuse of discretion"). We have reviewed the pertinent portions of the record on this issue and find no abuse of discretion with regard to this evidentiary ruling.

At trial, in addition to the DNA evidence and other evidence concerning the offenses, there was one witness, Laverda Jessamy, who identified Davis as being one of the robbers at the scene of the bank robbery and Schwindler shooting. She had done so both from a photographic array and in person at trial. In response to this identification, Davis sought to introduce the testimony of Dr. Jeffrey Neuschatz as an expert in eyewitness identifications. According to his expert witness report, Dr. Neuschatz intended to testify that the lineup procedure used with Ms. Jessamy did not meet the good practices guidelines of the American Psychology–Law Society and to testify concerning a number of factors which might result in a misidentification.

The government moved to exclude this evidence, contending that much of the proffered testimony consisted of common sense factors within the jury's understanding and not requiring expert testimony. After a hearing, the district court granted the government's motion to exclude Dr. Neuschatz's testimony on the grounds that it would not assist the jury. The court also explained that the testimony was not admissible under Fed.R.Evid. 403. In particular, the district court concluded that the probative value of the testimony was low because there was significant other evidence of guilt other than the eyewitness testimony and it was not a case where the government was relying, either exclusively or primarily, on eyewitness testimony. Thus, the danger of unfair prejudice, confusing of the issues or misleading the jury heavily outweighed the probative value of the testimony.

We have reviewed Dr. Neuschatz's report and his testimony at the *Daubert* hearing, and find that the district court did not abuse its discretion in concluding that the proffered evidence was not "scientific knowledge" that would be of benefit to the jury. This is consistent with our prior decision in *United States v. Harris,* 995 F.2d 532 (4th Cir.1993). In *Harris,* we recognized the "trend in recent years to allow such

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

testimony under [narrow] circumstances," but nonetheless concluded that "jurors using common sense and their faculties of observation can judge the credibility of an eyewitness identification, especially since deficiencies or inconsistencies in an eyewitness's testimony can be brought out with skillful cross-examination." *Id.* at 534–35.

The district court also did not abuse its discretion when concluding that, even if it qualified as a proper subject of expert testimony, the probative value of the testimony, which was low, was outweighed by the danger of prejudice or confusing the jury. Accordingly, it was not an abuse of discretion to exclude the evidence on Rule 403 grounds.

***258** Finally, we also agree with the government that, even if the testimony was wrongfully excluded, it was at most, harmless error. Most of the points that would have been made by Dr. Neuschatz were made by Davis' counsel on cross-examination. The compelling DNA evidence against Davis, as well as the evidence of unexplained cash purchases by him and his girlfriend in the days following the robbery were overwhelming evidence of guilt. The detailed jury instruction given by the court, moreover, further recognized and correctly advised the jury as to the legal issues concerning eyewitness identifications. In light of all these factors, we find no abuse of discretion by the district court in excluding the witness.

VI.

For the foregoing reasons, the judgment of the district court is

AFFIRMED.

DAVIS, Circuit Judge, dissenting:

There is much in the majority's thoughtful and thorough opinion with which I agree. Alas, however, "I feel constrained by a sense of duty to express my nonconcurrence in the action of the court in this present case." *Twining v. New Jersey,* 211 U.S. 78, 114, 29 S.Ct. 14, 53 L.Ed. 97 (1908) (Harlan, J., dissenting). I part company from the majority on two issues: (1) its application of the plain view exception to justify the seizure of the bag containing Davis's clothing from the hospital and the subsequent search of that bag and (2) its refusal to apply the exclusionary rule. [1] I conclude for the reasons explained herein that the seizure of the bag was unlawful and, even assuming the seizure could somehow be justified, the subsequent *search* of the bag effected a distinct violation of Davis's constitutionally protected privacy interests. Furthermore, I conclude that the majority's creation of a free-standing, ad hoc exception to the exclusionary rule is unwise and unsupported by the facts of this case, extant Supreme Court precedents, or our own precedents. Thus, I would vacate the judgment, reverse the denial of Davis's motion to suppress, and remand this case for further proceedings, as appropriate. [2]

***259** I.

A.

On August 29, 2000, Davis was treated at Howard County (Maryland) General Hospital for a gunshot wound to his right thigh. Davis told hospital staff that he had been shot in the course of a robbery. As required by state law, hospital personnel notified the Howard County Police Department ("HCPD") that it was treating a gunshot victim. *See* Md.Code Ann., Health–Gen. § 20–703. Detective Joseph King of the HCPD, then a uniformed patrol officer, was the first to respond to the hospital; King spoke with Davis concerning the circumstances of the shooting. Detective King testified at the suppression hearing that the hospital had been on his beat for approximately two years, and that he had responded on previous occasions to individuals with gunshot wounds. When he arrived at the hospital, he located Davis in the emergency room on a bed or gurney. According to Detective King, Davis presented him with a District of Columbia driver's license that showed his photograph and the name "Gary Edmonds."

Detective King observed Davis's gunshot wound. He then seized a bag containing Davis's pants and boxer shorts, which had been removed by hospital personnel, placed in the bag, and stored on a shelf beneath the bed. Detective King testified that he considered the clothing to be evidence of the crime reported, i.e., Davis's shooting. Detective King did not receive assistance from hospital personnel in retrieving the bag, which he testified was similar to other occasions on which he had responded to the hospital to investigate shootings. Detective King did not seek or obtain Davis's consent to take the bag or otherwise discuss the matter with Davis. He assumed Davis was aware that he was taking the bag because Davis observed him take possession

of it. Detective King described Davis's attitude towards questioning as "uncooperative." J.A. 143.

A short time later, Lieutenant Steven Lampe appeared at the hospital. Lieutenant Lampe took the bag from Detective King and later submitted it to the HCPD property room to be held as evidence. Lieutenant Lampe testified that the clothing was in a plastic bag when he took it from Detective King, but he could not recall what the bag looked like. Lieutenant Lampe did not inspect the clothing right away. Consistent with Detective King's testimony, he stated that Davis was not forthcoming in response to questioning, gave only vague information about the shooting, and was not interested in reporting the crime. After speaking with Davis, the police attempted to confirm his identity through various computer inquiries and found no history of a "Gary Edmonds."

Because the officers believed that Davis was being untruthful in his report of how he was shot, in part due to his lack of cooperation, the officers located the vehicle in which Davis's friend had driven him to the hospital, observed what appeared to be blood on the front passenger seat, and requested a K–9 officer to have his dog scan the car. The dog positively alerted to the presence of a controlled dangerous substance ("CDS"), and the car was searched. The police recovered a small amount of marijuana in the vehicle and accordingly arrested Davis and took him into custody upon his release from the hospital later that day. Lieutenant Lampe testified that the hospital staff had given Davis something to wear, Davis's clothing having been seized by Detective King. The police subsequently identified Davis by his fingerprints as "Earl Davis," and he admitted his true identity. Davis was charged with possession of marijuana and possession ***260** of CDS paraphernalia, but the charges were later dismissed.

The investigation into Davis's shooting concluded without an arrest, and the case was considered closed as of November 7, 2000. To that point, no forensic testing had been conducted on the bloody clothing seized from Davis at the hospital. Davis was not contacted or otherwise advised that the shooting investigation was closed.

Several months later, in June 2001, an individual named Michael Neal was murdered in nearby Prince George's County, Maryland. At some point in the ensuing three years detectives in the Prince George's County Police Department ("PGCPD") came to suspect Davis of having committed the murder. In the course of investigating the Neal murder, in April 2004 members of the PGCPD contacted Lieutenant Lampe to inquire about Davis's arrest at Howard County General Hospital in 2000. The PGCPD officers specifically asked whether any property had been seized from Davis that might contain his DNA. Lieutenant Lampe understood from this inquiry that Davis was now a suspect in a homicide. Later that month, two PGCPD homicide detectives who were familiar with the facts of the Neal murder went to the HCPD to pick up Davis's clothing for the purpose of DNA testing. Lieutenant Lampe delivered the clothing to the PGCPD detectives on April 29, 2004. On the property form for the clothing, Davis was clearly identified as a "victim." J.A. 164. Davis was not notified that the PGCPD had obtained his clothing. The PGCPD detectives submitted Davis's clothing to their DNA lab in connection with their investigation of the Neal murder.

Shortly thereafter, in or around June 2004, Davis's DNA was extracted from the blood stains on his boxer shorts, his profile was created, and the profile was compared to an unknown DNA profile derived from evidence obtained at the scene of the Neal homicide. The profiles did not match, and Davis was therefore excluded as the source of the evidentiary sample from the Neal murder. Davis's DNA profile was then entered into the local Prince George's County Combined DNA Index System ("CODIS") database. His DNA profile was never expunged or otherwise removed from the database.

B.

On August 6, 2004, shortly before 1:00 p.m., Jason Schwindler, an armored car employee, picked up a bank deposit from a local business and took it to a nearby BB & T bank in Hyattsville, Maryland, located in Prince George's County. As Schwindler walked up to the bank entrance, two gunmen exited a Jeep Cherokee and shot Schwindler, killing him. When their escape in the Jeep was thwarted by the armored truck driver, the assailants carjacked a bank customer and fled in her Pontiac Grand Am. The carjacked vehicle was later recovered.

After Schwindler's murder, officers from the PGCPD responded to the crime scene and collected evidence. Numerous items were recovered, including a baseball cap worn by one of the shooters, two firearms, and steering wheel covers from the Jeep Cherokee and the Pontiac Grand Am, the vehicles the shooters had driven to and away from the crime scene, respectively. These items were swabbed and analyzed for DNA. The DNA profiles of the major contributor to the

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

DNA found in the ballcap and on the trigger and grip of the recovered firearms were entered into the Prince George's County CODIS database. As a result of a search of the local database, on or about August 14, 2004, there was a "cold hit" between the DNA profile derived from material found on the baseball ***261** cap recovered at the crime scene and Davis's DNA profile in the database.

Law enforcement officers were notified of the match and, based on the cold hit, they promptly sought, and a state judge issued, warrants authorizing them to obtain DNA from Davis and to search the home of his girlfriend, Dana Holmes. Pursuant to the search warrant, a DNA sample was taken from Davis and his DNA profile was compared to the profiles derived from the DNA deposited on items recovered from the crime scene. The DNA analyst concluded that, to a reasonable degree of scientific certainty, Davis was the source of the DNA recovered from three pieces of evidence related to the Schwindler murder: (1) the steering wheel cover of the stolen Jeep Cherokee the assailants drove to the bank; (2) a baseball cap dropped by one of the assailants during the course of the robbery; and (3) the steering wheel cover of the Pontiac Grand Am in which the assailants fled the scene.

C.

On March 31, 2008, a federal grand jury returned a superseding indictment charging Davis with one count of Hobbs Act robbery, in violation of 18 U.S.C. § 1959; two counts of possession and discharge of a firearm in furtherance of a crime of violence, in violation of 18 U.S.C. § 924(c); one count of possession and discharge of a firearm resulting in death (murder), in violation of 18 U.S.C. § 924(j); one count of carjacking, in violation of 18 U.S.C. § 2119; and one count of felon in possession of a firearm, in violation of 18 U.S.C. § 922(g). Davis pleaded not guilty and proceeded to trial.

Prior to trial, Davis moved to suppress all direct and derivative evidence obtained from the warrantless seizure of his clothing at Howard County General Hospital, including his DNA profile. The district court denied Davis's motion to suppress after holding an evidentiary hearing and, following the conclusion of trial, filed a thoughtful opinion accepting some of Davis's arguments and rejecting others, but ultimately reaffirming its earlier denial of the motion to suppress. *United States v. Davis,* 657 F.Supp.2d 630 (D.Md.2009).

The DNA evidence presented at trial consisted of the PGCPD analyst's finding that Davis's DNA profile matched the DNA profile derived from the evidence recovered from the scene of the Schwindler murder to a reasonable degree of scientific certainty. Davis challenged the validity of the analyst's findings. In particular, he questioned whether the amount of DNA recovered from the crime scene was sufficient to produce accurate results and whether the government's statistical probability calculations (i.e., the statistics supporting the conclusion that Davis was the source of the DNA on each of the three items recovered from the crime scene) were reliable and accurate.

Davis's trial began on May 5, 2009, and lasted approximately five weeks. At the conclusion of the trial on June 3, 2009, the jury returned a guilty verdict on all counts. The district court sentenced Davis to a term of life imprisonment plus 420 months. Davis timely appealed the district court's denial of his motion to suppress and grant of the government's motion to exclude expert testimony.

II.

As the majority explains, Davis argues the district court committed reversible error in denying his motion to suppress DNA evidence. He contends that the following separate Fourth Amendment violations led to the "cold hit" match that implicated him in the Schwindler murder.[3] ***262** First, Davis argues that the initial nonconsensual, warrantless seizure of the bag of clothing from Howard County General Hospital by the HCPD in 2000 violated his Fourth Amendment rights. Second, he contends that the related, subsequent nonconsensual, warrantless search of the bag was unlawful, rendering all further uses of the evidence derived therefrom inadmissible as "fruit of the poisonous tree." Third, he asserts that PGCPD officials violated the Fourth Amendment when they extracted and chemically analyzed a sample of his DNA from the clothing without consent or a warrant in 2004. Fourth, Davis contends that the nonconsensual, warrantless uploading and retention of his DNA profile in the local CODIS database constituted yet a further Fourth Amendment violation. Of these four alleged violations, the district court found that only the retention of Davis's DNA profile in the CODIS database

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

constituted a Fourth Amendment violation, although it ultimately concluded that applying the exclusionary rule was not appropriate on the basis of the good-faith exception.

The majority agrees with the district court's analysis in significant part. In particular, the majority agrees that the warrantless seizure of the bag containing Davis's clothing, as well as the subsequent, distinct search of the bag, and the subsequent seizure of the contents of that bag, resulting in the extraction of Davis's biological material, all may be justified on the basis of the plain view seizure exception to the warrant clause of the Fourth Amendment. I respectfully dissent from that extraordinary holding. The plain view exception does not apply under the circumstances in this case. Furthermore, even if it could be applied in some plausibly recognizable manner, the plain view seizure doctrine could not possibly justify the separate search of the bag containing Davis's clothing. Accordingly, the majority's substantive Fourth Amendment analysis is fatally flawed, quite apart from its unwarranted refusal to apply the exclusionary rule.

A.

As the district court correctly observed, *Davis,* 657 F.Supp.2d at 636, the government bears the burden of proving, by a preponderance, the legality of the search and seizure of evidence obtained without a warrant (or evidence derived therefrom) which it intends to introduce at trial. *See* *Welsh v. Wisconsin,* 466 U.S. 740, 749–50, 104 S.Ct. 2091, 80 L.Ed.2d 732 (1984) (exigent circumstances); *United States v. Mendenhall,* 446 U.S. 544, 557, 100 S.Ct. 1870, 64 L.Ed.2d 497 (1980) (consent); *United States v. Matlock,* 415 U.S. 164, 177 n. 14, 94 S.Ct. 988, 39 L.Ed.2d 242 (1974) (same); *cf.* *Illinois v. McArthur,* 531 U.S. 326, 338, 121 S.Ct. 946, 148 L.Ed.2d 838 (2001) (Souter, J., concurring) ("[M]ost states follow the rule which is utilized in the federal courts: if the search or seizure was pursuant to a warrant, the ***263** defendant has the burden of proof; but if the police acted without a warrant the burden of proof is on the prosecution.") (quoting 5 W. LaFave, Search and Seizure § 11.2(b), p. 38 (3d ed.1996)). In assessing a trial court's ruling on a motion to suppress, we review factual findings for clear error and legal determinations, including "determination[s] of whether the historical facts satisfy a constitutional standard," de novo. *United States v. Gwinn,* 219 F.3d 326, 331 (4th Cir.2000); *see also* *Ornelas v. United States,* 517 U.S. 690, 699, 116 S.Ct. 1657, 134 L.Ed.2d 911 (1996); *United States v. Wilson,* 484 F.3d 267, 280 (4th Cir.2007). When a motion to suppress has been denied in the court below, we review the evidence in the light most favorable to the government. *United States v. Seidman,* 156 F.3d 542, 547 (4th Cir.1998).

B.

The HCPD's original nonconsensual, warrantless procurement of Davis's bloody boxer shorts and pants in 2000 requires that we decide whether the district court erred in its legal conclusion that Detective King was entitled to both seize the bag containing the clothing and to search its contents without consent and in the absence of a judicial warrant. Echoing the district court's analysis, the majority concludes that Detective King was justified in seizing the bag because he had "lawful access" to it and because it was "immediately apparent" to him, and would have been so to any reasonable officer in his position, that the bag contained Davis's pants and that the pants contained a bullet hole, i.e., evidence of a crime. Maj. Op. at 235–37. The majority further elaborates its unique reconception of the longstanding plain view seizure doctrine by concluding that King was justified in searching the bag's contents, without obtaining Davis's consent or a warrant, because it was a "foregone conclusion" that the bag contained evidence of a crime. Maj. Op. at 235, 236–37 (relying upon *Williams,* 41 F.3d 192).

The majority's analysis is deeply flawed. As I explain in subsection II.B.1, application of rudimentary and long-established Fourth Amendment principles demonstrates that Detective King's seizure of the bag from Davis's possession violated Davis's Fourth Amendment right to be free of an unreasonable seizure of his personal "effects" and cannot be shoehorned into a plain view seizure analysis. Furthermore, as I show more specifically in subsections II.B.2 and II.B.3, long-settled understandings of the plain view seizure doctrine demonstrate that under no reasonable interpretation of the facts found by the district court can it be said that the nonconsensual, warrantless search of the bag was justified under that doctrine. As I demonstrate, neither *Williams,* nor any other precedent cited to us by the government supports, let alone compels, the remarkable application of the plain view seizure doctrine engaged in by the majority.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

1.

It is common ground among the panel that a well-established exception to the Fourth Amendment's warrant requirement provides that a law enforcement officer may seize evidence in "plain view" without a warrant where (1) the officer is lawfully located in a place from which the item can plainly be seen; (2) the officer has a lawful right of access to the item itself; and (3) the incriminating nature of the seized item is immediately apparent. *See* *Horton v. California,* 496 U.S. 128, 136–37, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990). As this test makes clear, the intrusions implicated by the first two prongs of the test must be *lawful.* In other words, in both viewing the item to be seized and in actually taking ***264** physical possession of it, police must not infringe constitutionally protected privacy or possessory interests in the absence of a warrant or other well-recognized exception to the warrant requirement. *See* *Texas v. Brown,* 460 U.S. 730, 738–39, 103 S.Ct. 1535, 75 L.Ed.2d 502 (opining that "plain view" should not be considered an independent exception to the warrant requirement, but rather an extension of a prior justification for an officer's "access to an object") (plurality opinion); *see also* *Horton,* 496 U.S. at 137 n. 7, 110 S.Ct. 2301 (explaining that the lawful right of access requirement is "simply a corollary of the familiar principle ... that no amount of probable cause can justify a warrantless search or seizure absent 'exigent circumstances' ") (quoting *Coolidge v. New Hampshire,* 403 U.S. 443, 468, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971) (plurality opinion)).

In addition, the item's incriminating nature must be "immediately apparent" at the time the police view it, meaning that there is a "practical, nontechnical probability that incriminating evidence is involved." *Brown,* 460 U.S. at 742, 103 S.Ct. 1535 (internal quotation marks omitted); *see also* *Minnesota v. Dickerson,* 508 U.S. 366, 375, 113 S.Ct. 2130, 124 L.Ed.2d 334 (1993) ("If ... the police lack probable cause to believe that an object in plain view is contraband without conducting some further search of the object—i.e., if its incriminating character is not immediately apparent, *Horton,* 496 U.S. at 136, 110 S.Ct. 2301—the plain-view doctrine cannot justify its seizure.") (internal quotation marks and brackets omitted); *Soldal v. Cook County, Illinois,* 506 U.S. 56, 66, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992) (explaining that " 'plain view' seizures ... can be justified only if they meet the probable-cause standard").

The government has failed to meet its burden here to establish that the seizure of the bag containing Davis's clothing can be justified by application of the plain view seizure doctrine, and the subsequent search of the bag could never be justified by the plain view seizure doctrine in any event, no matter how much evidence the government could muster.

There is no dispute that Detective King was lawfully present in the emergency room where Davis was being treated, and thus viewed the bag from a lawful vantage point. There is a constitutionally cognizable distinction, however, between the emergency room generally and the more narrowly delineated area beneath Davis's bed where the bag had been stored. Thus, the majority fails (or simply refuses) to recognize that although this case does not involve the paradigmatic factual scenario in which police view an item through a window before entering a premises to retrieve it, *see* Maj. Op. at 233–34, the lawful vantage point and lawful access prongs do not necessarily rise and fall together. Rather, there are distinct possessory and privacy interests implicated by the facts before us, namely the specific location of the bag and the fact that it contained non-contraband personalty or, to use the constitutional parlance, Davis's constitutionally protected "effects."

As a matter of law, Davis never relinquished his possessory rights in his effects prior to their seizure. *See* *United States v. Neely,* 345 F.3d 366, 369 & n. 4 (5th Cir.2003) ("[A]n emergency room patient does not forfeit his possessory rights to clothing simply by walking (or in many cases being carried) through the hospital door.") (collecting cases). Howard County General Hospital personnel ensured that Davis's clothing was in his *immediate personal possession and control* when they placed it in a bag on the shelf directly ***265** beneath his bed. *See* *People v. Yaniak,* 190 Misc.2d 84, 738 N.Y.S.2d 492, 495–96 (N.Y.Co.Ct.2001) ("[T]he placing of the garments in the green plastic bag by hospital personnel evinced an objective belief that the items were still the personal property of the defendant and that, when he felt better, they would be returned to him.").

Of course, Davis would have retained his possessory interest in the clothing (and thus the bag containing the clothing), as well as his residual privacy interest in his clothing, [4] even if the hospital had safeguarded it in some other location. *See*

Neely, 345 F.3d at 370 (explaining that once clothing is taken from the patient and secured by hospital employees, the hospital becomes a bailee and employees have no authority to permit police to retrieve the clothing without a warrant) (citation omitted). In addition, there is no evidence that Davis abandoned his clothing or that he consented to the seizure. Accordingly, under the circumstances, the police no more had "lawful access" to the bag containing Davis's clothing as he lay in the hospital receiving treatment than they would have had if the bag had been locked in a cabinet for patients' belongings or, indeed, held in Davis's hands while he was being treated. [5]

Manifestly, an officer's physical access to a citizen's non-contraband personalty in the possession of the citizen is not equivalent to an officer's "lawful access" to that personalty under the plain view doctrine. In other words, the mere existence of ***266** probable cause to believe a container in the possession of a citizen holds evidence of criminal activity, where the evidence is not contraband, is not alone sufficient to effect a warrantless seizure of that container from the possession of the citizen. [6]

As Davis correctly argues, and as the district court acknowledged, "A warrantless seizure is 'per se unreasonable under the Fourth Amendment subject only to a few specifically established and well-delineated exceptions' to the warrant requirement. *Katz v. United States,* 389 U.S. 347, 357, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (footnotes omitted); *Flippo v. West Virginia,* 528 U.S. 11, 13–14, 120 S.Ct. 7, 145 L.Ed.2d 16 (1999) (same)." Appellant's Br. at 21; *see Davis,* 657 F.Supp.2d at 636. The plain view seizure doctrine does not supplant the need for such an exception where an officer intrudes upon constitutionally protected privacy or possessory interests in physically retrieving the item to be seized from the person of its owner. *See Horton,* 496 U.S. at 137, 110 S.Ct. 2301 ("[N]ot only must the officer be lawfully located in a place from which the object can be plainly seen, but he or she must also have a lawful right of access to the object itself."); *Jones v. State,* 648 So.2d 669, 678 (Fla.1994) (explaining that the lawful access requirement "ensures that the scope of the intrusion into Fourth Amendment rights is no greater than that already authorized in connection with the lawful entry"); *see also infra* pp. 275–76 (explaining why seizures of containers holding "mere evidence" are distinguishable from containers holding contraband). Accordingly, in the absence of a recognized justification (e.g., exigent circumstances, which the district court did not find applicable) for intrusion upon Davis's protected interests, Detective King could not lawfully seize the bag under the plain view seizure doctrine from Davis's possession without a warrant or consent, irrespective of whether it was "immediately apparent" that the clothing suspected of being contained ***267** therein constituted evidence of a crime. [7] As the government accurately describes the relevant circumstances, "the [bag containing the] clothing was readily accessible to Detective King," Govt's Br. at 33–34, but that most assuredly does not mean that Detective King had "lawful access" to the bag or the clothing contained therein under the plain view seizure doctrine.

2.

Of course, even if Detective King could conceivably, on some theory, lawfully seize the bag, that does not mean that he could inspect its contents, i.e., search the bag, without obtaining Davis's consent or a judicial warrant. [8] "Even when government agents may lawfully seize such a package to prevent loss or destruction of suspected contraband [or mere evidence], the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package," *United States v. Jacobsen,* 466 U.S. 109, 114, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984) (brackets added), or otherwise satisfy one of the exceptions to the warrant requirement. *Horton,* 496 U.S. at 141 n. 11, 110 S.Ct. 2301. In other words, as Judge Niemeyer (who, three years earlier, ***268** had been a member of the panel in *Williams*) has cogently explained, "The 'plain-view' doctrine provides an exception to the warrant requirement for the *seizure* of property, but it does not provide an exception for a search." *United States v. Jackson,* 131 F.3d 1105, 1108 (4th Cir.1997) (emphasis in original); *accord United States v. Rumley,* 588 F.3d 202, 205 (4th Cir.2009).

Only in a very limited subset of cases involving "closed, opaque container[s]" may an officer open the container without first obtaining a warrant or the owner's consent, *Robbins v. California,* 453 U.S. 420, 426, 101 S.Ct. 2841, 69 L.Ed.2d 744 (1981) (plurality opinion), at least where, as here, the container is not located in a vehicle. One exception

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

to the search warrant requirement in this context is in cases involving exigency. *See* *Chadwick,* 433 U.S. at 15 n. 9, 97 S.Ct. 2476 ("Of course, there may be other justifications for a warrantless search of luggage taken from a suspect at the time of his arrest; for example, if officers have reason to believe that luggage contains some immediately dangerous instrumentality, such as explosives, it would be foolhardy to transport it to the station house without opening the luggage and disarming the weapon."). [9] Another exception, the one the district court and the majority erroneously rely on, is for "containers (for example a kit of burglar tools or a gun case) [that] by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance." *Sanders,* 442 U.S. at 764 n. 13, 99 S.Ct. 2586. In those cases, because "the distinctive configuration of [the] container proclaims its contents," the owner of the container has no reasonable expectation of privacy in those contents, *Robbins,* 453 U.S. at 427, 101 S.Ct. 2841 (plurality opinion)—and thus an officer's observation of those contents does not constitute a separate "search" for Fourth Amendment purposes. *See* *Illinois v. Andreas,* 463 U.S. 765, 771, 103 S.Ct. 3319, 77 L.Ed.2d 1003 (1983) ("If the inspection by police does not intrude upon a legitimate expectation of privacy, there is no 'search'...."). In such cases the shape and/or character of the container, including where relevant its labeling, even if closed and opaque, is constitutionally equivalent to one that is open or transparent, because it "clearly reveal[s] its contents." *Id.; see also* *Arizona v. Hicks,* 480 U.S. 321, 328, 107 S.Ct. 1149, 94 L.Ed.2d 347 (1987) ("[A] truly cursory inspection—one that involves merely looking at what is already exposed to view, without disturbing it—is not a 'search' for Fourth Amendment purposes, and therefore does not even require reasonable suspicion."); *United States v. Payne,* 181 F.3d 781, 787 n. 4 (6th Cir.1999) ("There is no such thing as a 'plain-view search.' "). [10]

***269** We have carefully limited the scope of this "proclaims its contents" exception to cases where the incriminating nature of the contents is a "foregone conclusion." *See* *Williams,* 41 F.3d at 192; *see also* *Sanders,* 442 U.S. at 764 n. 13, 99 S.Ct. 2586 (requiring that the container's owner not maintain "*any* reasonable expectation of privacy" in the contents) (emphasis added). [11] Indeed in *United States v. Corral,* 970 F.2d 719 (10th Cir.1992), on which *Williams* principally relied, the court found that no search occurred only because there was a "virtual certainty" that the package contained, in that case, cocaine. *Id.* at 726 (quoting *Brown,* 460 U.S. at 751 n. 5, 103 S.Ct. 1535 (Stevens, J., concurring in the judgment)). The obviousness of a container's contents must be such that an officer's view of the container is "*equivalent* to the plain view" of the incriminating contents themselves. *Id.* (emphasis added). [12] The analogy we used ***270** in *Williams* illustrates both the centrality to the plain view seizure doctrine of the character of the container and the high degree of certainty required: "[W]hen a person opens a Hershey bar, it is a foregone conclusion that there is chocolate inside." 41 F.3d at 198; *see also* *Brown,* 460 U.S. at 750–51, 103 S.Ct. 1535 (Stevens, J., concurring in the judgment) (concurring in the application of the exception because the container there—a knotted party balloon located in a car close to several small plastic vials, quantities of loose white powder, and an open bag of party balloons—was "one of those rare single-purpose containers which 'by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance' "). Only if the character of a closed, opaque container proclaims its incriminating contents to such a degree do we excuse officers from obtaining a search warrant to open the container, assuming the officer has lawfully come into possession of the container. [13]

The above principles reflect the longstanding interplay between the two separate interests at stake: citizens' interest in retaining possession of their property and their interest in maintaining personal privacy. These two interests roughly correspond to seizures and searches, respectively, as "[a] seizure threatens the former, a search the latter." *Brown,* 460 U.S. at 747, 103 S.Ct. 1535 (Stevens, J., concurring in the judgment). This distinction, in turn, informs the plain view seizure doctrine in this context. As Justice Stevens has explained,

> As a matter of timing, a seizure is usually preceded by a search, but when a container is involved the converse is often true. Significantly, the two protected interests are not always present to the same extent;

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> for example, the seizure of a locked suitcase does not necessarily compromise the secrecy of its contents, and the search of a stopped vehicle does not necessarily deprive its owner of possession.

Id. at 747–48, 103 S.Ct. 1535.

Apart from the special concerns arising from seizures of containers, we allow police officers to seize incriminating *objects* in ***271** plain view with a showing only of probable cause because the seizure "threatens only the interest in possession;" such objects "can be seized without compromising any interest in privacy." *Id.* at 748, 103 S.Ct. 1535. "[I]f an officer has probable cause to believe that a publicly situated item is associated with criminal activity" the owner's interest in possession is "diminish[ed]," and becomes "outweighed by the risk that such an item might disappear or be put to its intended use before a warrant could be obtained," and the object may be seized without a warrant. *Id.* (citing *G.M. Leasing Corp. v. United States,* 429 U.S. 338, 354, 97 S.Ct. 619, 50 L.Ed.2d 530 (1977); *Payton v. New York,* 445 U.S. 573, 587, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980)).

Where there is a "link" between the seizure and "a prior or subsequent search," however, there is a "danger ... that officers will enlarge a specific authorization, furnished by a warrant or an exigency, into the equivalent of a general warrant to rummage and seize at will." *Id.* Averting that danger requires not only that the officer have probable cause to connect the item with criminal behavior, but also that the seizure "entail[s] no significant additional invasion of privacy." *Id.* This danger is particularly acute where, as here, "an officer comes upon a container in plain view and wants both to seize it and to examine its contents." *Id.* at 749, 103 S.Ct. 1535. The Court has "emphasiz[ed] the Fourth Amendment privacy values implicated whenever a container is opened." *Id.*

In light of these controlling principles, the dispositive issues bearing on the applicability of the plain view seizure doctrine before the district court were fairly straightforward. Given the above concerns, the issues can be easily framed: Could the government justify Detective King's nonconsensual, warrantless seizure of the bag, a closed, opaque container, on the one hand? Relatedly (but distinctly), did King's immediate opening of such a container constitute a "non-search" (because it does not invade its owner's reasonable expectation of privacy) or, instead, an impermissible warrantless search, on the other hand? Although the district court and the majority of the panel conclude that our *Williams* precedent provides easy answers to those questions, upon a close view of the facts in *Williams* and in light the precedents discussed above, it is clear that the majority's reliance on that case is wholly misplaced.

In *Williams,* an airline employee conducted a private search of the defendant's luggage and found several cellophane-wrapped packages that, according to her, "looked like dope." 41 F.3d at 198. She alerted police officers, who seized the packages and then removed some of the content, conducting a chemical field test that revealed that the packages contained cocaine. *Id.* at 194. The seizure was proper under the plain view doctrine, we concluded, because not only did the officers have lawful access to the packages; there was "no doubt" of the packages' "incriminating nature": "the packages were wrapped in heavy cellophane with a brown opaque material inside, and were found with towels, dirty blankets and a shirt in an otherwise empty suitcase." *Id.* at 196–97. In fact, the seizing officer later testified that "in his ten years of experience such packages *always* contained narcotics." *Id.* at 197 (emphasis added).

We then turned to whether the police needed a warrant to remove any of the contents of the packages. To justify the warrantless search, we explained, the government must not only show there was probable cause the container contained evidence ***272** of a crime, but rather that, based on characteristics of the container itself and "the circumstances under which an officer [found] the container," the contents' incriminating nature was "a foregone conclusion." *Id.* at 197 (citing *Blair,* 665 F.2d at 507). We concluded that "the incriminating nature of the five packages found in Williams' suitcase was a foregone conclusion," given

WESTLAW © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> (1) the manner in which the cocaine was packaged (apparently weighing approximately one kilogram each, heavily wrapped in cellophane with a brown opaque material inside); (2) Detective Finkel's firm belief, based on his ten years' experience, that packages appearing in this manner always contained narcotics; (3) [the airline employee's] belief that the packages contained narcotics; and (4) that the only items found in Williams' suitcase besides the five packages of cocaine were towels, dirty blankets, and a shirt with a cigarette burn.

Id. at 198. Because the presence of illegal narcotics in the packages was a foregone conclusion, Williams had no reasonable expectation of privacy in those contents. Accordingly, under the venerable Katz principle, *see* *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring), the officers' observation of those contents did not constitute a "search," and thus "a search warrant was unnecessary." *Williams,* 41 F.3d at 198; *See* *Jackson,* 131 F.3d at 1108 (reaffirming that no "search" occurs when the plain view seizure doctrine properly applies to the contents of an opaque container).

Simply put, despite the majority's labored efforts to the contrary, this case is not *Williams* or *Corral.* Most important, under a proper plain view seizure analysis, it cannot be said that a reasonable officer in King's position had "knowledge approaching certainty," *Corral,* 970 F.2d at 725, that the bag under Davis's hospital bed contained evidence of a felonious shooting in which Davis was a "victim." [14] The district court and the majority treat the bag of Davis's clothing as analogous to the cellophane-wrapped cocaine in *Williams. See* Maj. Op. at 236 (holding that "the totality of the circumstances ... support[s] the determination that it was a foregone conclusion the bag under Davis' hospital bed contained the clothing he wore when he was shot," and that the clothing was evidence of a crime). I disagree.

As a matter of law, based on what was known by the officers after they attempted to interview Davis at the hospital, the likelihood that the bag contained probative evidence of a felonious shooting in which Davis was a victim does not rise to the level of probable cause. In the first place, there is unwarranted confidence shown by the district court and the majority that Davis's pants would contain a bullet hole. *See id.* at 236–37 ("We have little trouble, however, in concluding that Davis' pants would contain a bullet hole, and would thus be incriminating evidence in the prosecution of his assailant. Such a conclusion is based on the circumstances, Davis' appearance, and the location of his bullet wound."). The facts of *United States v. Jamison,* 509 F.3d 623 (4th Cir.2007), illustrate why this confidence is misplaced.

***273** The defendant in *Jamison* was a felon who accidentally shot himself in the groin area with a gun he had been carrying in his waistband. 509 F.3d at 625. Like Davis here, when Jamison was transported by his associates to the hospital for treatment, he relayed to investigating officers a fanciful falsehood that he was the victim of an attempted robbery. *Id.* at 626. The investigating officer noticed Jamison's clothing on a chair in the treatment room and confirmed by the absence of a bullet hole in Jamison's pants that Jamison was lying about the circumstances surrounding how he was shot. [15] *Id.* It was far from "a foregone conclusion" that, apart from the likely presence of blood on Davis's clothing, the contents of the bag would serve as useful evidence in the prosecution of an illusory "shooter" about whom Davis would provide no information. Indeed, the photograph in the record of Davis's high-thigh wound depicts a wound that is entirely consistent with one that would be suffered from an accidental discharge of a weapon by someone carrying a firearm in his waistband.

Equally important, there can be scant doubt that, in view of Davis's refusal to cooperate with the officers who responded to the hospital to investigate, the HCPD officers fairly quickly turned their attention to Davis as a suspect in criminal activity, just as Jamison quickly became a suspect in his own shooting. Indeed, even the government contends on appeal (contrary to the majority's facile attempt to show that in seizing Davis's personal property the Howard County police were seeking to "protect" Davis), that the police appropriately deemed Davis to be "not an innocent crime victim." Govt's Br. at 46–47 n. 13. *But see* *Davis,* 657 F.Supp.2d at 640 ("Davis was positively the victim of a violent crime.").

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

The actions of the officers in searching the car in which Davis was transported to the hospital and in eventually arresting Davis and his friend bear out this highly likely scenario. Indeed, the facts of this case show that because Davis used a falsely made District of Columbia driver's license bearing his photograph under the alias "Gary Edmonds," the only way in which the HCPD could reliably identify Davis was to arrest him and take his fingerprints. That is exactly what they were determined to do and that is exactly what they did. In short, even the investigating officers did not believe Davis was a victim; rather, they were investigating his possible involvement in criminal activity. Thus, rather than accept uncritically the officers' post hoc rationalization that they needed Davis's clothing to prosecute the unknown person who allegedly shot him, under the circumstances of this case, "[w]e should be reiterating the usual exhortation: 'Get a ***274** warrant.' " *United States v. Norman,* 701 F.2d 295, 302 (4th Cir.) (Murnaghan, J., concurring), *cert. denied,* 464 U.S. 820, 104 S.Ct. 82, 78 L.Ed.2d 92 (1983). [16]

As should thus be apparent, the "incriminating" nature of the contents of the bag here was nowhere close to being so obvious that no "search" occurred—unlike in *Williams.* In *Williams,* the drug packaging at issue was so readily recognizable that even a lay person, the airline employee who originally opened the baggage, testified that she immediately reported her discovery because "the bags looked like dope." *See* 41 F.3d at 198 (noting that "[b]ecause Lee is a layperson, not trained in law enforcement, her belief that the five packages contained 'dope' strongly supports the district court's conclusion that the contents of the packages were a foregone conclusion"). The hearing testimony in this case did not indicate that the bag was distinctive in any way; thus, the government did not satisfy its burden on that issue. Indeed, the district court noted that "[t]here was no testimony as to whether the bag was open or closed, or whether it was transparent, opaque, or somewhere in-between." *Davis,* 657 F.Supp.2d at 638. Neither Detective King nor Lieutenant Lampe was able to provide a description of the bag beyond Lieutenant Lampe's comment that it was probably plastic.

Moreover, the *Williams* court emphasized Detective Finkel's testimony that, based on his ten years of experience in narcotics enforcement, packages of the sort at issue "*always* " contain narcotics. 41 F.3d at 198 (emphasis in original).

In this case, Detective King testified on cross-examination that "the hospital makes a practice to secure any property that they take. Clothing from a victim, they place it under their bed." J.A. 147. When asked the follow up question, "So you're familiar it's the hospital's practice to secure that clothing in a white opaque plastic bag; is that correct?," Detective King responded, "It's been in different things. Sometimes it all depends on if somebody bags it or not." *Id.* In addition, as stated *supra,* neither Detective King nor Lieutenant Lampe was able to describe the bag. Detective King's testimony clearly does not ***275** rise to the level of familiarity or certainty expressed by Detective Finkel in *Williams.* Manifestly, it does not rise to Justice Stevens's "virtually certain" metric. The government's evidence of the nature of the bag and the surrounding circumstances was equivocal at best, and clearly did not rise to the level of virtual certainty that the bag would contain contraband, which the government would have to show to establish that no "search" of the bag's contents occurred.

Williams is also inapposite on its facts in two additional meaningful respects, such that the case does not support, let alone dictate, the result reached by the majority. First, the *Williams* court, in language and reasoning that was wholly unnecessary to the outcome of its analysis, considered not only the extrinsic evidence of the contents of the packages, but *also* the physical appearance and character of the packages to bolster its conclusion, whereas the district court in this case considered *only* extrinsic evidence. Considering only extrinsic evidence, and not the physical appearance and character of the container itself, takes the "foregone conclusion" analysis too far from the origins of the plain view seizure container exception acknowledged in *Sanders* footnote 13, in which the Supreme Court provided the quintessential examples of a single-purpose container, namely "a kit of burglar tools or a gun case." 442 U.S. at 764 n. 13, 99 S.Ct. 2586. The *Sanders* Court noted that the contents of such containers "can be inferred from their outward appearance." *Id.* Narcotics packaging is so readily recognizable as to rise to the level of the archetypal kit of burglar tools or a gun case. A non-descript plastic bag does not so betray its contents. [17]

Second, and critically, the search in *Williams* was a search for contraband and not mere evidence of someone's criminal

act.[18] For the reasons expressed above, *see supra* pp. 264–65, in addition to his possessory interest in the bag and its contents, Davis clearly enjoyed a reasonable expectation of privacy in his own clothing and their contents every bit as much as he enjoyed a reasonable expectation of privacy, as the majority rightly holds, in the ***276** chemical facts concerning his biological material and blood.[19] Indeed, it is curious, to say the least, to reason as does the majority that Davis retained, for several years after the bag was seized at the hospital, a reasonable expectation of privacy in the character of his DNA molecules, but that he lacked any reasonable expectation of privacy in the presence of those molecules in his blood while they were embedded in his clothing and hidden from the government in a bag which was effectively in his actual possession at the hospital. Thus, I would limit *Williams* and its reliance on extrinsic indicia of the container's contents to cases involving the plain view seizure of containers holding contraband.

For all these reasons, *Williams* does not control the outcome in this case.[20]

C.

For the foregoing reasons, unlike the majority, I would hold, at minimum, that not only the extraction of Davis's DNA, the creation of his DNA profile and its retention in the local DNA database violated Davis's constitutional right to be free from unreasonable searches, but that the nonconsensual, warrantless search of the bag containing his personal effects likewise violated that right. Accordingly, I respectfully dissent from the majority's contrary resolution of the merits of the Fourth Amendment issue. "[T]he value of the Fourth Amendment derives from the consideration that only when it is applied evenhandedly—to smugglers, murderers, and rapists as well as to others—does it retain its effectiveness for the decent citizenry." *Norman,* 701 F.2d 295 at 302 ***277** (Murnaghan, J., concurring). I regret the majority's distortion of the plain view doctrine in order to save the unconstitutional search challenged in this case.

III.

The majority, having concluded that only the extraction and analysis of Davis's DNA by the PGCPD violated the Fourth Amendment, and having assumed that the retention of his DNA in the local CODIS database was a further violation, nevertheless refuses to apply the exclusionary rule. I respectfully dissent from that choice. I would find that the district court erred in admitting evidence flowing from the HCPD's unlawful seizure and search of Davis's clothing and the PGCPD's unlawful extraction, analysis and retention of his DNA profile, including in particular the evidence of the match between the known sample obtained pursuant to the search warrant and DNA recovered from the scene of the Schwindler murder. Because this case does not fall within any version of the "good faith" exception recognized under extant Supreme Court or Fourth Circuit precedent, I would reject the district court's decision not to apply the exclusionary rule.

The Fourth Amendment protects the fundamental "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," U.S. Const. amend. IV, but "contains no provision expressly precluding the use of evidence obtained in violation of its commands," *Arizona v. Evans,* 514 U.S. 1, 10, 115 S.Ct. 1185, 131 L.Ed.2d 34 (1995). Thus, the Supreme Court created the exclusionary rule, an auxiliary to the Amendment which "compel[s] respect for the constitutional guaranty," *Elkins v. United States,* 364 U.S. 206, 217, 80 S.Ct. 1437, 4 L.Ed.2d 1669 (1960), by forbidding the use of illegally obtained evidence at trial. *See* *Weeks v. United States,* 232 U.S. 383, 34 S.Ct. 341, 58 L.Ed. 652 (1914) (adopting federal exclusionary rule); *Mapp v. Ohio,* 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961) (applying exclusionary rule to the states through the Fourteenth Amendment). Suppression is not an automatic consequence of all Fourth Amendment violations, however. *See* *Herring v. United States,* 555 U.S. 135, 137, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009).

The Supreme Court created the "good-faith" exception to the exclusionary rule in *United States v. Leon,* 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). In *Leon,* the Court held that the exclusionary rule does not apply when the police conduct a search in "objectively reasonable reliance" on a warrant later held invalid. *Id.* at 922, 104 S.Ct. 3405; *see also* *Massachusetts v. Sheppard,* 468 U.S. 981, 990–91, 104 S.Ct. 3424, 82 L.Ed.2d 737 (1984) (companion case declining to apply exclusionary rule where

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

warrant held invalid as a result of judge's clerical error). In the twenty-eight years since deciding *Leon,* a sharply-divided Supreme Court has applied variations on the *Leon* good-faith exception in several specific circumstances. In *Illinois v. Krull,* 480 U.S. 340, 107 S.Ct. 1160, 94 L.Ed.2d 364 (1987), the Court applied the good-faith exception to a search conducted in reasonable reliance on a subsequently invalidated statute. *Id.* at 349–50, 107 S.Ct. 1160. In *Evans,* 514 U.S. 1, 115 S.Ct. 1185, the Court applied the good-faith exception where police reasonably relied on erroneous information concerning an arrest warrant in a database maintained by non-law enforcement, judicial employees. *Id.* at 6, 14–16, 115 S.Ct. 1185.

More recently, in *Herring,* decided approximately nine months prior to the district court's decision in this case, the Supreme Court addressed a question left ***278** unresolved by *Evans,* namely "whether the evidence should be suppressed if police personnel were responsible for the error." 555 U.S. at 142–43, 129 S.Ct. 695 (quoting *Evans,* 514 U.S. at 16 n. 5, 115 S.Ct. 1185) (internal quotation marks omitted). Considering whether the exclusionary rule applies where police failed to update records in a warrant database, leading to the unlawful arrest of the defendant on the basis of a recalled warrant, the *Herring* Court held, over a spirited dissent, that where "the error was the result of isolated negligence attenuated from the arrest ... the jury should not be barred from considering all the evidence." *Id.* at 137–38, 129 S.Ct. 695. The Court reasoned that, "when police mistakes are the result of negligence ..., rather than systemic error or reckless disregard of constitutional requirements, any marginal deterrence does not pay its way." *Id.* at 147–48, 129 S.Ct. 695 (internal quotation marks omitted). Most recently, the Court in *Davis v. United States,* —— U.S. ——, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011), applied a further variation on the *Leon* good-faith exception where police conducted a search in objectively reasonable reliance upon binding judicial precedent that was later overruled. *Id.* at 2423–24.

The majority reasons that, "[i]n order to properly apply *Leon,* *Herring*, and *Davis* here, we must focus on the culpability of the actors who committed the violations." Maj. Op. at 253. The majority assumes without discussion that *Leon* and its progeny govern here, and thus proceeds directly to the broad cost-benefit analysis that underlies the narrow holdings in those cases. As discussed *infra,* however, each of the cases upon which the majority relies is clearly distinguishable from the case at bar. Thus, the majority's application of the good-faith exception to preclude suppression in this case marks a departure from the Supreme Court's exclusionary rule precedents and represents a new, free-standing exception never sanctioned by the Court or by precedent in this Circuit.

In *Leon,* *Krull,* *Evans* and *Davis,* the Supreme Court reasoned that exclusion does not serve to deter unconstitutional police conduct where the actor primarily responsible for the Fourth Amendment violation is not a law enforcement officer. *See* *Leon,* 468 U.S. 897, 104 S.Ct. 3405 (magistrate judge); *Krull,* 480 U.S. 340, 107 S.Ct. 1160 (legislators); *Evans,* 514 U.S. 1, 115 S.Ct. 1185 (clerk in the employ of the judiciary); *Davis,* 131 S.Ct. 2419 (judiciary). This rationale clearly does not apply here, where HCPD and PGCPD employees violated the Fourth Amendment. In this respect, our case is most like *Herring,* which also dealt with unconstitutional conduct by law enforcement personnel. Nevertheless, *Herring* is likewise inapplicable because it crafted a narrow exception to the exclusionary rule that applies only where "the error was the result of isolated negligence attenuated from arrest." 555 U.S. at 137, 129 S.Ct. 695. The majority fails to recognize that neither of the qualifiers present in *Herring,* namely "isolated negligence" and "attenuation," is present here.

Instead, the record in our case shows unmistakably that the constitutionally violative conduct is not only deliberate and intentional but is systemic; most assuredly, it was not an isolated blunder. Detective King testified that, as on previous occasions when he has responded to Howard County General Hospital to investigate shootings, hospital personnel did not assist him in obtaining Davis's effects. This statement indicates that Detective King has seized patients' belongings in the manner at issue here on other occasions. *See supra* n. 11. In addition, the DNA analyst ***279** who entered Davis's profile into the local CODIS database testified that she was

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

aware that Davis had been cleared of suspicion in the Neal murder before his DNA profile was added to the local CODIS database.

Furthermore, the "Request for Examination" form submitted to the PGCPD Serology DNA Laboratory ("DNA Lab") along with Davis's bloody clothing indicated that "these samples are from a shooting the suspect was a victim of in Howard Co. MD." Supp. J.A. 76. The DNA analyst testified that the database contained profiles of both suspects and victims, indicating that the PGCPD regularly retained the DNA profiles of persons, such as Davis, who had not been arrested, charged with, or convicted of any crime. The government confirmed at oral argument that it was the PGCPD's policy to upload *every* DNA profile it analyzed into the local CODIS database, regardless of the individual's status, the method by which the sample was obtained, or whether the sample might be tainted by an antecedent constitutional violation. Oral Arg. Tr. at 28:40. Thus, the record indicates that the PGCPD analyst and officers knew that Davis was a victim at the time the sample was collected, that Davis was not a suspect when his DNA profile was entered into the local database, and that it was the PGCPD's policy and practice to retain the DNA profiles of such persons. Thus, by the government's own admission, the constitutionally violative conduct was clearly systemic. *See* *Hudson v. Michigan,* 547 U.S. 586, 604, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006) (Kennedy, J., concurring in part and concurring in the judgment) (opining that, "[i]f a widespread pattern of violations were shown, and particularly if those violations were committed against persons who lacked the means or voice to mount an effective protest, there would be reason for grave concern").

The expungement provisions in the Maryland and federal indexing statutes also recognize a privacy interest for those in Davis's position. As the district court recognized, "[b]oth laws require that an individual's DNA record be expunged from the database if the defendant is never convicted, his conviction is reversed or vacated, or the charges are dismissed." *Davis,* 657 F.Supp.2d at 659 (citing 42 U.S.C. §§ 14132(d)(1)(A)(i)-(ii); 42 U.S.C. §§ 14132(d)(2)(A)(i)-(ii); Md.Code Ann., Pub. Safety § 2–511). While "[t]he expungement provisions do not directly apply to Davis' situation because they are drafted specifically to address circumstances in which an individual's DNA was placed in the database on the basis of a conviction or arrest," I agree with the district court that "the construction of the statute strongly suggests that Congress and the Maryland legislature respected the privacy interest of those individuals never convicted for qualifying offenses, and did not intend for ordinary citizens' or victims' DNA to be included in the database." *Id.*

In addition, unlike the constitutionally violative conduct at issue in *Herring,* the conduct in this case is not "attenuated" from the discovery of Davis's identity as the source of the DNA recovered from the scene of the Schwindler murder; the cold hit which led to Davis's arrest was a *direct result* of the seizure and search of his clothing and the subsequent extraction, analysis and retention of his DNA profile. *Cf.* *Hudson,* 547 U.S. at 592, 126 S.Ct. 2159 (exclusionary rule inapplicable where violation of the knock and announce rule was not but-for cause of obtaining evidence pursuant to search warrant). Given that the cold hit supplied the sole probable cause for the search warrant leading to the known DNA match, the causal connection required to invoke the exclusionary rule is clearly present in this case.

***280** As we recognized in *United States v. Oscar–Torres,* 507 F.3d 224 (4th Cir.2007), application of the exclusionary rule is the "usual remedy" where evidence of identity is derived from unlawful searches and seizures:

> Indisputably, suppression of evidence obtained during illegal police conduct provides the usual remedy for Fourth Amendment violations. *See* *Mapp v. Ohio,* 367 U.S. 643, 655, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961). Courts will also suppress evidence that is the indirect product of the illegal police activity as "fruit of the poisonous tree." *See* *Wong Sun v. United States,* 371 U.S. 471, 488, 83 S.Ct. 407, 9 L.Ed.2d 441 (1963). Of course, not all evidence that "would not have come to light but for the illegal actions of the police" is suppressible as fruit of the poisonous tree. *Id.* Rather, the critical inquiry is "whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint." *Id.* (internal quotation marks omitted).

Id. at 227. There is no real dispute that the seizure of the bag containing Davis's clothing, the search of the bag and of Davis's clothing, including the extraction of his

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

DNA therefrom, and the subsequent creation and uploading of his DNA profile, means that the identification evidence introduced at trial was the product of an "exploitation" of the searches and seizures at issue in this case.[21] Rather than noting the critical distinctions between our case and extant good-faith exception precedents, the majority invents an ad hoc version of the exception by focusing on broad principles espoused by the *Herring* Court, including most notably its admonition that the deterrent effect of exclusion must outweigh its costs. This is unsurprising, perhaps, given that the *Herring* Court's " 'analysis' ... far outruns the holding." Wayne R. LaFave, *The Smell of Herring: A Critique of the Supreme Court's Latest Assault on the Exclusionary Rule,* 99 J.Crim. L. & Criminology 757, 770 (2009). In other words, there is a gap between the holding of *Herring,* which is quite narrow, and its rationale, which sweeps quite broadly. We should not so readily depart from the narrow holding of *Herring,* and the Supreme Court's other good-faith exception jurisprudence, given the critical role that the exclusionary rule plays in ensuring the vitality of the Fourth Amendment.

The rule provides an essential "incentive for the law enforcement profession as a whole to conduct themselves in accord with the Fourth Amendment," *Illinois v. Gates,* 462 U.S. 213, 221, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983) (White, J., concurring in judgment), thereby "safeguard[ing] Fourth Amendment rights generally through its deterrent effect," *United States v. Calandra,* 414 U.S. 338, 348, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974). *See also Herring,* 555 U.S. at 152, 129 S.Ct. 695 (Ginsburg, J., dissenting) (describing exclusionary rule as a "remedy necessary to ***281** ensure that the Fourth Amendment's prohibitions are observed in fact") (internal quotation marks omitted); *cf. United States v. Jones,* 678 F.3d 293 (4th Cir.2012).[22]

In this case, the HCPD officers deliberately and intentionally dispossessed Davis of his personal property. The HCPD officers then deliberately and intentionally retained that property. Then, the HCPD deliberately and intentionally delivered that property to the PGCPD officers, who deliberately and intentionally made a request for it. Having thus obtained possession, the PGCPD officers then deliberately and intentionally delivered Davis's property to their DNA lab for analysis and uploading into the local CODIS database, and, of course, the analyst, charged with knowledge that she was handling biological material taken from a crime victim, deliberately and intentionally uploaded the DNA profile into the database. This case is a poor candidate for the creation of a new variation on the good-faith exception to the exclusionary rule.

Davis has been convicted of a heinous crime. The cold-blooded mid-day murder of Jason Schwindler, a man simply conscientiously going about his work to support himself and his family, understandably generates outrage and dismay, an all-too-common episode of modern life from which all decent people recoil in horror. There is little reason to doubt that customary, equally conscientious, work by dedicated state and federal law enforcement officers would have brought deserved justice to those who participated. Nevertheless, duty to the judicial oath requires that we apply the law faithfully and evenhandedly.[23]

In short, I would apply the exclusionary rule in this case and leave it to the Supreme Court to extend the good-faith exception to the particular situation now before us, should it see fit to do so. I am mindful that the obituary marking the long slow death of the exclusionary rule has been written long before the rule will be interred.[24] Understandably, perhaps, there has been no want of volunteers among the judiciary to serve as pallbearers. I regret this development and fear that a measurable lessening in liberty will result from this freeing of law enforcement from the constraints of the Fourth Amendment through the invention of an ad hoc good-faith exception to suppression of unlawfully obtained evidence. To quote the second Justice Harlan, "I can see no good ***282** coming from this constitutional [mis]adventure." *Ker v. California,* 374 U.S. 23, 46, 83 S.Ct. 1623, 10 L.Ed.2d 726 (1963) (Harlan, J., concurring in the judgment).

For the reasons set forth, I respectfully dissent.

All Citations

690 F.3d 226

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Footnotes

1 Specifically, Davis was convicted of Hobbs Act robbery, in violation of 18 U.S.C. § 1951, two counts of possession and discharge of a firearm in furtherance of a crime of violence, in violation of 18 U.S.C. § 924(c), one count of possession and discharge of a firearm in furtherance of a crime of violence resulting in death, in violation of 18 U.S.C. § 924(j), and one count of carjacking, in violation of 18 U.S.C. § 2119.

2 CODIS is a linked system that allows local, state, and federal forensics laboratories the ability to exchange, share and compare DNA profiles electronically. *See United States v. Mitchell,* 652 F.3d 387, 399 (3d Cir.2011) (en banc).

3 The death penalty was originally sought in this case, but the district court held that Davis was ineligible for the death penalty because he meets the legal definition for mental retardation. That ruling is not challenged on appeal.

4 Although the parties and the district court sometimes referred to the two HCPD officers using their titles at the time of the suppression hearing, we use their titles in 2000, as described by them.

5 We use the term "DNA material" to refer to any physical body sample that contains deoxyribonucleic acid (DNA) identification information. *See* 42 U.S.C. § 14135a(c)(2) (defining DNA analysis for purposes of including DNA profiles in CODIS as the "analysis of [DNA] identification information in a bodily sample").

6 The parties are not clear in their briefs and do not point to any record evidence concerning what supported the PGCPD's suspicion that Davis was involved in the Neal murder. Nonetheless, we presume for purposes of this appeal that, whatever level of suspicion it was, it was insufficient to establish probable cause.

7 Davis was initially charged in Prince George's County Circuit Court and prosecution began there by the Prince George's County State's Attorney's Office. That office later dismissed the case against Davis in coordination with the U.S. Attorney's Office in favor of a federal prosecution. The testimony of the analyst before the Maryland court was attached as Exhibit H to the Government's Consolidated Response to Motions filed before the district court below.

8 Although not in evidence, there was a limited discussion at oral argument regarding what the common policy or practice was at that time. *See infra* at 254–55.

9 The accuracy of the DNA match is uncontested on appeal.

10 Before the district court, Davis' counsel argued six different points in which the Fourth Amendment could be implicated. On appeal, he limits his Fourth Amendment challenges to the three recited.

11 Relying on *United States v. Jackson,* 131 F.3d 1105, 1108 (4th Cir.1997), the dissent criticizes the majority opinion for its alleged failure to recognize that the plain view doctrine can justify a seizure, but not a warrantless search. *See generally post* at 267–69.

> We recognize and acknowledge, as explained in *Jackson,* that the plain view doctrine is not an exception to the warrant requirement for a Fourth Amendment search. 131 F.3d at 1108. Rather, the proper analysis is that there was a "non-search" here—for Fourth Amendment purposes—because no privacy interests were implicated. That is so because the police were justified in "searching" the bag of Davis' clothing because it was a foregone conclusion that the bag contained evidence of a crime; just as in

United States v. Williams, upon which we rely, the police lawfully searched a seized container because it was a foregone conclusion it contained evidence of a crime. 41 F.3d 192, 198 (4th Cir.1994). We describe the action of the police in either looking in the bag or cataloguing its contents as a "search," as that term is used in the non-technical sense, since that is the framework utilized by the parties, by the dissent, and by the court in *Williams. See id.* ("When a container has been legally seized, and its contents are a foregone conclusion, we hold that a subsequent search of the container is lawful under the plain view container doctrine."). To the extent there is an issue, it is more of labeling than of substance.

12 The government also contends that, even if the plain view exception did not apply, the clothing and DNA on it are not subject to exclusion because those items would have been discovered and seized upon Davis' arrest for narcotics violations as he left the hospital. The district court rejected this argument. *Davis,* 657 F.Supp.2d at 641. In light of our ruling that the plain view exception applies, we do not address the alternative argument of the government.

13 The dissent devotes considerable ink to disputing the lawful access prong, complete with hypotheticals unrelated to the situation in the case at bar. *See post* at 264–67 and corresponding notes. Context matters, however, and the context of this case is that of a police officer who was lawfully fulfilling his duty to investigate a reported shooting. In doing so, he lawfully entered the emergency room of a hospital to interview the victim of the shooting, and observed both the victim, unclothed from the waist down, lying on a gurney with a visible gunshot wound to his upper thigh, and a plastic bag of clothing underneath the victim's gurney. That context informs our conclusion that the officer had lawful access to the bag.

14 While the dissent appears to disagree with the holding of *Williams* in some respects, *see post* at 270 n. 13, 275, we are bound to follow our own Circuit's precedent "absent contrary law from an *en banc* decision of this Court or a Supreme Court decision." *United States v. Jeffery,* 631 F.3d 669, 677 (4th Cir.2011).

15 It is unsurprising that neither officer could remember, at the time of their testimony at the suppression hearing in September 2008, precisely what the plastic bag looked like given that they had seen it briefly more than eight years earlier, in August 2000.

16 Contrary to the dissent's unfounded claim that we are engaging in "extraordinary appellate fact-finding," *post* at 269 n. 12, we are simply quoting from the undisputed testimony of Officer King in the record. While the government bears the burden of proof to show that the warrantless seizure was justified, the district court ruled in the government's favor and thus any inferences to be drawn from the testimony are to be viewed in the light most favorable to the government. *Seidman,* 156 F.3d at 547. Moreover, nowhere in its brief does the government "concede" that King did not know it was clothing in the bag. *Cf. post* at 269 n. 12.

17 The dissent's lengthy discussion of *United States v. Jamison,* 509 F.3d 623 (4th Cir.2007), *see post* at 272–73 & n. 15, to suggest that a bullet hole might not have been present in Davis' pants, is unavailing. *Jamison* did not involve any challenge to the search or seizure of evidence; the issue there was whether the defendant was in custody for *Miranda* purposes at the time police questioned him. Moreover, the fact that it was theoretically possible, at the time that Officer King seized the clothing, that Davis was: a) lying about being shot by someone else and had instead shot himself; and b) done so in a manner that somehow avoided putting a hole in his own pants, does not alter our conclusion. As the Tenth Circuit has explained, the knowledge required to establish a "foregone conclusion" is not absolute certainty, but "knowledge *approaching* certainty." *United States v. Jackson,* 381 F.3d 984, 989 n. 2 (10th Cir.2004) (emphasis in original). That standard is met here.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

18 The Fifth Circuit reasoned in *Chavis* that "[c]learly, the officer ... would have been derelict in his duty had he not taken custody of Chavis' clothing as evidence of a possible homicide that he was investigating." 488 F.2d at 1078; *see also* *Jamison,* 509 F.3d at 631–32 (in context of addressing interrogation and gun-powder residue testing of a hospital patient who was admitted with a gunshot wound, noting that a reasonable person who is admitted to a hospital with a gunshot wound and reports that he was shot by someone else would expect to be interviewed and "might complain of police malfeasance had [the police] *not* immediately investigated the shooting[,] [since a] reasonable person would tolerate nothing less than a thorough investigation into such a shooting").

19 The dissent cites *Clay v. State,* 290 Ga. 822, 725 S.E.2d 260 (2012), as a case in which a court concluded the plain view exception did not warrant the search of a bag of clothing. *See post* at 274 n. 16. Contrary to the dissent's description of *Clay* as having "nearly identical" facts, however, the defendant in *Clay* was an unconscious murder *suspect* at the time the police reported to the hospital and conducted a search of the bag containing his personal effects. *See* 725 S.E.2d at 264–65. Significantly, there was no evidence in that case that the police knew there would be blood on his clothing or other evidence of any crime. Unlike Davis, the suspect had not been shot or assaulted and was not being treated for any wounds, nor were any wounds visible, that would indicate there would be blood on his clothing. *Id.* Under these circumstances, the court concluded that it was not a " 'foregone conclusion' that the bag contained [the suspect's] bloody clothes." *Id.* at 269. Here, by contrast, there was ample evidence in plain sight (including most notably the gunshot wound on Davis' upper thigh) from which Officer King could conclude it was a foregone conclusion that the bag contained Davis' clothing, and that the clothing contained evidence of a crime.

Moreover, while Davis and the dissent cite to decisions of other courts for the "unremarkable proposition" that hospital patients retain a reasonable expectation of privacy in their clothing, *see post* at 274 n. 16, that proposition is far from universally accepted. Indeed, other courts have found that a reasonable expectation of privacy was lacking under facts similar to those here and thus upheld the warrantless seizure and search of clothing belonging to a hospital patient. *See, e.g., Mitchell v. State,* 321 Ark. 570, 906 S.W.2d 307, 309 (1995) (affirming warrantless seizure of clothing from hospital and subsequent inventory search, explaining that "[t]he totality of the circumstances herein includes the fact that the appellant was thought to be a victim [and] [t]he clothing of a gunshot victim is evidence of the commission of a crime"); *Holt v. United States,* 675 A.2d 474, 477, 480 (D.C.1996) (Fourth Amendment was not violated by the search or the subsequent seizure of defendant's clothing from a "visible, unsealed plastic bag under [defendant's] gurney in which hospital personnel had stored [his] clothing before treating him" after defendant had admitted himself with a gunshot wound, particularly where he had "voluntarily walked into [the hospital] emergency room wearing —for everyone to see—the clothing the police later inspected" and he never expressed "a desire to remove [the clothing] from public view"); *People v. Sutherland,* 92 Ill.App.3d 338, 47 Ill.Dec. 954, 415 N.E.2d 1267, 1271 (1980) (gunshot victim whose clothes were removed at the hospital had no reasonable expectation of privacy in those clothes and thus they could be obtained and inspected without a warrant); *State v. Adams,* 224 N.J.Super. 669, 541 A.2d 262, 265 (N.J.Super.Ct.App.Div.1988) (exigent circumstances permitted the search and inspection of clothing taken from an unconscious hospital patient in the emergency room, who was believed to be the victim of a shooting); *Wagner v. Hedrick,* 181 W.Va. 482, 383 S.E.2d 286, 291 (1989) (motorcycle accident victim had no "reasonable expectation of privacy in his personal effects" under the control of emergency room staff).

20 Indeed, in gauging what is "readily recognizable," we think it likely that the vast majority of people who have spent time in a hospital (either as a patient or with a friend or family member) know that hospitals commonly

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

place a patient's clothing in a plastic bag that either stays in his room or travels with him on his bed or gurney. On the other hand, most lay people do not have personal experience with the types of packaging used by drug traffickers. Regardless of which container hypothetically is more recognizable in the absence of context and personal experience, we readily conclude that the bag here was readily identifiable as containing Davis' clothing.

21 Because DNA is found in many bodily substances, *see* *Kaemmerling v. Lappin,* 553 F.3d 669, 682 (D.C.Cir.2008) ("DNA exists in numerous parts of the body that even nonviolent criminals leave behind, including hair, saliva, and skin cells....") (citation omitted), the mere fact that DNA material is present on a physical item of seized evidence cannot automatically infringe upon a person's privacy interest in his or her DNA. It is not until the DNA is tested and extracted and a DNA profile created that the privacy interest in DNA might be implicated. Put differently, it cannot be the rule that an otherwise lawful seizure of physical evidence becomes illegal merely because a non-perpetrator's DNA may be on that evidence.

22 In *Jones,* in the context of obtaining DNA profiles from incarcerated felons, we analogized DNA profiling to fingerprinting, *i.e.,* a more sophisticated or refined means of identification. 962 F.2d at 306–07; *see also* *Mitchell,* 652 F.3d at 413 ("at present DNA profiling is simply a more precise method of ascertaining identity and is thus akin to fingerprinting, which has long been accepted as part of routine booking procedures"); *see also* *United States v. Amerson,* 483 F.3d 73, 85–86 (2d Cir.2007) ("at least in the current state of scientific knowledge, the DNA profile derived from the offender's blood sample establishes only a record of the offender's identity" and "a probationer's expectation of privacy in his or her identity is severely diminished."); *Boroian v. Mueller,* 616 F.3d 60, 66–67 (1st Cir.2010) ("Given the [federal] DNA Act's stringent limitations on the creation and use of DNA profiles, CODIS currently functions much like a traditional fingerprint database" and citing to cases from the Second, Tenth, and District of Columbia Circuits so stating). However, courts also have recognized the limitations of this analogy, which stem from the fact that a DNA profile, unlike a fingerprint, is drawn from DNA that stores a wealth of personal information. *See* *Johnson v. Quander,* 440 F.3d 489, 499 (D.C.Cir.2006) ("genetic fingerprints differ somewhat from their metacarpal brethren"); *United States v. Kincade,* 379 F.3d 813, 841–42 & n. 3 (9th Cir.2004) (en banc) (Gould, J., concurring) ("Like DNA, a fingerprint identifies a person, but unlike DNA, a fingerprint says nothing about the person's health, propensity for particular disease, race and gender characteristics, and perhaps even propensity for certain conduct.").

> In any event, both a thorough examination of the science of DNA profiling, as well as the operation and interplay of local, state, and federal DNA law enforcement databases, are far beyond the scope of this opinion. Other courts have examined these issues in detail and we will not do so here. *See, e.g.,* *Mitchell,* 652 F.3d at 398–402 (discussing the process of creating a DNA profile for CODIS and the use of "junk" DNA, the federal DNA act and the levels of database that contribute to CODIS); *Boroian,* 616 F.3d at 63–64, 65–67 (explaining how DNA samples are obtained, summarizing the provisions of the federal DNA act, and describing how CODIS works and how the database has grown and expanded since its initial development).

23 The Supreme Court's recent decision in *United States v. Jones,* —— U.S. ——, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) does not change our analysis in this case. In *Jones,* the Court held that the Fourth Amendment was violated when law enforcement officers, without a valid warrant, installed a GPS tracking device on the undercarriage of the defendant's Jeep while it was parked in a public parking lot. In determining whether this action constituted a "search," the majority did not reach the issue of whether the Defendant had a

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

"reasonable expectation of privacy" in the underbody of the Jeep. *Id.* at 950. Instead, its conclusion rested entirely on the fact that the "Government physically occupied private property for the purpose of obtaining information," *id.* at 949, and that constituted a violation of the Fourth Amendment right "to be secure against unreasonable searches and seizures in their persons, houses, papers and effects." *Id.* In so holding, the Court emphasized that *Katz* simply established that "property rights are not the sole measure of Fourth Amendment violations," but that *Katz* did not extinguish the "previously recognized protection for property." *Id.* at 951; *see also* *id.* at 954–55 (Sotomayor, J., concurring). In the case at bar, once the police had lawful possession of Davis' clothing, there was no further intrusion of, or trespass upon, his property rights. Thus, the only basis on which the later testing of the clothing could constitute a search is if Davis retained a reasonable expectation of privacy in his clothing or the blood on it.

24 The government also relies on *United States v. Gargotto,* 476 F.2d 1009 (6th Cir.1973) and *Wallace v. State,* 373 Md. 69, 816 A.2d 883 (2003). In *Gargotto,* the Sixth Circuit held that a defendant's records seized in a state investigation could be given to federal authorities without a separate search warrant, and used as evidence in an unrelated federal case. 476 F.2d at 1014. Similarly, *Wallace* affirmed the warrantless search and visual inspection of the defendant's clothing in conjunction with a murder charge, where the clothing had been initially seized during an inventory search upon his arrest for drug charges, because the defendant had no reasonable expectation of privacy in that clothing. 816 A.2d at 897, 901. The district court considered *Wallace* and other similar cases, but found them all distinguishable on the grounds that the evidence in the other cases lawfully entered police custody pursuant to a defendant's arrest or was seized pursuant to a warrant supported by probable cause. *Davis,* 657 F.Supp.2d at 646. By contrast, Davis' pants with the bloodstain were in lawful police custody as evidence of a crime in which he was the reported victim. *Id.* at 647.

25 The *Boroian* court relies on *Amerson* as a case supporting this principle. 616 F.3d at 68. However, a careful reading of *Amerson* reflects that the Second Circuit found a reasonable expectation of privacy in the retention of a DNA profile in CODIS, and periodic matching of the profile, *see* 483 F.3d at 85 n. 12, 86, but ultimately concluded that the search was justified under the special needs test. *Id.* at 86–87 (upholding the federal DNA Act against Fourth Amendment challenges and "acknowledg[ing] that the DNA profile of appellants will be stored in CODIS, and potentially used to identify them, long after their status as probationers —and the reduced expectation of privacy that such a status involves—has ended," but concluding that fact did not "change [ ] the ultimate analysis.")

26 Even in cases where a person is subject to some type of criminal charge or restraint, there are varying viewpoints regarding the proper approach and its application. In the Ninth Circuit's *Kincade* case, which was heard en banc, a five-member plurality voted to uphold the federal DNA Act against a Fourth Amendment challenge and employed a totality of the circumstances test. 379 F.3d at 832 (en banc) (O'Scannlain, J., plurality opinion). Judge Gould, concurring in the result, voted to uphold the Act, but would have applied the "special needs" analysis. *Id.* at 840 (Gould, J., concurring). Five dissenting judges would have found a Fourth Amendment violation, but would have employed different approaches. *See* *id.* at 842–76 (dissenting opinions); *see also* *id.* at 830–31 (O'Scannlain, J., plurality opinion) (collecting authority and comparing

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

cases which have applied a special needs test in the context of DNA profile collection and cases which have applied a "totality of the circumstances" balancing test); *Mitchell,* 652 F.3d at 403 n. 15 (noting that only the Second and Seventh Circuits have consistently held that the special needs test should apply in addressing the constitutionality of a DNA indexing statute and concluding that the totality of the circumstances is the proper test).

27 In an alternative argument as to why the retention of Davis' DNA profile does not constitute a separate search, the government contends that once the district court had determined there was no Fourth Amendment violation in the extraction and testing of Davis' DNA from his clothing as part of the Neal investigation, Davis no longer had any expectation of privacy in the DNA profile. (Appellee's Br. at 50–51 (citing *Johnson v. Quander,* 440 F.3d 489, 498–99 (D.C.Cir.2006) and state court opinions).)

28 Neither party argues for the application of the "special needs" test here. We also conclude it should not apply here because it applies in contexts "beyond the normal need for law enforcement," *Rendon,* 607 F.3d at 989, and only normal law enforcement interests are involved here.

29 Subsequent to briefing and argument in this case, the Maryland Court of Appeals upheld an as-applied constitutional challenge to a portion of the Maryland DNA Collection Act (enacted several years after the events in the case at bar) that authorizes the warrantless collection and uploading of certain arrestees' DNA into the Maryland DNA database. *See* *King v. State,* 425 Md. 550, 42 A.3d 549 (2012). (The mandate in *King,* however, has been stayed pending the Supreme Court's ruling on the state's petition for certiorari. *See,* *Maryland v. King,* ––U.S. ––––, –– S.Ct. ––––, –– L.Ed.2d ––––, 2012 WL 3064878 (July 30, 2012)). The *King* court, as we have, utilized a "totality of the circumstances" test to determine whether the search at issue was reasonable.

> We note, however, that the ultimate conclusion of the *King* Court does not alter our analysis. First, the case is factually distinguishable. Not only did it involve a portion of Maryland's DNA statute not in effect at the time of events in the case at bar, but it involved the taking of a DNA swab from an arrestee, rather than the creation of a DNA profile from a victim's DNA sample already lawfully in police possession. Second—and significantly—the *King* Court did not address at all the application of the good faith exception, nor is there any indication in the opinion that it was asked to do so.
>
> Since the question is not before us, we express no opinion on the *King* Court's conclusion, although we note that it is contrary to decisions by the Third and Ninth Circuits. *See, e.g., supra* at 245–46, 249–50 (citing *Haskell v. Harris,* 669 F.3d 1049, 1062 (9th Cir.2012), *reh'g en banc granted,* 686 F.3d 1121 (2012) and *United States v. Mitchell,* 652 F.3d 387, 407 (3d Cir.2011) (en banc), both of which upheld statutes requiring the collection of DNA from arrestees).

30 *See, e.g.,* *Wallace,* 816 A.2d at 896–97 (collecting cases); *Williams v. Commonwealth,* 259 Va. 377, 527 S.E.2d 131, 136 (2000) (holding that defendant had no expectation of privacy in boots that were seized incident to his arrest and thus that "later examination of the property by another law enforcement official [with a different department] does not violate the Fourth Amendment", even if being examined for a different charge than the charge for which he was arrested); *United States v. Turner,* 28 F.3d 981, 983 (9th Cir.1994) (removal of defendant's cap from jail by postal inspector without a warrant was proper since it remained in the possession of the police); *United States v. Thompson,* 837 F.2d 673, 674 (5th Cir.1988) ("A person lawfully arrested has no reasonable expectation of privacy with respect to property properly taken from his person for inventory by the police. Later examination of that property by another law-enforcement officer is, therefore, not

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

an unreasonable search within the meaning of the Fourth Amendment."); *United States v. Johnson,* 820 F.2d 1065, 1072 (9th Cir.1987) (money seized by state authorities upon defendant's arrest for driving under the influence could be later reviewed by a federal agent to obtain serial numbers in a robbery investigation without a warrant); *United States v. Jenkins,* 496 F.2d 57 (2d Cir.1974) (relying on *Edwards* to conclude there was no Fourth Amendment violation where a federal agent took "second look" and seized without a warrant money that had been taken from the defendant following his arrest on unrelated state charges and maintained in the jail safe).

31 Counsel prefaced her comments by referencing the policy at the time Davis' profile was uploaded. The record does not disclose whether that policy has changed in light of subsequent developments in the Maryland or federal DNA laws, or as a result of decisions like the district court's decision in the instant case, issued in 2009.

32 Because those are not the facts before us, we need not resolve the constitutionality of the DNA searches in those hypothetical cases. But those slight differences in fact might well alter our conclusions regarding the constitutionality of the police actions and the uploading of DNA profiles. Thus, the mere existence of the policy stated by counsel does not necessarily mean that the violation here was anything other than isolated.

33 While the analyst testified that she knew the state level database required deletion of a profile once a court had exonerated a person previously convicted, there is nothing in the record to support that she knew the profile of either a victim or a suspect was required to be destroyed in the circumstances here, nor has Davis pointed to any statute with such a requirement.

34 Contrary to the dissent's contention, we are not creating a "new, freestanding exception" to the exclusionary rule. *Post* at 278. Rather, we have faithfully applied the Supreme Court's precedent, including its recent application of *Leon* in *Herring* and *Davis.* While the dissent refers to the "narrow holding[s]" in those cases, and deems inapplicable the "broad cost-benefit analysis" that underlies those holdings, *post* at 278, 280, the Supreme Court's analysis in those cases is not dicta, but is the rationale supporting the Court's application of the good-faith exclusion.

1 The majority "assume[s], without deciding, that there was a separate Fourth Amendment violation in retaining Davis' DNA profile in the local CODIS database." Maj. Op. at 233. While it is not critical to my analysis in this case, I would likely hold that under circumstances such as those presented here, the state action involved in (1) extracting Davis's DNA from the biological material recovered from his clothing, (2) chemically analyzing that material to create a DNA profile, and (3) uploading the profile into the local DNA database essentially constitutes a single continuous course of constitutionally implicated endeavors subject to Fourth Amendment scrutiny. Governments undertake to engage in this full course of conduct inasmuch as the purpose of this extraordinary forensic science is to enable law enforcement to identify persons, and that cannot be achieved through less than the full protocol we have come to know. For present purposes, however, I join in the majority's assumption.

2 I would not reach the question whether the district court properly excluded the testimony of Dr. Jeffrey Neuschatz, Davis's proposed expert on eyewitness identifications. The district court excluded Dr. Neuschatz's testimony in significant part because it had previously decided to admit the DNA evidence, which meant that "the significance of eyewitness identification" in the case was "[not] high." J.A. 2323. Because I would reverse the district court's denial of Davis's motion to suppress the DNA evidence, that premise of the district court's decision would no longer apply, and in a retrial without that evidence the court might very well come to a different conclusion. Thus, I find it unnecessary to address the district court's grant of the government's motion to exclude Dr. Neuschatz's testimony.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

3 Although the majority, following the lead of the parties, purports to identify *three* alleged Fourth Amendment violations, as I explain within, a proper analysis of this case must distinguish as separate constitutionally cognizable invasions: (1) the seizure of the bag at the hospital followed by (2) the search of the bag. Indeed, as the majority's own analysis shows, *see* Maj. Op. at 235 ("As to both the seizure of the bag and the subsequent search of the bag, the district court's reliance on *United States v. Williams,* 41 F.3d 192 (4th Cir.1994) was appropriate."), the seizure and search of the bag are indeed distinct undertakings. Moreover, although Davis combined these two challenges in some ways, there is no question that he has challenged each distinct invasion of his rights. *See* Appellant's Br. at 17 ("First, the police illegally seized and searched the white bag containing Mr. Davis' clothes beneath his hospital bed when he came in as a shooting victim four years prior to the Schwindler robbery and shooting.").

4 Unlike the majority, it is difficult if not impossible for me to imagine that a person, even a hospital patient undergoing treatment in an emergency room as was Davis, lacks a reasonable expectation of privacy in his underwear which is concealed by hospital personnel in a bag and left within easy reach of the patient.

5 The very case relied on by the majority for its expansive application of the "lawful access" element of the plain view doctrine in response to this dissent makes clear that the typical plain view seizure case involves concern for protection of a citizen's spatial privacy, e.g., the lawfulness of an entry, not with the distinct constitutional question of whether a seizure of a constitutionally protected "effect" from the personal possession of its owner is "lawful." *See* Maj. Op. at 234 (contending that the "lawful right of access" requirement "is meant to guard against warrantless entry onto premises whenever contraband is viewed from off the premises in the absence of exigent circumstances"; thus, while "lawfully positioned" "refers to where the officer stands when she sees the item," "lawful right of access" refers "to where she must be to retrieve the item") (quoting *Boone v. Spurgess,* 385 F.3d 923, 928 (6th Cir.2004) (holding that disputed issue of fact precluded summary judgment for officers in plaintiff's Fourth Amendment claim under 42 U.S.C. § 1983 where plaintiff disputed officers' assertion that they could see handgun in his car while they were standing outside the vehicle, and thus permissibly entered vehicle to retrieve the firearm and then arrested plaintiff)).

Nor does the majority's invocation of *Washington v. Chrisman,* 455 U.S. 1, 102 S.Ct. 812, 70 L.Ed.2d 778 (1982), *see* Maj. Op. at 234, aid its cause. In that case, "the officer noticed seeds and a small pipe lying on a desk 8 to 10 feet from where he was standing [in the threshold of defendant's college dormitory room after having detained the defendant's roommate for underage possession of an alcoholic beverage]. From his training and experience, the officer believed the seeds were marihuana and the pipe was of a type used to smoke marihuana. He entered the room and examined the pipe and seeds, confirming that the seeds were marihuana and observing that the pipe smelled of marihuana." 455 U.S. at 4, 102 S.Ct. 812. Chrisman's expectation of privacy *in his room* gave way to the officer's duty to keep in close contact with the roommate, whom the officer had allowed to reenter the room to retrieve his identification, and who had actually consented to the officer's presence. *Id.* at 3, 102 S.Ct. 812. In short, *Chrisman* has nothing whatsoever to do with plain view seizures of, or "lawful access" to the contents of, *containers.*

6 Imagine, for instance, that a murder suspect's father is sitting in a fast food restaurant eating a salad and reading the morning paper. A homicide detective working the case has been told by a reliable informant that the suspect has admitted to the informant that he, the suspect, had written a full confession and mailed it to his father and that his father keeps the letter with him at all times in a distinctive black briefcase that his father carries wherever he goes. The black briefcase described by the informant is resting on the floor of the fast food restaurant at the feet of the father when the detective enters the restaurant. The detective seizes the briefcase and, without consent or a warrant, immediately opens it. He observes instantly the letter and,

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

quite unexpectedly, wads of counterfeit U.S. currency. The letter is used by the state to prosecute the son for homicide and the possession of counterfeit currency charge is prosecuted in federal court against the father.

Does the majority truly believe that the detective, having what the majority would call "lawful access" to the briefcase, and with probable cause to believe that evidence of a murder would be found in the briefcase, i.e., it was "immediately apparent" (based on the highly reliable information possessed by the detective) that the container held evidence of a criminal offense, could seize the briefcase and search it on the basis of the plain view seizure exception?

Of course not.

Arguably, the briefcase could be seized on the basis of exigency, *see* *United States v. Chadwick,* 433 U.S. 1, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977), *abrogated on other grounds by* *California v. Acevedo,* 500 U.S. 565, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991), but surely even the majority would agree that a warrant would be required to search the briefcase. Even apart from a nice question of the son's standing to challenge the search of the father's briefcase, there clearly is no standing issue as to the father, and the plain view exception simply could not justify the search of the briefcase, despite the "virtual certainty" that evidence of a criminal offense was contained therein. So it is here.

7 In my view, the nonconsensual, warrantless seizure of the bag in this case could only be justified by exigent circumstances, rather than by the plain view seizure doctrine. It appears, however, that the government did not press such an argument before the district court, and with good reason. Although the notion that police need clothes with bullet holes in them to help prove someone got shot is beyond fanciful, there is some support for the view that Detective King had probable cause to believe that the bag beneath Davis's bed contained evidence of his shooting. *But see infra* at 271–73 (explaining why the officers' interaction with Davis demonstrated conclusively that they did not believe his story and, accordingly, they lacked probable cause to believe he had been the victim of a felonious shooting). Therefore, particularly given Detective King's testimony that Davis was uncooperative in response to questioning about the crime, King could reasonably have feared that the clothing would disappear due to a deliberate act of Davis or an inadvertent act of hospital personnel. On the other hand, a police officer might have been posted to safeguard the clothing until a warrant was obtained. Regardless, the government does not raise this argument and, as discussed *infra,* the subsequent search of the bag was unconstitutional in any event.

Indeed, as both the majority and district court opinions demonstrate, application of an exigency exception to the warrant requirement would not save the subsequent search of the bag in this case because no conceivable exigency would apply once the bag was in the custody of law enforcement.

8 It is evident that the police removed Davis's clothing from the bag at some point, but the record does not indicate when the police first opened the bag, so it is not clear when the warrantless container search actually occurred. Lieutenant Lampe testified that the clothing was still in the bag when he arrived at the hospital and retrieved it from Detective King. He recalled that the bag was plastic, but could not recall what it looked like, and he stated that he did not inspect the clothes right away.

To the extent the majority laments the officers' failure of memory about what the bag looked like and what precisely they did many years before they were called to testify on behalf of the government in this case, *see* Maj. Op. 236 n. 15, the majority has done little more than highlight still *another* reason for the imperative of the warrant—issuing function of the state and federal courts. Had the officers properly conducted themselves in searching the bag on the authority of a judicial warrant, there would be no basis for the majority's lament. "Ever since 1878 when Mr. Justice Field's opinion for the Court in *Ex parte Jackson,* 96 U.S. 727, 24 L.Ed. 877 (1877), established that sealed packages in the mail cannot be opened

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

without a warrant, it has been settled that an officer's authority to possess a package is distinct from his authority to examine its contents." *Walter v. United States,* 447 U.S. 649, 654, 100 S.Ct. 2395, 65 L.Ed.2d 410 (1980) (plurality opinion) (citing *Arkansas v. Sanders,* 442 U.S. 753, 758, 99 S.Ct. 2586, 61 L.Ed.2d 235 (1979), and *United States v. Chadwick,* 433 U.S. 1, 10, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977)).

9 The majority's conclusory assertion that, "[T]he subsequent search of the bag (whether to identify or examine its contents), was warranted if it was a foregone conclusion that the bag contained the clothing, which was evidence of a crime," Maj. Op. at 235, is confounding. As explained below, King could only have opened the bag and inspected its contents if their incriminating nature was so obvious that no "search" occurred—but the majority agrees that a search did occur. Of course, having chosen to ignore entirely this dissent's reliance on *Chadwick*, *Robbins*, and *Sanders,* the majority's sole escape is to stand silent in the face of clearly applicable Supreme Court precedents which cannot rationally be distinguished. Those cases, among others, make clear that whether a search occurs is not simply a matter of "labeling." *Cf.* Maj. Op. at 232–33 n. 11.

10 "As *Robbins v. California* ... has established, it takes an open package, or one whose configuration is distinctive as to its contents (i.e., a kit of burglary tools or a gun case) to bring into play the plain view exception to the generally unyielding rule that a warrant must first be obtained." *Blair v. United States,* 665 F.2d 500, 513 (4th Cir.1981) (Murnaghan, J., dissenting); *see id.* at 510 (Murnaghan, J., dissenting) ("It is elementary that probable cause alone does not permit a search. It only provides a substantiating basis for issuance of a warrant.").

11 To the extent *Sanders* and the *Robbins* plurality required that officers who have probable cause that a vehicle contained evidence of crime must obtain a warrant to search closed containers in the vehicle, those cases were overruled. *See United States v. Ross,* 456 U.S. 798, 825, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982); *California v. Acevedo,* 500 U.S. 565, 580, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991). The discussions in *Sanders* and *Robbins* of when the contents of a closed, opaque container are nonetheless obvious, however, remain accurate and unaltered. *See Williams,* 41 F.3d at 196.

12 The majority suggests, utterly without support in the record, that Detective King's testimony that he observed "a bag underneath of the hospital bed that contained clothing," Maj. Op. at 235–36 (citing J.A. 140), "fairly supports an inference that Officer King could see the clothing through the bag or that the bag was partially open, revealing clothing," *id.* at 236. The majority's reasoning is clearly flawed; Detective King's conclusory statement reflecting his own personal belief that the bag contained clothing does nothing to confirm that the belief was anything but an unfounded assumption. For instance, if an employee of a McDonald's restaurant stated that a happy meal contained French fries, we could not reasonably infer that the employee had looked into the box. Instead, it is most likely that the employee merely assumed that the customer had chosen that classic side item, when the customer may well have thought better and opted for apple slices instead.

Contrary to the majority's speculation that Detective King seized the clothing because he could actually see it in or through the bag, the government concedes in its brief that Detective King's nonconsensual, warrantless seizure of Davis's personal property was simply King's standard operating procedure. *See* Govt's Br. at 19 ("As was his practice in previous shooting investigations, Detective King secured the victim's clothing, which had been removed by hospital staff to treat the injury...."). The district court's analysis on this point could not be clearer: "There was no testimony as to whether the bag was open or closed, or whether it was transparent, opaque, or somewhere in-between." *Davis,* 657 F.Supp.2d at 638.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> The majority is not entitled to enhance this negative finding so that it becomes the basis for an inference favorable to the government.
>
> Thus, the majority's extraordinary appellate factfinding ignores the undisputed applicability of the rule that in this case the government bore the burden of proof to establish all the facts necessary to the existence of whatever warrant exception might save the search and seizure in this case, *see supra* pp. 261–63. The majority indulges a so-called "inference" never propounded by the government or drawn by the district court, and not supported by any finding of the district court, in favor of the government. *See, e.g.,* Maj. Op. at 236 ("Nothing in the record contradicts such a conclusion."). Davis had no burden to disprove anything regarding the lawfulness of the search of the bag. Any absence of evidence on the point should count against the party with the burden of proof, here the government.

13 The constitutionality of this corollary to the plain view seizure doctrine is widely accepted, but there seems to be a circuit split with respect to whether the "foregone conclusion" analysis incorporates extrinsic evidence and/or an officer's specialized knowledge. In *Williams* we considered relevant that the officer had years of experience in narcotics investigations. 41 F.3d at 198. Other circuits have instead analyzed the question from the objective viewpoint of a reasonable layperson. *See, e.g., United States v. Gust,* 405 F.3d 797, 803 (9th Cir.2005) ("[C]ourts should assess the nature of a container primarily with reference to general social norms rather than solely by the experience and expertise of law enforcement officers.") (internal quotation marks and alteration omitted); *United States v. Meada,* 408 F.3d 14, 23 (1st Cir.2005) (holding that the defendant had no reasonable expectation of privacy in the contents of a container that was labeled "GUN GUARD" and thus was "readily identifiable as a gun case"); *United States v. Villarreal,* 963 F.2d 770, 775–76 (5th Cir.1992) (holding that even though fifty-five gallon drums were labeled "phosphoric acid," their contents could not necessarily be "inferred"; "The fact that the exterior of a container purports to reveal some information about its contents does not necessarily mean that its owner has no reasonable expectation that those contents will remain free from inspection by others."); *United States v. Bonitz,* 826 F.2d 954, 956 (10th Cir.1987) ("This hard plastic case did not reveal its contents to the trial court even though it could perhaps have been identified as a gun case by a firearms expert."). I believe the latter view is the proper one, because it is consistent with the underlying rationale that a person does not maintain a reasonable expectation of privacy in contents of a container that are essentially open to view.

14 As noted above, a determination whether "historical facts satisfy a constitutional standard" is reviewed de novo. *Gwinn,* 219 F.3d at 331. The question whether the information available to Detective King rendered the incriminating nature of the contents a "foregone conclusion" is such a determination, as the historical facts surrounding the seizure of the bag are not in dispute.

15 We described this turn of events as follows in our opinion reversing the district court's grant of Jamison's motion to suppress evidence for violation of the *Miranda* doctrine:

> Without securing Jamison's consent, Detective Macer examined Jamison's injury, partially exposing his genitalia. He found charring and stippling at the entry wound consistent with a shot fired at close range. He further observed a downward trajectory from the entry wound to the exit wound. Finding these facts to be in tension with Jamison's account of the shooting, Detective Macer then examined Jamison's clothing and found no bullet holes. Detective Macer again asked Jamison to explain the shooting; Jamison repeated that he was shot while using drugs. When Detective Macer explained that his observations seemed inconsistent with Jamison's story, Jamison admitted that he shot himself with a handgun and

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

> threw the gun away. Detective Macer asked Jamison to reveal the location of the gun so that it could be secured, but Jamison refused, explaining that he was on probation.
>
> *Jamison,* 509 F.3d at 626–27 (footnote omitted).

16 A unanimous Supreme Court of Georgia recently reached the same conclusion on material facts nearly identical to those here in an interlocutory appeal in a capital case. In *Clay v. State,* 290 Ga. 822, 725 S.E.2d 260 (2012), an officer had seized a bag containing a murder suspect's bloody clothing while the suspect (who, unlike Davis, was unconscious at the time of the seizure) was undergoing treatment at a hospital. 725 S.E.2d at 264, 269. The court found that the officers were not justified in opening the bag because "all that was in plain view when Officer Cupp seized the bagged clothing from the counter was the pink and white personal effects bag itself." *Id.* at 269. "[W]ithout opening the bag, it was not a 'foregone conclusion' that the bag contained [the suspect's] bloody clothes," and so the "full-blown search of the bag" constituted an unlawful search. *Id.*

> Concomitantly, Davis cites to us, as he cited to the district court, a raft of cases supporting the unremarkable proposition, largely accepted by the district court but ignored by the majority, that a hospital patient retains his constitutionally protected interests in his clothing removed by hospital personnel in the course of their rendering treatment to him. *See* Appellant's Br. at 23–24 (citing *Jones v. State,* 648 So.2d 669 (Fla.1994)); *People v. Jordan,* 187 Mich.App. 582, 468 N.W.2d 294, 301 (1991); *Commonwealth v. Silo,* 480 Pa. 15, 389 A.2d 62, 63–67 (1978); *People v. Watt,* 118 Misc.2d 930, 462 N.Y.S.2d 389, 391–92 (N.Y.Sup.Ct.1983); *Morris v. Commonwealth,* 208 Va. 331, 157 S.E.2d 191, 194 (1967); *People v. Hayes,* 154 Misc.2d 429, 430–34, 584 N.Y.S.2d 1001 (N.Y.Sup.Ct.1992); *State v. Lopez,* 197 W.Va. 556, 476 S.E.2d 227, 231–34 (W.V.1996). Not a single one of these courts accepted the deeply flawed conception of the plain view doctrine applied by the district court in this case and accepted here by the majority.

17 None of the cases cited by the government in support of its reconceptualization of the plain view seizure doctrine are to the contrary. *See* *United States v. Jackson,* 381 F.3d 984 (10th Cir.2004) (after officer searched baby powder container with defendant's consent and discovered cocaine secreted inside, officer could replace lid to container, arrest defendant, and then reopen the container at the police station without obtaining a warrant); *United States v. Eschweiler,* 745 F.2d 435, 439 (7th Cir.1984) (during search of premises, key to safety deposit box discovered in an envelope marked "safety deposit box"); *United States v. Morgan,* 744 F.2d 1215, 1222 (6th Cir.1984) (after airline employee opened suspicious package and discovered container marked with names of controlled substances used to dilute illegal narcotics, and then without a request by drug agents, reopened suitcase when drug agents arrived, chemicals were in "plain view" of agents and marked containers could be opened without a warrant).

18 Of course, I do not seek a return to the "mere evidence" doctrine discarded by the Supreme Court in *Warden v. Hayden,* 387 U.S. 294, 301–02, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967). Rather, the point here is that my search of Supreme Court and circuit authority, as I discuss in the text, does not reveal an instance in which a law enforcement officer has been authorized to seize a closed, opaque container containing non-contraband personalty from the possession of a person on the basis of the plain view exception. In such circumstances, even assuming a seizure is allowed, absent some applicable warrant exception, if the ensuing

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

search of the container was without a warrant, the search violates the Fourth Amendment. Ample Supreme Court authority supports this view. *See supra* pp. 263–66.

19 In contrast, one never has a reasonable expectation of privacy in regard to his possession of contraband. *See* *United States v. Moore,* 562 F.2d 106, 111 (1st Cir.1977) (observing that "the possessors of [contraband and stolen property] have no legitimate expectation of privacy in substances which they have no right to possess at all"), *cert. denied,* 435 U.S. 926, 98 S.Ct. 1493, 55 L.Ed.2d 521 (1978); *cf.* *Jacobsen,* 466 U.S. at 123, 104 S.Ct. 1652 ("A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy."). *Jacobsen* and the cases relied on by the majority, *see* Maj. Op. at 237–38, are entirely consistent with this longstanding rule. *See, e.g.,* *United States v. Smith,* 459 F.3d 1276, 1293 (11th Cir.2006) (plain view seizure of child pornography in the course of a search for narcotics); *United States v. Rodriguez,* 601 F.3d 402, 408 (5th Cir.2010) (where officers came upon a sawed-off shotgun in the course of responding to a domestic violence call, the court reasoned that, "The shotgun was properly seized on a temporary basis to secure it so that the officers could investigate the domestic disturbance call. Once seized for this purpose, the incriminating nature of the weapon became apparent and it was then subject to permanent seizure as contraband.").

20 In fairness to my well-meaning colleagues in the majority, they are not the first judges to misapply the plain view seizure doctrine. *See, e.g.,* *Boone v. Spurgess,* 385 F.3d 923, 928 (6th Cir.2004) (discussed *supra* n. 5.) For example, in jurisdictions such as Maryland, where transporting an unsecured handgun in a vehicle is generally prohibited, if during a traffic stop an officer observed from outside the vehicle the barrel of a handgun, it is not the plain view seizure doctrine that authorizes the officer to enter the vehicle to seize the weapon. Rather, now with probable cause to arrest all the occupants, *see* *Maryland v. Pringle,* 540 U.S. 366, 124 S.Ct. 795, 157 L.Ed.2d 769 (2003), and with probable cause to believe that the vehicle contains evidence of a criminal offense, the officer can search the vehicle and seize the firearm under either the search incident to arrest exception or the automobile exception to the warrant requirement. *See* *id.* The officer's view of the firearm was certainly "plain" in the "Merriam Webster" sense, but there is no occasion for proper application of the plain view seizure doctrine. Whether such cases come to the court by virtue of governmental theorizing or otherwise I cannot say, but we should guard against, rather than embrace, such distortions of doctrine.

21 We and other circuits have recognized what is surely obvious: the *Leon* good-faith exception does not salvage evidence seized on the authority of a tainted search warrant, i.e., one in which probable cause is based on the fruits of a prior illegal search, as in this case. *See* *United States v. Mowatt,* 513 F.3d 395, 405 (4th Cir.2008) (good-faith exception does not apply where search warrant was prompted by previous warrantless illegal search), *abrogated on other grounds,* *Kentucky v. King,* —— U.S. ——, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011); *United States v. McGough,* 412 F.3d 1232, 1240 (11th Cir.2005); *United States v. Reilly,* 76 F.3d 1271, 1280 (2d Cir.1996); *United States v. Scales,* 903 F.2d 765, 768 (10th Cir.1990); *United States v. Wanless,* 882 F.2d 1459, 1466 (9th Cir.1989).

22 As we explained in *Jones,*

> "the exclusionary rule is our sole means of ensuring that police refrain from engaging in the unwarranted harassment or unlawful seizure of anyone," regardless of where that person resides or visits. *United*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

States v. Foster, 634 F.3d 243, 249 (4th Cir.2011). Accordingly, we find the exclusion of evidence to be the proper remedy in this case because of the "the potential ... to deter wrongful police conduct." *See* *Herring v. United States,* 555 U.S. 135, 137, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009).

678 F.3d at 305, n. 7.

23 I respect my good colleagues' discomfort with a reversal in this case, a discomfort that is shared by all members of this panel. *Cf.* *Blair,* 665 F.2d at 509 (Murnaghan, J., dissenting) ("Whenever the exclusionary rule applies, with the resulting suppression of trenchant evidence of guilt, and the substantial and regrettable consequence that an offender against society may go free, the judge is apt to wince or at least to feel a twinge."). Nevertheless, without clearer, more definitive instructions from the Supreme Court than those relied on by the majority, "We should not avoid or vitiate the effectiveness of the exclusionary rule by distorting what constitutes the essential ingredients of a proper search or seizure." *Id.*

24 *See* Adam Liptak, Supreme Court Edging Closer to Repeal of Evidence Ruling, N.Y. Times, Jan. 31, 2009, at Al.

* * * * * *

End of Document © 2022 Thomson Reuters. No claim to original U.S. Government Works.

239 *Id.*

240 *Id.* at 111-12.

241 *Id.* at 112 (further explaining that "a hotel guest customarily has no reason to expect the manager to allow anyone but his own employees into his room").

242 *Id.*

243 *Id.* at 113.

244 *Id.* at 114.

245 *Id.*

246 Fernandez v. California, 571 U.S. 292, 303-304 (2014).

247 *Id.*

248 *Id.*

249 *Id.* at 1131.

250 *Id.* at 1135.

251 *Id.*

252 *Matlock*, 415 U.S. at 171, n. 7.

253 New York University Law Professor Erin Murphy explained, "If I'm making a decision that affects my brother, my sister, my father, my children, essentially everybody I'm related to, I think that's really different." Megan Jula, *The Breakthrough DNA Technique that Led Cops to the Golden State Killer Suspect Is Exciting--and Terrifying,* MOTHER JONES (Apr. 27, 2018), https://www.motherjones.com/crime-justice/2018/04/the-breakthrough-dna-technique-that-led-cops-to-the-golden-state-killer-suspect-is-exciting-and-terrifying/.

254 *Id.*

255 *Matlock*, 415 U.S. at 170.

256 *Id.* at 171, n. 7.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

257 *Id.*

258 *Randolph*, 547 U.S. at 106, 111.

259 *Fernandez*, 571 U.S. at 303.

260 *Randolph*, 547 U.S. at 111.

261 *Id.*

262 *Id.*

263 Cyrus Farivar, *GEDmatch, a Tiny DNA Analysis Firm, Was Key for Golden State Killer Case*, ARS TECHNICA (Apr. 27, 2018), https://arstechnica.com/tech-policy/2018/04/gedmatch-a-tiny-dna-analysis-firm-was-key-for-golden-state-killer-case/ ("In fact, when it first began in 2010, GEDmatch did not even require a login.").

264 Wilson v. Arkansas, 514 U.S. 927, 931 (1995).

265 Kolata, *supra* note 66; *see generally* Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html. ("Cambridge Analytica, a political data firm hired by President Trump's 2016 election campaign, gained access to private information on more than 50 million Facebook users. The firm offered tools that could identify the personalities of American voters and influence their behavior.")

266 Kolata, *supra* note 66.

267 *Carpenter*, 138 S. Ct. at 2223.

268 Walter v. United States, 447 U.S. 649, 651 (1980); *see also* United States v. Jacobsen, 466 U.S. 109, 115 (1984) ("While there was no single opinion of the Court [in *Walter*], a majority did agree on the appropriate analysis of a governmental search which follows on the heels of a private one.").

269 *Id.* at 651-52.

270 *Id.* at 652.

271 *Id.*

272 *Id.* at 651.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

273 *Id.* at 656.

274 *Id.*

275 *Id.*

276 *Id.* at 657.

277 *Id.*

278 *Id.*

279 United States v. Jacobsen, 466 U.S. 109, 116 (1984).

280 *Walter*, 447 U.S. at 651-52.

281 *Id.* at 659.

282 *Id.*

283 United States v. Jacobsen, 466 U.S. 109 (1984).

284 *Id.* at 111.

285 *Id.*

286 *Id.*

287 *Id.* at 111-12.

288 *Id.* at 115.

289 *Id.*

290 *Id.* at 117.

291 *Id.*

292 *Id. Jacobsen* noted, "In such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant." *Id.* at 117-18.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

293 *Id.* at 118.

294 *Id.* at 118-119.

295 *Id.* at 119.

296 *Id.* at 119-120.

297 *Id.* at 122.

298 *Id.*

299 *Id.*

300 *Id.* at 123.

301 *Walter*, 447 U.S. at 651-52, 658.

302 *Jacobsen*, 466 U.S. at 116.

303 *Id.*

304 The DEA's field test of the powder in *Jacobsen*, unlike the FBI search in *Walter*, was found to not implicate a "legitimate" expectation of privacy. *Id.* at 123.

305 Jouvenal, TO FIND ALLEGED GOLDEN STATE KILLER, supra note 2, at 2. Officials also examined "police and commercial databases." *Id.* While law enforcement's reference to its own databases should not trigger a Fourth Amendment issue, the privacy concerns surrounding use of "commercial" databases would depend on the specifics involved in each particular visit. *Id.*

306 Winton, *supra* note 60.

307 Jouvenal, *supra* note 2, at 2.

308 The Court, in *Byrd v. United States*, commented, "It is worth noting that most courts analyzing the question presented in this case ... have described it as one of Fourth Amendment 'standing.'" 138 S. Ct. 1518, 1530 (2018).

309 Rakas v. Illinois, 439 U.S. 128, 133 (1978).

310 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

311 *Id.* at 130.

312 *Id.*

313 *Id.* at 130.

314 *Id.*

315 *Id.* at 132.

316 *Id.* at 139.

317 *Id.* at 133.

318 *Id.*

319 *Id.* at 140.

320 *Id.* at 133-34.

321 *Id.* at 134.

322 *Id.*

323 *Id.* at 150, n. 17.

324 *Byrd*, 138 S. Ct. at 1530.

325 *Id.* at 1524.

326 *Id.*

327 *Id.*

328 *Id.*

329 *Id.* at 1523.

330 *Id.* at 1527. Deciding whether Byrd had "his own Fourth Amendment rights infringed by the search" meant determining whether he had a "legitimate expectation of privacy" in the place searched. *Id.* at 1526.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

331 *Id.* at 1527. The "understandings that are recognized and permitted by society" will not be explored in this Article in light of the previous discussions regarding privacy expectations in *supra* Section B of Part IV and "widely shared social expectations" in *supra* Section C of Part IV.

332 *Id.* at 1527, 1528.

333 *Id.* at 1528.

334 *Id.* at 1529.

335 *Id.*

336 *Id.* at 1531.

337 *GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last modified May 20, 2018).

338 Jouvenal et al., *supra* note 62.

339 *GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last modified May 20, 2018).

340 *Id.*

341 *Byrd*, 138 S. Ct. at 1528.

342 Jouvenal et al., *supra* note 62.

343 *Id.*

344 *Id.*

345 *Id.*

346 Gafni, *supra* note 57.

347 *Id.*

348 *King*, 569 U.S. at 449, 462.

349 *Carpenter*, 138 S. Ct. at 2223.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

350 *Id.*

351 *Randolph*, 547 U.S. at 111.

352 *Jacobsen*, 466 U.S. at 116.

353 *Byrd*, 138 S. Ct. at 1528.

354 *Id.*

10 HSTSTLJ 103

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

10 Hastings Sci. & Tech. L.J. 103

Hastings Science & Technology Law Journal
Summer, 2019

Article
George M. Dery III

Copyright © 2019 by Hastings College of the Law; George M. Dery III

CAN A DISTANT RELATIVE ALLOW THE GOVERNMENT ACCESS TO YOUR DNA?
The Fourth Amendment Implications of Law Enforcement's Genealogical Search for the Golden State Killer and Other Genetic Genealogy Investigations

Abstract

This Article considers the advent of genetic genealogy, used by law enforcement in capturing the Golden State Killer suspect and in other cold cases. In these investigations, police used genetic information obtained from the open source genealogy site, GEDmatch, to build vast family trees spanning the entire country and several generations in order to locate suspects whose DNA matched that left at a crime scene. This Article analyzes the Fourth Amendment implications of government use of such powerful technology to explore such sensitive information as DNA. The conclusion the Supreme Court could reach, should it be called upon to examine the privacy issues involved in such intrusions, would vary depending on which avenue of Fourth Amendment analysis it chose to pursue. *Maryland v. King*, Court precedent on government collection of DNA, is so narrow that it provides little guidance on the issues presented by genetic genealogy. Instead, the Court could consult its recent ruling in *Carpenter v. United States*, which limited the third party doctrine that had previously nullified privacy expectations in shared information. If it relied on *Carpenter*, the Court would likely prohibit government downloads from genealogy sites without a warrant. Further, the Court could view individuals' uploads of genetic information onto open source genealogy sites as amounting to consent to view the DNA shared with all relatives. The Court might therefore apply its third party consent precedent, which, in relying on widely shared societal expectations, would likely prevent warrantless collection of genetic information from genealogy sites. The Court could, however, view police visits to genealogy sites as government searches that occurred after private intrusions. If the Court chose this approach, it could rule that law enforcement is free to collect the DNA ***104** information because it is only viewing information already exposed by private parties. Finally, the Court could see law enforcement's use of genetic genealogy as an issue of standing, as recently analyzed in Byrd v. United States. Application of Byrd's property rights definition of standing would likely enable the government to admit genetic evidence since suspects lack the power to exclude others from open source sites. Thus, although some Fourth Amendment doctrines would forbid warrantless collection of DNA information, the government could likely rely on either antecedent private search or standing precedent to successfully use genetic genealogy evidence.

INTRODUCTION 105
THE FUNDAMENTALS OF FOURTH AMENDMENT PROTECTION AGAINST UNREASONABLE SEARCHES 108
A. The Definition of a "Fourth Amendment Search" 108
B. The Warrant Requirement 110
THE SEARCH FOR THE GOLDEN STATE KILLER SUSPECT AND OTHER INVESTIGATIONS 111
IMPLICATIONS OF THE COLLECTION AND USE OF DNA INFORMATION FROM GENEALOGY SITES 116
A. *Maryland v. King*'s Ruling on Government DNA Collection Is So Narrow that it Provides Inadequate Guidance for Government Use of Genealogy Sites 116

B. *Carpenter v. United States* Recent Limit on the Third Party Doctrine, Which Held that Persons Undermine Their Privacy Expectations by Sharing Information, Could Dramatically Constrain Government Downloads from Genealogical Sites 121
C. The Fourth Amendment's Third-Party Consent Precedent Will Likely Not Support Government Exploration of Genealogical Sites for Genetic Information 128
D. If the Court Characterizes Law Enforcement's Use of Genealogical Sites as a Government Search that Occurred after a Private Intrusion, the Lawfulness of the Official Search Will Be Assessed in Reference to the Scope of the Earlier Private Search 135
CONCLUSION 144

***105 Introduction**

How well do you know your relatives? Can you name every cousin, uncle, or great grandparent? Would you base your right to privacy on the whims of every one of your blood relations? Perhaps there is a "black sheep" in your family who continually runs afoul of the law. Maybe there is a flaky uncle always looking for shortcuts or a grandchild who suffers from drug addiction. Moreover, there are likely many distant relatives whose very existence is unknown to you. Would you risk the privacy of your most personal information, housed in your deoxyribonucleic acid (DNA), on this person's judgment?

On National DNA Day, Sacramento District Attorney Anne Marie Schubert announced the arrest of Joseph James DeAngelo, alleging he was the Golden State Killer, [1] believed responsible for 12 killings, 50 rapes, and 100 burglaries from 1974 and 1986. [2] To catch their quarry, police used crime scene DNA to make a partial match with the "DNA of a relative on the open-source genealogy website GEDmatch." [3] Officials then painstakingly constructed "25 family trees containing thousands of relatives" in order to trace "the killer's great-great-great grandparents, who lived in the early 1800's." [4] Investigators dug through "census records, newspaper obituaries, gravesite locators, and police and commercial databases" to whittle the possible suspects down to DeAngelo. [5] District Attorney Schubert accurately characterized law enforcement's efforts as ***106** finding "the needle in the haystack." [6] "The answer was always going to be in the DNA," [7] she concluded.

Law enforcement have every reason to be satisfied with its apparent success in capturing the "clever" and "sadistic" criminal [8] variously known as the "East Area Rapist," the "Original Night Stalker," the "Golden State Killer," [9] the "Diamond Knot Killer," and the "Visalia Ransacker." [10] Erika Hutchcraft, an investigator with the Orange County District Attorney's Office, considered the Golden State Killer's "[v]ery cold, very violent" crimes to be "some of the most horrific [she's] had to investigate." [11] Sacramento County Sheriff's Department Detective Carol Daly deemed this criminal "the most heinous rapist I had ever known." [12] The killer "planned meticulously," calling victims to learn their routines, [13] casing homes, cutting phone lines, and even turning off air conditioners "so he could hear every sound." [14] Such careful planning enabled his attacks to be "bizarre, cruel, and long-lasting." [15] When he was once "cornered" in a backyard with police dogs swarming the area, "he just disappeared into thin air." [16] Police, in finally capturing such a dangerous and elusive suspect, can rightly celebrate the innovation and dedication leading to such a significant achievement. Moreover, law enforcement can report other recent successes in cases long unsolved; the genetic genealogy employed in the Golden State Killer case has already been used to bring other notorious suspects to justice. [17]

***107** While the stakes in tracking down the Golden State Killer and other cold-case suspects are particularly high, the Fourth Amendment privacy concerns involved in government exploration of DNA websites are equally significant. [18] DNA, after all, is the genetic blueprint of our bodies that is embedded in the nucleus--the core--of each cell in the human body. [19] The genetic material in every cell "carries the full sequence of your DNA, including the mutation pattern that makes it uniquely yours." [20] DNA holds the secret to such personal details as one's Neanderthal ancestry, the potential for afflictions with rare diseases, and paternity. [21] One expert warns, "[f]or a non-trivial percentage of us, there really are scary things in our genomes." [22] In certain circumstances, DNA is coveted by companies, insurers and police and can be considered "the most valuable thing you own." [23]

The analytical approach the Court chooses to examine government exploration of DNA on genealogical sites will determine how it decides the Fourth Amendment issues triggered by this new intrusion. Therefore, after Part II reviews the definition of a Fourth Amendment "search" and the Court's warrant requirement. Part III examines the Golden State Killer investigation,

and Part IV analyzes the paths the Court might take in deciding the Fourth Amendment issues concerning genetic genealogy. Part IV discusses *Maryland v. King*'s Fourth Amendment consideration of government DNA collection, [24] and the Court's third party doctrine, which has traditionally limited the privacy expectations of those who share ***108** information. In addition, this section considers *Carpenter's* latest word on the third party doctrine, and its potential, dramatic effect on the Fourth Amendment privacy of the relatives of those who upload information to genealogy sites. [25] It then explores third party consent based on an assumption of risk and shared social expectations, and its potential impact on the official use of genealogical sites. The Court could approach government genetic genealogy as a state intrusion that occurs only after a private search has been performed, thus, triggering precedent that assesses an official probe by reference to the scope of an earlier private invasion. Finally, since the Court might question whether a person could even claim a Fourth Amendment violation from government exploration of a relative's DNA, this article explores whether a suspect could have "standing" or the right to contest an official visit to a particular genealogy site. The standing discussion will consider the Court's most recent case on this issue, *Byrd v. United States*. [26]

The Fundamentals of Fourth Amendment Protection Against Unreasonable Searches

A. The Definition of a "Fourth Amendment Search"

The Fourth Amendment prohibits "unreasonable searches and seizures" of individuals' "persons, houses, papers, and effects." [27] In *Katz v. United States*, the Court defined a "search" as a government intrusion on a person's reasonable expectation of privacy. [28] In *Katz*, the Federal Bureau of Investigation (FBI) caught Katz "transmitting wagering information by telephone from Los Angeles to Miami and Boston in violation of a federal ***109** statute." [29] The FBI had obtained Katz's side of a telephone conversation by bugging his phone booth. [30] When the parties argued over whether the government's eavesdropping by an electronic device attached to the outside of the phone booth [31] constituted a "physical penetration of a constitutionally protected area," the Court rejected this formulation of the issue as "misleading." [32] The focus on "whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected'" deflected attention away from the question of whether a person sought to preserve privacy, even in a publicly accessible area. [33] *Katz* concluded that a person who occupies a phone booth, "shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world." It fell to Justice Harlan, in his concurring opinion, to provide the definition of a Fourth Amendment "search:"

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." [34]

The Court has repeatedly employed *Katz's* definition of a search, as crafted by Justice Harlan, for five decades to determine whether searches have occurred in such diverse situations as government entry into burned buildings, [35] barns, [36] bookstores, [37] and bus bins. [38] The resulting importance of *Katz* can be seen in the fact that the Court has deemed this definition of a search its "lodestar." [39]

***110** B. The Warrant Requirement

The Fourth Amendment prohibits all but reasonable searches and seizures. [40] Although reasonableness is "the ultimate touchstone of the Fourth Amendment," the Constitution itself provides no yardstick for measuring what is and is not reasonable. [41] The Court worried that simply deeming an official intrusion "reasonable," without tying this conclusion to "some criterion of reason," would cause protection under the Fourth Amendment to "approach the evaporation point." [42] The Court also noted that the Fourth Amendment "was in large part a reaction to the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence." [43] The Framers included the "no Warrants shall issue, but upon probable cause" provision to ensure that an objective magistrate "might weigh the need to invade that privacy in order to enforce the law." [44] The Court, therefore, recognized what came to be known as the warrant requirement, which generally mandated officers obtain a warrant before making a search. [45]

Riley v. California reaffirmed the Court's warrant requirement. In *Riley*, officers accessed information on a cell phone and a smart phone. [46] The Court in *Riley* refused to allow a search of these phones as part of a search incident to arrest, instead flatly ruling, "get a warrant." [47] *Riley* explained, "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, ... reasonableness generally requires the obtaining of a judicial warrant." [48] If police fails to obtain a warrant, the search is presumed unreasonable unless "it falls within a specific exception to the warrant requirement." [49]

Carpenter v. United States, decided in 2018, repeatedly referenced the warrant requirement. [50] The Court noted, "our cases establish that ***111** warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing," and, therefore, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." [51] Thus, the warrant mandate, articulated by the Court as early as 1925, still limits police discretion today. [52]

The Search for the Golden State Killer Suspect and Other Investigations

The Golden State Killer was a cold-blooded "serial predator" who elaborately planned his attacks. [53] Before "closing in for the kill," he would terrorize his victims with such strange behavior as breaking into the home to take women's underwear, making hang-up phone calls, or leaving drawings on a bedroom window "that appeared to have been written in 'bodily fluids." [54] He "stalked his victims through drainage ditches" and returned to one neighborhood so many times that its residents slept in shifts. [55] He wore a mask and blindfolded and gagged his victims. [56]

In pursuing its suspect, the investigators themselves became equally careful and inventive. Paul Holes, a cold case expert who had worked as an inspector for the Contra Costa County District Attorney, spent some seven years using "open source" genealogy websites to locate the Golden State Killer suspect. [57] Holes first used "Ysearch.org" to generate a "weak match" with a 73-year-old man in Clackamas County, Oregon. [58] The man willingly ***112** provided a DNA sample, which established his innocence. [59] After this setback, Holes visited other jurisdictions that had suffered the Golden State Killer's crimes in order to obtain DNA to use at a different genealogy website, GEDmatch. [60]

GEDmatch is an "open-source genealogy website" based in Florida "that pools raw genetic profiles that people publicly share to find long-lost relatives." [61] GEDmatch differs from commercial genealogy sites such as 23andMe and Ancestry.com, which charge a fee to "millions of customers wanting detailed information on their family, lineage and ethnicity." [62] 23andMe and Ancestry.com sell testing kits that require customers to supply a tube of saliva. [63] These direct-to-consumer sites then "work very hard to protect their customers' privacy." [64] A spokesperson for 23andMe declared that it had "never given customer information to law enforcement officials," and that the company did "not share information with employers or insurance companies, ever, under any circumstance." [65]

GEDmatch does not follow the direct-to-consumer sites' model. Instead of forming a commercial and confidential relationship with consumers, it invites anyone to upload DNA profiles already generated by the commercial sites. [66] Hobbyists researching their genealogy have uploaded "roughly a million distinct DNA sets" onto GEDmatch. [67] The ***113** very utility of GEDmatch is based on its openness. [68] When he later learned of the government use of GEDmatch, Curtis Rogers, a GEDmatch operator noted "it has always been GEDmatch's policy to inform users that the database could be used for other uses, as set forth in the Site Policy." [69] Rogers warned, "[W]hile the database was created for genealogical research, it is important that GEDmatch participants understand the possible uses of their DNA, including identification of relatives that have committed crimes or were victims of crimes." [70] According to Paul Holes, such openness offered law enforcement officials access to "a large pool of profiles and didn't require a court order." [71]

After Holes' prompting, Steve Rhods, an investigator with the Ventura County District Attorney's Office, found a second rape kit in the county's coroner's office that proved to be "the mother lode of DNA." [72] The upload to GEDmatch revealed a distant match

that was "roughly the equivalent of third cousins." [73] Holes traced back these distant relatives to find a common ancestor. [74] His search created a family lineage that "went back to 'great-great-great-grandparents in the early 1800s"' that mostly identified persons "from the East Coast or Midwest." [75] The investigators slowly tracked their suspect through the generations by tracing "offspring to the present day." [76] Holes whittled down the "huge" family trees he had created on Ancestry.com by consulting "census data, old newspaper clippings," gravesite locator, and LexisNexis. [77] The task investigators faced was daunting; out of some 25 family trees, the one including DeAngelo contained about 1,000 members. [78]

***114** Towards the end of the investigation, Holes had focused on five white men, including DeAngelo. [79] Holes considered some of DeAngelo's factors, such as his age and his "serving full-time as a cop," as "strike(s) against" being the killer. [80] One fact, however, was particularly damning for DeAngelo. During a July 1978 rape, the East Area Rapist "was sobbing and saying, 'I hate you Bonnie, I hate you Bonnie." [81] Investigators learned that DeAngelo "had been engaged to a woman named Bonnie in 1970." [82] In April 2018, police observed DeAngelo speeding his motorcycle down the freeway in excess of 100 miles an hour. [83] Holes noted "stop signs are optional for this guy." [84] Detectives collected DeAngelo's DNA from the door of his car while he shopped in a Hobby Lobby in Roseville, California. [85] This DNA "matched semen recovered at the scene of some of the Golden State Killer's crime scenes." [86] They later obtained a second sample "from a tissue in DeAngelo's trash outside of his home." [87] Police arrested DeAngelo on April 24, 2018. [88] The warrant police obtained to search DeAngelo's home was based in part on the earlier genealogical search in this case. [89]

The pursuit of the Golden State Killer through genealogical sites is not an isolated case. In June of 2018, Lancaster County District Attorney, Craig Stedman, announced at a news conference the arrest of Raymond Rowe for the beating, sexual assault, and strangulation of Christy Mirack. [90] Mirack was a 25-year-old schoolteacher whose murder case went cold despite the forensic testing of 60 suspects and the conducting of over 1,500 ***115** interviews. [91] Mirack's mother made a "deathbed plea in the newspaper for new information" and her brother put up a billboard and started a Facebook page seeking tips. [92] Recognizing that they "didn't have any more arrows in the quiver," authorities turned to genetic genealogy. [93] The District Attorney's Office worked with Parabon NanoLabs, which created "a genotype file" from semen found on the "carpeting under the victim's body and on her person." [94] Parabon NanoLabs uploaded this file to GEDmatch, which enabled them to build family trees offering "highly scientific" suggestions for traditional police investigations. [95] Pennsylvania State Police narrowed the search to Rowe, who was scheduled to perform as a DJ at an elementary school event. [96] Undercover officers then collected chewing gum and a water bottle that Rowe had used and then discarded. [97] The crime lab linked Rowe to the Mirack homicide with a "1 in 200 octillion chance the match is to another member of the Caucasian population who is not Rowe." [98]

Law enforcement also visited public genealogy sites to solve the 1988 abduction, rape, and strangulation-murder of eight-year-old April Tinsley of Fort Wayne, Indiana. [99] The case became Indiana's "most notorious cold case" in part due to the alleged killer's threats toward other little girls in Fort Wayne starting in 2004. [100] The attacker left notes, found inside bags with used condoms or Polaroid pictures of his body, on the girls' bicycles. [101] One note chillingly read, "Hi honey I been watching you I am the same person that kidnapped an rape an kill Aproil Tinsley you are my ***116** next vitem (sic)." [102] Authorities again turned to Parabon NanoLabs to analyze the DNA samples and then visited genealogy sites to gain a list of suspects. [103] After narrowing their search to two brothers, police collected used condoms from the trash outside the trailer home of John D. Miller. Obtaining a match with the crime scene samples, officials contacted Miller and asked, "[W]hy he thought police were interested in speaking with him." [104] Police reported that Miller answered, "April Tinsley." [105]

The genetic genealogy investigations of DeAngelo, Rowe, and Miller are the advent of a potentially game-changing technology that represents hope for victims and families long suffering from seemingly unsolvable crimes. At the same time, this search technology is so uniquely powerful that it presents issues of crucial concern for Fourth Amendment rights.

Implications of the Collection and Use of DNA Information from Genealogy Sites

A. *Maryland v. King*'s Ruling on Government DNA Collection Is So Narrow that it Provides Inadequate Guidance for Government Use of Genealogy Sites

Should the Golden State Killer case reach the Court, one might suppose that the Court would consult its first case involving the Fourth Amendment implications of government use of DNA evidence in a criminal matter, Maryland v. King. [106] Close scrutiny of King, however, might not support such an assumption. In King, the Court considered "whether the Fourth Amendment prohibits the collection and analysis of a DNA sample from persons arrested, but not yet convicted, on felony charges." [107] Officers arrested Alonzo King for assault by "menacing a group of people with a shotgun." [108] Police collected a DNA sample from King, as "part of a routine booking procedure for serious offenses," by rubbing a "filter paper or cotton swab" against the inside of his cheek. [109] ***117** King's DNA matched a sample of DNA taken from a rape occurring six years earlier, resulting in his trial and conviction of rape. [110]

The corrections officers at the booking facility in King automatically collected DNA in reliance on a Maryland statute authorizing "law enforcement authorities to collect DNA samples from 'an individual who is charged with ... a crime of violence or an attempt to commit a crime of violence; or ... burglary or an attempt to commit burglary.'" [111] The collected sample was not to be added to a government database until after probable cause was found at the arraignment or the detainee provided consent. [112] The statute specifically limited the use of DNA records to identification purposes only. [113] Maryland's law explicitly prohibited searching for "familial matches," providing: "A person may not perform a search of the statewide DNA data base for the purpose of identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the DNA sample was acquired." [114] Government officials uploaded King's DNA information to Maryland's DNA database. [115] The identification of King as a rapist was based in part on the "national project to standardize collection and storage of DNA profiles" known as the "Combined DNA Index System (CODIS)." [116] Created by Congress and supervised by the FBI, CODIS "has grown to include all 50 states and a number of federal agencies." [117] CODIS "collects DNA profiles provided by local laboratories taken from arrestees, convicted offenders, and forensic evidence found at crime scenes." [118]

The *King* Court concluded that routine collection and analysis of DNA upon booking was reasonable under the Fourth Amendment because "[W]hen officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment." [119] *King* reached this ***118** result without relying on the Fourth Amendment's traditional norms of the warrant requirement or individualized suspicion. [120] Instead, the Court assessed the reasonableness of the DNA collection by balancing the interests of government and individual. [121] To *King*, context was key; the particular circumstances in which officials assumed responsibility over persons taken into their custody both heightened government interests [122] and lessened individual privacy concerns. [123]

When considering government concerns, *King* was acutely aware of the high stakes involved in taking a person into custody because "the law is in the act of subjecting the body of the accused to its physical dominion." [124] Officials had practical reasons for knowing "who has been arrested and who is being tried." [125] Learning identity revealed criminal history, which is crucial information because persons "detained for minor offenses can turn out to be the most devious and dangerous criminals." [126] Proper identification could alert officials to "a record of violence or mental disorder," and therefore disclose "the type of person" officers are detaining." [127] Corrections officers could thus ensure that an arrestee did "not create inordinate 'risks for facility staff, for the existing detainee population, and for a new detainee.'" [128] DNA identification also promoted the "substantial interest in ensuring that persons accused of crimes are available for trials" because it alerted officials to persons likely to fail to appear in court due to outstanding pending cases. [129] Further, knowing a detainee's past was "essential to an assessment of the danger he poses to ***119** the public," a vital factor in assessing bail eligibility. [130] Fixing identity also served "the interests of justice" because properly connecting an arrestee to a crime could exonerate someone "wrongfully imprisoned for the same offense." [131]

An individual arrestee's interests suffered by comparison to the "substantial government interest" in the "unique effectiveness of DNA identification." [132] *King* viewed the intrusion of a DNA cheek swab as "minimal" [133] and the processing of a DNA sample in CODIS as reasonable. [134] While noting that genes, "the coding regions" of DNA, provide instructions for making the proteins in an individual's body, [135] *King* dismissed the "noncoding" DNA, which the government used to make a DNA identification of a person, as "'junk' DNA" [136] which did not reveal "information beyond identification." [137]

Further, the legitimacy of privacy expectations was dependent upon "the individual's legal relationship with the State." [138] King's expectations were necessarily "diminished" because he was "an individual taken into police custody." [139] As a person who "has been arrested on probable cause for a dangerous offense," King's "freedom from police scrutiny" was simply reduced. [140] Indeed, situational factors were so central to the analysis that the Court explicitly distinguished King's DNA collection from a ***120** search of "the average citizen." [141] *King* warned that changing context could result in a different ruling; the Court noted, "If in the future police analyze samples to determine, for instance, an arrestee's predisposition for a particular disease or other hereditary factors not relevant to identity, that case would present additional privacy concerns not present here." [142] The Court thus concluded, "In light of the context of a valid arrest supported by probable cause respondent's expectations of privacy were not offended" by the DNA collection in this case. [143]

As the Court's only case directly dealing with a Fourth Amendment search of a person's DNA, *King* must be accounted for when considering police use of genetic genealogy. *King* deemed reasonable the mandatory collection of DNA from arrestees of violent offenses about to be taken into official custody. [144] The utility of this holding in assessing government collection of DNA information from genealogical sites, however, might be quite limited. The context of *King*, so important to the Court, significantly differed from that of genetic genealogy. In *King*, officers had probable cause that the person searched had committed a crime. [145] The government therefore had the "uncontested" right, "always recognized under English and American law," to search the lawfully arrested person. [146] Further, King was jailed and therefore exposed to booking procedures having "different constitutional justifications" than searches in other places. [147] *King's* jail context was crucial because State interests "are further different" when the government takes on the grave responsibility of "subjecting the body of the accused to its physical dominion." [148] In this setting, DNA identification was critical for a host of government interests, including safety of staff, fellow prisoners, and the arrestee himself, [149] determination of availability for trial, potential danger to the public, [150] and the interests of justice. [151] In contrast, the government visits to genealogy sites in pursuit of DeAngelo, Rowe, and Miller lacked all the contextual justifications bolstering *King's* ***121** collection of DNA. To say that police lacked probable cause pinpointing these suspects is an enormous understatement; law enforcement did not even have these individuals on its radar. As for jail, these cases had become so cold that, before GEDmatch, subjecting the bodies of these suspects to the government's physical dominion was a practical impossibility.

King's contextual limit similarly suffers when comparing King's individual interests with those of the genetic genealogy suspects. King, due to his "legal relationship with the state" as an arrestee entering custody, had "diminished" privacy expectations. [152] DeAngelo, Rowe, and Miller, having no such custodial relationship with the State when law enforcement visited the genealogy sites, suffered no corresponding diminution of privacy expectations. Instead, they were the very "average citizen(s)" *King* distinguished from jail inmates. [153] Finally, *King* explicitly noted its case did not involve "familial" matching," the central strategy involved in the genetic genealogy cases. [154] Thus, while *King* offers a detailed picture of the Court's analysis of Fourth Amendment privacy issues involving DNA, the narrowness of its ruling undermines its usefulness in providing guidance for government exploration of genealogical sites.

B. *Carpenter v. United States'* Recent Limit on the Third Party Doctrine, Which Held that Persons Undermine Their Privacy Expectations by Sharing Information, Could Dramatically Constrain Government Downloads from Genealogical Sites

When one uploads his or her genetic information onto a genealogical site, he or she shares it with third parties. The whole point of exposing this information to the public on the website is to enable someone else to access the information about one's DNA in hopes of identifying lost or unknown relatives. In revealing genetic information when searching for one's family, is

a person giving up his or her right to privacy from a government search of this information? The Court's third party doctrine could directly affect the Fourth Amendment rights of those who upload their DNA. [155]

Katz rejected the notion that a Fourth Amendment "search" requires a physical trespass upon a constitutionally protected area, explaining that what a person "seeks to preserve as private, even in an area accessible to ***122** the public, may be constitutionally protected. [156] By the same token, however, the Court declared, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." [157] *Katz*'s "knowingly exposes" language ultimately took on great significance in creating the third party doctrine where "an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." [158]

For decades, the Court ruled that sharing information with another person often amounted to losing any Fourth Amendment privacy protection in the information disclosed. In *United States v. Dionisio*, where a grand jury subpoenaed an illegal gambling suspect to provide a voice exemplar for comparison with FBI recordings, the Court found that the government demand involved no intrusion on a reasonable expectation of privacy. [159] Because "nothing is being exposed to the grand jury that has not previously been exposed to the public at large," Dionisio could not have "a reasonable expectation that others" would not know the sound of his voice "any more than he can reasonably expect that his face will be a mystery to the world." [160]

Information sharing with a "third party" squandered Fourth Amendment privacy in *United States v. Miller*. [161] In *Miller*, the government sought a bank depositor's "checks and other bank records" in its investigation of the depositor's unregistered still and whiskey business. [162] When Miller objected that his bank documents had been illegally seized, the Court found no intrusion of a Fourth Amendment interest. [163] *Miller* noted that the depositor, "in revealing his affairs to another," took the risk that the information so revealed would "be conveyed by that person to the Government." [164] The Court therefore ruled, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose ***123** and the confidence placed in the third party will not be betrayed." [165] Sharing information, even as sensitive as personal finances and even with an institution as discrete as a bank, led to exposure of that information to the government without Fourth Amendment protection.

In *Smith v. Maryland*, the Court determined that what was true about sharing one's voice and banking records was also true about sharing numbers dialed from a phone. [166] In *Smith*, police used a pen register to collect the numbers a robber dialed from his phone in making threatening calls to a robbery victim. [167] When Smith sought to suppress the dialed numbers, the Court refused to do so, noting that he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business" [168] *Smith* declared once again that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." [169]

The Court, in *California v. Greenwood*, even applied its third party doctrine to persons who roll their trash to the curb for collection. [170] *Greenwood* found no Fourth Amendment search occurred when police rummaged through garbage for narcotics evidence because the residents "exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection." [171] Placing trash on the curb made it "readily accessible to animals, children, scavengers, (and) snoops." [172] The whole point of leaving refuse at the curb was "for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so." [173] Therefore, there was "no reasonable expectation of privacy" in the discarded items. [174]

The Court's latest pronouncement on the third party doctrine, in its 2018 case, *Carpenter v. United States*, was more nuanced than previous declarations. In *Carpenter*, police officers and FBI agents suspected Timothy Carpenter of being involved in robberies of nine stores in ***124** Michigan and Ohio. [175] Federal prosecutors therefore sought court orders "under the Stored Communications Act" to obtain Carpenter's cell phone records. [176] Federal magistrate judges ordered MetroPCS and Sprint to provide cell site information for Carpenter's phone over the four months during which the robberies were committed. [177] Pursuant to the orders, agents collected "cell-site location information (CSLI)" over 127 days from MetroPCS alone. [178] CSLI

is the information wireless carriers collect from cell phones in order to "continuously scan their environment looking for the best signal, which generally comes from the closest cell site." [179] Smartphones tap into the wireless network "several times a minute" even when the owner is not using the phone. [180] The resulting "time-stamped" records, which companies store for their own business purposes, are the CSLI. [181] CSLI gives authorities a precise map of where a phone, and therefore the phone's owner, has been. The collection of Carpenter's CSLI provided officials with "12,898 location points cataloging Carpenter's movements--an average of 101 data points per day." [182] When the government used the CSLI to place Carpenter near four of the robberies, Carpenter objected that the use of these data constituted an unreasonable search made in absence of a warrant or an exception to the warrant requirement. [183]

In considering Carpenter's claim, the Court acknowledged that it had previously held, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." [184] The government, therefore, was "typically free to obtain" the shared information "from the recipient without triggering Fourth Amendment protections." [185] *Carpenter*, however, asserted that the third party doctrine had been limited from the start. The Court noted that, in *Miller*, the case ***125** where the third party doctrine traced its "roots," the information lacking Fourth Amendment protection had: 1) a particular "nature," and 2) a specific relationship with the person claiming privacy. [186] The nature of *Miller's* documents "confirmed Miller's limited expectation of privacy" because they were "not confidential communications but negotiable documents," such as checks "exposed" to employees "in the ordinary course of business." [187] As for Miller's relationship with the documents, it was quite weak because he could "assert neither ownership nor possession" of the papers. [188] *Carpenter* then declared that *Smith*, the third party case occurring only three years after *Miller*, was a similarly narrow case. [189] *Smith* involved pen registers--devices that merely recorded numbers dialed from a phone--a technology with "limited capabilities." [190] Together, *Miller* and *Smith* "did not rely solely on the act of sharing" but instead took into account the "nature" of the information sought and the "limited capabilities" of the government technology used to collect the information. [191]

Carpenter then distinguished *Miller* and *Smith* from the facts in its own case. The nature of the information collected in *Carpenter* represented a "world of difference" from that obtained in *Miller* and *Smith*. [192] The CSLI presented "an all-encompassing record" of the "privacies of life," including aspects of "familial, political, professional, religious, and sexual associations." [193] Unlike prior methodologies, cell phone location had a "retrospective quality" enabling the government to "travel back in time" to reconstruct a person's movements "every moment of every day for five years." [194] Further, unlike the information in earlier third-party precedent, CSLI information had a particularly intimate relationship with the phone user because a cell phone has become "almost a 'feature of human anatomy'" that can reveal visits to "doctor's offices, political headquarters, and other potentially revealing locales." [195] Finally, the capabilities of CSLI represented a "seismic shift" in technology from *Miller* and *Smith* because ***126** the "exhaustive chronicle of location information" can be "casually collected" with a "click of a button." [196]

DNA, in 1) the nature of the information it contains, 2) the relationship of that information with the individuals claiming Fourth Amendment protection and 3) the capability of the technology exploiting it, shares similarities with the CSLI in *Carpenter*. Analysis of these three factors indicates that the Court would refuse to extend its third-party doctrine to warrantless government collection of DNA information from genealogical sites. Trouble starts for officials using genetic genealogy with the first factor regarding the "nature" of the information collected. It is hard to overstate the intimacy of DNA information, housed in the "nucleus of all human cells," which offers a blueprint to the entire body. [197] DNA provides a "treasure trove" of private data, including details on "family, lineage and ethnicity" and even a window into potential disease. [198] The very sensitivity of DNA information forces commercial sites such as 23andMe to "work very hard to protect their customers' privacy." [199] While *Carpenter's* CSLI could reveal a visit to the doctor's office, DNA could expose the underlying health issue itself. [200]

Carpenter's focus on the relationship of information to the individual also favors Fourth Amendment protection of genealogical information. If a cellphone is "almost a 'feature of human anatomy,'" DNA is quite literally a feature of human anatomy. [201] DNA is "deeply revealing" precisely because it intimately maps a person's behavior and, in part, fate. [202] Without discounting the importance of environment, DNA has been linked to such deeply sensitive personal traits as promiscuity, learning ability,

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

and violent criminality.[203] The information on genealogy sites would therefore ***127** represent a "world of difference" from *Miller* and *Smith*, thus distinguishing this precedent into insignificance.[204]

Finally, *Carpenter's* discussion regarding the capabilities of the government technology being used militates against allowing visits to genealogical sites without a warrant. *Carpenter* forbade warrantless use of cell phone data because of the "depth, breadth, and comprehensive reach" of CSLI technology.[205] The daunting scope of CSLI searches was presumably due to its ability to penetrate fully into the many aspects of its target's lives by learning a person's every location in collecting no less than 101 data points a day.[206] In comparison, the DNA making up genealogical information penetrates at a deeper level, revealing such secrets as susceptibility to certain diseases, such as breast cancer, Huntington's disease, and cystic fibrosis.[207] Moreover, DNA can reveal a person's potential longevity, risk of obesity, his or her body clock (whether an early riser or a night owl), and possession of "sensation-seeking and impulsive tendencies."[208] Therefore, the Court that was offended by the prospect of the government tracking individuals by every nearby cell site would likely be appalled by official intrusion into DNA.

Further, *Carpenter* worried about the "inescapable and automatic nature" of CSLI collection.[209] Anyone who uses a smartphone--a technology so necessary today that people "compulsively carry cellphones with them all the time"--is exposed to information collection even when the phone is not in use.[210] DNA housed on genealogy sites shares the involuntary character of CSLI exposure. No one could stop a government official from looking at the DNA one shares with a relative. Once an individual uploads his or her DNA, any distant cousin or granddaughter sharing this DNA is helpless to opt out. More fundamentally, one does not choose his or her DNA at birth and, so far, has no ability to change it ***128** thereafter. The DNA, automatically self-replicating in each cell, generates by a process beyond human will.

Carpenter also feared the time-machine character of CSLI technology, noting that a search of cell site data enabled officials to "travel back in time to retrace a person's whereabouts.[211] To perform such tracking, police "need not even know in advance whether they want to follow a particular individual, or when."[212] When it comes to investigating the intricate details of a person's past, DNA is even more Orwellian than CSLI. While CSLI can allow the government to review "five years," genealogical genetics enables officialdom to explore untold generations.[213]

In the past, the Court has recognized the potential for "highly sophisticated" technology to corrode privacy.[214] Indeed, the Court has explicitly noted, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[215] *Carpenter's* concerns, therefore, are not unjustified. If the Court found CSLI collection to be "qualitatively different" from earlier cases allowing government access to shared information, the prospect of official use of the even more intrusive technology--genetic genealogy--will likely raise the Court's ire.[216] When confronted with government exploitation of genealogy sites, therefore, the Court will probably follow *Carpenter* in ensuring that the "'progress of science' does not erode Fourth Amendment protections."[217]

C. The Fourth Amendment's Third-Party Consent Precedent Will Likely Not Support Government Exploration of Genealogical Sites for Genetic Information

When a person uploads his or her DNA information to a genealogy site, this individual is giving consent for others to access this information. ***129** Since the genetic information the person is providing is partly shared by others, the upload could be seen as an example of third-party consent, where one person gives permission to intrude on an area or thing commonly possessed with another. The Court explored the Fourth Amendment implications of third-party consent in *United States v. Matlock.*[218] In *Matlock*, police officers arrested William Matlock for robbery in the front yard of his residence.[219] After placing Matlock in a squad car,[220] the officers went to the house and met Mrs. Gayle Graff, "who was dressed in a robe and was holding her son in her arms."[221] Mrs. Graff permitted police to search for money and a gun in the bedroom of a home that she jointly occupied with Matlock.[222] As a result of the consensual search of the bedroom, officers found $4,995.00 in cash inside a diaper bag.[223]

Since Matlock himself did not consent to the search, the issue before the Court was "whether Mrs. Graff's relationship to the east bedroom was sufficient to make her consent to the search valid against ... Matlock."[224] The Court ruled, "the consent of

one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared." [225] A person's "common authority" to give consent is not based on "mere property interest." [226] This power instead rests "on mutual use of the property by persons generally having joint access or control for most purposes." [227] The sharing of access or control makes it "reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched." [228] In sharing a place with another person, one automatically assumes that other person might expose that "common area" ***130** to others, even the police. Thus, Matlock, in sharing a bedroom with Mrs. Graff, took the risk that she might allow officers to enter and search it. [229]

Matlock, tucked away in a patrol car before police approached his home, never had the opportunity to object to a search of his bedroom. [230] Scott Randolph, in *Georgia v. Randolph*, was under no similar restraint. [231] In *Randolph*, Scott Randolph was present and arguing with his estranged wife, Janet Randolph, when she "readily gave" consent to search for Scott's "items of drug evidence" in their house. [232] Relying on Janet's consent, the officer recovered cocaine from the Randolph's bedroom. [233] The issue presented to the Court was whether a search based on third party consent is lawful "with the permission of one occupant when the other, who later seeks to suppress the evidence, is present at the scene and expressly refuses to consent." [234] *Randolph* held, "a physically present co-occupant's stated refusal to permit entry prevails, rendering the warrantless search unreasonable and invalid as to him." [235]

Randolph based its ruling on "widely shared social expectations." [236] Society's understanding about who possesses the authority to consent to a particular search, while influenced by property law, is "not controlled by its rules." [237] Instead, social expectations about consent are "a function of commonly held understandings about the authority that co-inhabitants may exercise in ways that affect each other's interests." [238] *Randolph* elucidated its "commonly held understanding" concept through a series of examples. The Court first presented the societal expectations of *Matlock*:

> When someone comes to the door of a domestic dwelling with a baby at her hip, as Mrs. Graff did, she shows that she belongs there, and that fact standing alone is enough to tell a law enforcement officer or any other visitor that if she occupies the place along with others, she probably lives there subject to the assumption tenants usually make about their common authority ***131** when they share quarters. They understand that any one of them may admit visitors, with the consequence that a guest obnoxious to one may nevertheless be admitted in his absence by another. [239]

Matlock, in choosing to live in such an arrangement, assumed a risk that his cohabitant would invite others inside the home in his absence, an arrangement so typical that officers rightly could rely upon it without making inquiries into the possibility of some "eccentric scheme" to the contrary. [240] In contrast, *Randolph* noted that "no common authority could sensibly be suspected" for a landlord offering admission into an apartment without first seeking permission from the tenant or a hotel manager allowing entry into a room without asking for approval from the current hotel guest. [241] Moreover, an eight-year-old child, who could invite a "pollster or salesman" across the threshold of a home, could not allow rummaging "through his parents' bedroom." [242] Finally, a homeowner's authority to admit someone "over the objection of" his or her houseguest was limited because of the "customary expectation of courtesy or deference" shown a houseguest. [243] *Randolph* concluded, "there is no common understanding that one co-tenant generally has a right or authority to prevail over the express wishes of another, whether the issue is the color of the curtains or invitations to outsiders." [244]

The Court again considered a "disputed invitation" [245] in *Fernandez v. California*, a case in which Fernandez objected to an officer's entry by announcing, "You don't have any right to come in here. I know my rights." [246] Having probable cause that Fernandez had assaulted his domestic partner, police arrested him and took him to the station. [247] An officer then returned to Fernandez's residence, successfully gaining permission to search from his domestic partner, Rojas. [248] The resulting search recovered evidence linking Fernandez to a robbery. [249] While noting ***132** that a caller would have "no confidence" in one occupant's invitation if a co-occupant was present and objecting, *Fernandez* believed that the calculus "would be quite different"

if "the objecting tenant was not standing at the door."[250] With the objecting occupant absent, "the friend or visitor is much more likely to accept the invitation to enter."[251] *Fernandez* thus adhered to the social norms analysis developed in *Randolph*.

If the Court applied only *Matlock's* "assumption of risk" test, it would provide inadequate answers for those whose relatives have uploaded DNA onto genealogical websites.[252] When a person shares his or her genetic information with an open source site, such as GEDmatch, this individual makes a privacy decision for his or her whole family.[253] The GEDmatch user forfeits "the genetic privacy of an entire family for generations,"[254] destroying the privacy both of relatives unknown and unborn. *Matlock's* reliance on "mutual use" would fail family members because even though two distant relatives may both possess certain segments of information in their chromosomes, such "mutual use" would fail to establish the "common authority" envisioned by the Court.[255] Rather than making a conscious choice to share a particular piece of property, relatives having the same portion of DNA instead share information--without any volitional decision. Also, unlike *Matlock's* shared bedroom, mutual use does not provide "joint control," as each relative "uses" his or her genome separately and automatically, through biological processes, without input from any other family member.[256] This lack of interaction among mutual users denies any opportunity to negotiate the terms of privacy. Since the transmission of DNA by birth is a wholly programmed process, common possessors of DNA could not be said to have "assumed the risk" that, in the involuntary "act" of sharing genes with family, any particular member has ***133** consciously chosen to allow another to expose shared information.[257] Since *Matlock's* underlying assumptions do not apply in the genetic genealogy context, its reasoning lacks convincing force, and therefore the case offers little guidance to the Court regarding government visits to genealogical sites.

In the face of *Matlock's* inadequacy in assessing genetic genealogy, the Court could turn to *Randolph* and *Fernandez*. However, as currently applied, *Randolph's* and *Fernandez's* objecting occupant would not clarify genealogical privacy issues. Considering "widely shared social expectations," *Randolph* bridled at the thought of overriding a physically present co-occupant's refusal to allow entry.[258] In contrast, *Fernandez* considered the situation "quite different" when an objecting tenant failed to be "standing at the door."[259] Since each of us has an untold number of relatives who could access genealogical sites at any time and any place on the globe, we cannot be ever-present at each computer a relative is using to access the Internet. All of us would inevitably be an absent occupant in most places and at most times. Under *Fernandez*, our absence at each genealogical site "door" upon which the government knocked when exploring DNA would deny us a right to privacy. Given the lack of an actual objection, the Court would simply return to the absent--and silent--cohabitant originally considered in *Matlock*.

To adequately address third party consent in the genetic genealogy context, the Court would need to refine *Randolph's* "widely shared social expectations" test for *Matlock's* absent and un-objecting mutual user context.[260] While *Randolph* did apply its societal expectations test to *Matlock's* facts, it concluded that an occupant could admit an "obnoxious" visitor in the cohabitant's absence.[261] Given the inability of an individual to be at every door the government might open by visiting a genealogy site, *Randolph's* willingness to admit every obnoxious visitor might be strained to the breaking point.

A flat rejection of *Randolph's* conclusion, however, would not alone identify the "widely shared social expectations" about genealogy sites.[262] There is a difficulty in analyzing social expectations in this context, due to the recent advent of genealogy sites. GEDmatch began operations as late as ***134** 2010.[263] Such newness has not allowed for a full societal consensus to emerge. In contrast, the rights of the homeowner have been understood with relative certainty since 1603, when articulated in *Semayne's Case*.[264] Further, a "consensus" has not even been formed in individual minds, if one considers the inconsistent behavior of persons using the Internet. Often people will blithely give up privacy by clicking "agree" to myriad privacy policies they have chosen not to read. When privacy invasions make the news, however, these same persons can be brought up short by the intrusiveness of an incursion. Peter Neufeld of The Innocence Project has noted, "There is a whole generation that says, 'I don't really care about privacy," until "there is a Cambridge Analytica."[265] Neufeld continued, "No one has thought about what are the possible consequences."[266] This same dynamic could play out with genealogy sites. Focused on the immediate goal of tracking down a lost relative, persons might not see the long view which, had they pondered it, could appall them.

If, with the passage of time, persons did pause to consider the privacy concerns of genetic genealogy, most would likely not expect that their relatives, however distant or unknown, could permit entry into something as "deeply revealing" as DNA.[267] It is one thing to enable another person to allow exploration of the privacy of a shared home. It is quite another to permit

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

investigation into the privacy of shared genes. Although the issue has not had time to fully cohere, "widely shared social expectations" will likely forbid one person giving the government permission to use shared DNA against a relative.

***135 D. If the Court Characterizes Law Enforcement's Use of Genealogical Sites as a Government Search that Occurred after a Private Intrusion, the Lawfulness of the Official Search Will Be Assessed in Reference to the Scope of the Earlier Private Search**

Suppose your neighbor, hoping to borrow a cup of sugar, enters the cupboard of your unlocked home without permission while you are away. Suppose further that your neighbor, looking in your bag of sugar, finds powder cocaine, of which he promptly tells the police. Nothing stops law enforcement from taking and using that knowledge about the cocaine's existence. Once a secret is out in the open, it can no longer be a secret; any privacy interest in that bit of information is dead.

Therefore, the Court has determined that an invasion of privacy by an individual citizen can have Fourth Amendment consequences on a later government search. In *Walter v. United States*, packages containing 871 boxes of sexually explicit 8-millimeter films were delivered to the wrong address, the hosiery company, L'Eggs Products, Inc.[268] When employees at the company opened the packages, they found on the boxes within "suggestive drawings" and "explicit descriptions of the contents."[269] They alerted the FBI to their find, causing agents to pick up the films and view them with a projector.[270] As a result, the federal government charged the defendant with interstate transportation of obscene films.[271] The *Walter* Court thus confronted the issue of "whether the Fourth Amendment required the agents to obtain a warrant before they screened the films."[272]

In considering the case, *Walter* noted that no Fourth Amendment violation occurred when the L'Eggs employees themselves opened the packages because "a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment."[273] Further, the "private wrongdoing" did not "deprive the government of the right to use evidence ***136** that it ha(d) acquired lawfully."[274] *Walter* measured the reasonableness of the government intrusion by reference to the earlier private invasion, noting that nothing was wrongful about the government's examination of the packages' contents "to the extent that they had already been examined by third parties."[275] Noting the evils of the "indiscriminate searches" performed under general warrants, *Walter* declared that any authorized search was "limited by the particular terms of its authorization."[276] In like manner, a private party's "invasion of another person's privacy" limited a later official search.[277] While the government could reexamine the materials previously viewed by private persons, it could not "exceed the scope" of the prior private search without independent justification.[278] Essentially, "the legality of the governmental search" had to be "tested by the scope of the antecedent private search."[279]

In *Walter*, the private search was limited, involving only the opening of the package to reveal the explicit drawings and pictures on the boxes inside, while the FBI's intrusion was more invasive, including the watching of the actual films.[280] Therefore, the earlier private search only frustrated the defendant's reasonable privacy expectations "in part;" it "did not simply strip the remaining unfrustrated portion of that expectation of all Fourth Amendment protection."[281] Ultimately, *Walter* ruled that since "the additional search conducted by the FBI--the screening of the films-- was not supported by any justification," it violated the Fourth Amendment.[282]

Package problems were the focus of the Court's next private party search case, *United States. v. Jacobsen*.[283] In *Jacobsen*, Federal Express employees, pursuant to company policy regarding insurance claims, examined "an ordinary cardboard box wrapped in brown paper" that was "torn by a forklift."[284] Inside the box, employees found a 10-inch long duct-tape tube, which they opened, finding plastic bags of white powder.[285] ***137** Replacing the bags in the tube and the tube into the box, the employees then alerted the Drug Enforcement Administration (DEA).[286] Upon arrival the DEA agent:

> saw that one end of the tube had been slit open; he removed the four plastic bags from the tube and saw the white powder. He then opened each of the four bags and removed a trace of the white substance with a knife blade. A field test made on the spot identified the substance as cocaine.[287]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

The Court in *Jacobsen* adopted the reasoning it applied in *Walter*. *Jacobsen*, noting that Federal Express employees cut the tube and exposed the white powder, declared, "Whether those invasions were accidental or deliberate, and whether they were reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character." [288] The DEA's "additional invasions" had to be "tested by the degree to which they exceeded the scope of the private search." [289] If the DEA did not move beyond the private invasion, then there was no Fourth Amendment violation. [290] Since the defendant could not complain about a frustration of privacy expectations by a private party, the government was welcome to use the "now-nonprivate information." [291] If instead the DEA intruded beyond Federal Express's initial invasion, then the Fourth Amendment was triggered "with respect to which the expectation of privacy has not already been frustrated." [292]

Jacobsen then specified two distinct intrusions the DEA committed: 1) the DEA agents "removed the tube from the box, the plastic bags from the tube and a trace of powder from the innermost bag," and 2) they "made a chemical test of the powder." [293] The DEA's first intrusion involving opening the package and picking up the tube gave the government no information it had not learned from the Federal Express employees. [294] The ***138** defendants "could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to their offices for the express purpose of viewing its contents." [295] Likewise, the DEA's removal of the bags from the tube and visually inspecting them "enabled the agent to learn nothing that had not previously been learned during the private search." [296]

The Court also analyzed the DEA's second intrusion "occasioned by the field test, which had not been conducted by the Federal Express agents and therefore exceeded the scope of the private search." [297] Since a Fourth Amendment search required government intrusion on a privacy expectation that was "reasonable"--or "legitimate"--*Jacobsen* viewed the field test intrusion through the prism of what interests could be considered "legitimate." [298] Society need not recognize as "legitimate" information regarding "wrongful" behavior, such as burglar's presence in an empty cabin. [299] The DEA's "chemical test," which merely disclosed the existence of cocaine--a substance illegal to possess--did not implicate "any legitimate interest in privacy." [300]

Thus, *Walter* and *Jacobsen's* key point was that the amount of Fourth Amendment protection from a government intrusion depended on the scope of any earlier private invasion. *Walter* only found fault when the FBI went beyond the prior private search--opening the package and viewing the explicit drawings and pictures on the boxes within them--by actually watching the films. [301] In short, the test was framed by the extent of the "the antecedent private search." [302] This analysis could open a path to admission for evidence from genetic genealogical sites. When a person, on his or her own initiative, provides a saliva sample to a commercial site, such as 23andMe, and then uploads the results to an open genealogical site, such as GEDmatch, the individual is essentially exposing the portions of his or her DNA shared with relatives. Much as *Walter's* L'Eggs employees opened the package or *Jacobsen's* Federal Express employees cut the tube, the individual family member uploading his genetic information tears open ***139** segments of the DNA of all of his or her relatives to public view. When investigators later obtain this genetic information from GEDmatch, this initial collection itself goes no further than the original "antecedent private search." [303]

The only question remaining is whether government use of the DNA information in forming family trees and in comparing genes with crime scene samples amounts to a further official intrusion akin to the FBI watching the film from the opened box in *Walter*. [304] The investigation techniques used to locate the Golden State Killer suspect after visiting GEDmatch do not seem likely to be considered further intrusions on par with viewing the film in *Walter*. Hole's subsequent investigation in pursuit of DeAngelo involved only old-fashioned gumshoe detective work into public information. Reviews of census records, gravesite locators, and old newspaper obituaries involve only the examination of information available to anyone wishing to view it. [305] The "antecedent private search" precedent could thus provide law enforcement with a door through which it might get genetic genealogy evidence admitted despite the lack of a warrant.

Any person challenging evidence from a relative that the government has obtained from a genealogical site will have to establish "standing," or the personal right to challenge the particular Fourth Amendment violation.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Suppose the government acknowledged that its search for the Golden State Killer suspect's distant relative on a genealogical site violated the Fourth Amendment. Would such concession help the suspect exclude the results of this genealogical search from court? It could be argued that the person who could claim invasion of privacy from the genealogical visit is not the suspect but the relative who's DNA was the subject of state scrutiny. Any link to the suspect came only from DNA the suspect left--or essentially abandoned--at the crime scene as semen, blood, or other biological material. As previously noted, the later tracing from a distant relative's common ancestor--the great, great, great, grandparent--involved [306] traditional types of investigation, such as looking at gravesites ***140** and checking newspapers and census records, [307] which would raise no Fourth Amendment red flags. This issue, commonly referred to as "standing," [308] involves the question of who precisely has the right to contest a particular Fourth Amendment violation. [309]

One of the most significant cases on the issue of "standing," or the right to contest a Fourth Amendment search, is *Rakas v. Illinois*, a case which altered even the language employed in this area of the law. [310] In *Rakas*, officers, suspecting a stopped car of being involved in a robbery, ordered its occupants out of the vehicle. [311] When Rakas and two others then exited the vehicle, the officers searched the car, discovering "a box of rifle shells in the glove compartment, which had been locked, and a sawed-off rifle under the front passenger seat." [312] Rakas moved to suppress these items as recovered during an unlawful search. [313] The trial court ruled Rakas lacked standing to contest the search because he, being merely a passenger, did not own the car and further did not claim ownership of the gun or shells. [314]

Rakas described the "concept of standing" as focusing on "whether the person seeking to challenge the legality of a search as a basis for suppressing evidence was himself the 'victim' of the search or seizure." [315] "Standing" involved two questions: "first, whether the proponent of a particular legal right has alleged "injury in fact," and, second, whether the proponent is asserting his own legal rights and interests rather than basing his claim for relief upon the rights of third parties." [316] *Rakas*, however, was less than pleased with the "'standing' terminology" [317] because such language caused the issue to be falsely seen as "theoretically distinct from the merits of a defendant's Fourth Amendment claim." [318] The Court concluded that the "definition" of Fourth Amendment rights was "more ***141** properly placed within the purview of substantive Fourth Amendment law than within that of standing." [319]

Rakas deemed Fourth Amendment rights as "personal rights" that could "not be vicariously asserted." [320] The Court ruled, "A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed. [321] Only those "whose Fourth Amendment rights have been violated" could seek exclusion of the evidence obtained from that violation. [322] Rakas contested the search of the glove compartment and the space under the car's seat, yet he did not claim that he had "any legitimate expectation of privacy" in these areas. [323] Lacking a reasonable privacy expectation, Rakas necessarily lacked a Fourth Amendment right in the car, and therefore could not contest the police illegality. In terms that Rakas would have disapproved, he lacked "standing" to claim the officer's search of the car violated his Fourth Amendment rights.

In the next case involving the right to contest a search of a vehicle, *Byrd v. United States*, the Court had mellowed its stance on the terminology of "standing" by noting, "The concept of standing in Fourth Amendment cases can be a useful shorthand for capturing the idea that a person must have a cognizable Fourth Amendment interest in the place searched before seeking relief for an unconstitutional search." [324] In *Byrd*, Terrence Byrd and Latasha Reed drove in Byrd's Honda to Budget car rental in New Jersey. Reed then entered the agency and rented a car while Byrd stayed outside in his Honda. After signing a rental contract that explicitly provided, "PERMITTING AN UNAUTHORIZED DRIVER TO OPERATE THE VEHICLE IS A VIOLATION OF THE RENTAL AGREEMENT," Reed handed the rental's keys to Byrd, who drove off in the rental car. [325] Later, a Pennsylvania trooper stopped Byrd as he was driving the rental car to Pittsburgh. [326] The officer noticed when he approached the car, Byrd was so nervous that he "was shaking and had a ***142** hard time obtaining his driver's license." [327] Another officer then arrived at the scene. [328] When the troopers learned Byrd was not listed as an authorized driver on the rental agreement, they told him they could search the car without consent. The resulting search of the car's trunk revealed "body armor and 49 bricks of heroin," exposing Byrd to federal drug charges. [329]

When presented with this case, the *Byrd* Court asked, "Does a driver of a rental car have a reasonable expectation of privacy in the car when he or she is not listed as an authorized driver on the rental agreement?" [330] While noting that the legitimacy of privacy expectations "must have a source outside of the Fourth Amendment," *Byrd* identified two such sources: 1) "concepts of real or personal property law," and 2) "understandings that are recognized and permitted by society." [331] Relying on the "general property-based concept," the Court determined that Byrd was the "sole occupant" of the car and therefore "could exclude others from it." [332] *Byrd* declared, "one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of [the] right to exclude." [333] Acknowledging that Byrd "violated the rental agreement," the Court dismissed this fact because, "As anyone who has rented a car knows, car-rental agreements are filled with long lists of restrictions." [334] "Few would contend," urged the Court, that violating such provisions as driving on an unpaved road or while holding a cellphone, "has anything to do with a driver's reasonable expectation of privacy in the rental car." [335] *Byrd* therefore held, "the mere fact that a driver in lawful possession or control of a rental car is not listed on the rental agreement will not defeat his or her otherwise reasonable expectation of privacy." [336]

***143** *Byrd*, in applying property law principles to determine whether a person possessed the reasonable expectation of privacy to contest a search, offered another test that could be used to consider the admissibility of evidence obtained from genealogy sites. Through *Byrd's* lens, asking whether a person has standing to challenge a government visit of a family member's genealogy site amounts to inquiring whether that person has a property right enabling him or her to exclude others from the site. The design and operation of GEDmatch undermines any such ability to exclude. In its "Terms of Service and Privacy Policy," GEDmatch alerts potential users, "GEDmatch exists to provide DNA and genealogy tools for comparison and research purposes." [337] The comparison and research that GEDmatch mentions are collaborative processes that can only work by sharing information. The sites' very existence, along with the million uploads made on it, demonstrate the inability to exclude others. [338] GEDmatch further notes, "DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this Site agree that their information will be shared with other users." [339] The site's terms of service, in twice explicitly referencing sharing, again show a lack of property interest by a relative in excluding others. Finally, GEDmatch explains, "Raw DNA data uploaded to GEDmatch.Com ('Raw Data') remains the property of the person who uploaded it." [340] In this statement, the only property interest GEDmatch acknowledges is that of the person uploading the DNA, not the relatives who might contest the viewing of it. Under *Byrd's* "general property-based concept," without a right to exclude, one has no property interest, without a property interest, one has no reasonable expectation of privacy, and without such a privacy expectation, one has no standing. [341] Since a relative cannot exclude others from GEDmatch's site, his or her standing fails at the outset.

***144 Conclusion**

Facing the daunting realization that there are "200,000-plus cold cases in the United States," Kenneth Mains, "founder of the American Investigative Society of Cold Cases," has argued that any resource which helps close such cases "needs to be utilized." [342] The National District Attorneys Association's Josh Marquis wondered, "Why in God's name would we come up with a reason that we are not able to use" these genetic websites? [343] While law enforcement is keenly aware of the potential "investigative goldmine" of these databases, the persons who use them "aren't really thinking through the implications of creating this treasure trove of data that can be mined." [344] University of Michigan law professor Barbara McQuade has noted that for most people, DNA is so "very private, very personal" that "even if you have given it up to one of these third-party services, maybe there should be a higher level of security." [345] There thus exists a gap between the perceptions of investigators zealously pursuing criminals and laypersons who have not considered the full consequences of this rapidly advancing technology. It is in this gap that Fourth Amendment rights, not fully appreciated by those using genealogical websites, might fall.

Further, full privacy protection from government use of genetic genealogy might be beyond the volitional power of any one individual. Those who, after educating themselves on every aspect of genealogical privacy, choose to forgo uploading their own DNA, might still find their genetic information probed by the government. "Even if we've never spit into a test tube, some of our genetic information may be public--and accessible to law enforcement." [346] There is no getting around the fact that any person, upon submitting DNA information to a public genealogy site, exposes the DNA of his or her relatives, even if "distant" or "far flung." [347] This breach occurs regardless of the consent or even the knowledge of thousands.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

If confronted with the Fourth Amendment issues of genetic genealogy, the Court could address the concerns created by this new technology in a variety of ways. The Court could turn to its earlier case ***145** involving DNA collection of arrestees entering custody, *Maryland v. King*. Such an approach would bear so little fruit, due to the narrowness of *King's* ruling, that the Court would have to craft a new rule for the entirely separate issue of government collection of DNA information on the Internet. [348] The Court could analyze genetic genealogy's privacy issues by considering *Carpenter's* latest application of the third-party doctrine. [349] The force of *Carpenter's* reasoning would likely cause the Court to view genetic genealogy as so sophisticated and the information it handled as so sensitive that a government visit to a genealogy site would be deemed a Fourth Amendment search requiring a warrant. [350] The Court could consider a person's uploading of DNA information as amounting to a grant of consent to search the portions of his or her genome held in common with relatives. Then, the third-party consent precedent's "widely shared social expectations" would likely reject government use of DNA information without a warrant. [351] Two other Fourth Amendment doctrines, *Walter* and *Jacobsen's* "antecedent private search" rule [352] and *Byrd's* "general property-based concept" definition of standing, offer law enforcement with potential avenues for admission of genetic genealogy evidence. [353] Should the Court deem a person's upload of DNA information onto a genealogy site to be a prior private search, then *Walter* and *Jacobsen* would permit the government to explore this same genetic information--previously exposed by a private person--without a warrant. Finally, following *Byrd's* reasoning, the government could avoid the exclusion of evidence obtained in visiting a genealogy site even if the warrantless download of genetic information was found to violate the Fourth Amendment. Since the family member could not exclude others from visiting the genealogy site, he or she could not establish a property interest sufficient to support standing to challenge the search in the first place. [354] The Court's decision about the Fourth Amendment reasonableness of warrantless government collection of genetic information from genealogy sites will thus turn on how it chooses to frame the question triggered by this new technology. When it comes to genetic genealogy, as with much else in the world of heredity, where you end up all depends on where you start.

Footnotes

1 Ray Sanchez, Elizabeth I. Johnson, Steve Almasy & Alanne Orjoux, *After Searching for more than 40 Years, Authorities Say an Ex-cop Is the Golden State Killer*, CNN (Apr. 27, 2018, 10:44 AM), https://www.cnn.com/2018/04/25/us/golden-state-killer-development/index.html.

2 Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-great-great Grandparents*, WASH. POST (Apr. 30, 2018), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html?utm_term=.26202e9e14a4.

3 Sarah Zhang, *How a Genealogy Website Led to the Alleged Golden State Killer: Powerful Tools are Now Available to Anyone Who Wants to Look for a DNA Match, Which Has Troubling Privacy Implications*, THE ATLANTIC (Apr. 27, 2018), https://www.theatlantic.com/science/archive/2018/04/golden-state-killer-east-area-rapist-dna-genealogy/559070/.

4 Jouvenal, *supra* note 2.

5 *Id.*

6 Sanchez et al., *supra* note 1.

7 Aja Romano, *DNA Profiles from Ancestry Websites Helped Identify the Golden State Killer Suspect: He Wasn't the First Criminal to Fall to Familial DNA Matching, and He Won't Be the Last*, VOX (Apr. 27, 2018, 5:20 PM), https://www.vox.com/2018/4/27/17290288/golden-state-killer-joseph-james-deangelo-dna-profile-match.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

8 Jouvenal, *supra* note 2.

9 Zhang, *supra* note 3.

10 Jouvenal, *supra* note 2.

11 Sanchez et al., *supra* note 1.

12 Jouvenal, *supra* note 2.

13 *Id.*

14 Joseph Serna, Richard Winton & Sarah Parvini, *As a Young Cop, Golden State Killer Suspect Was Aloof, Ambitious, 'Always Serious,'* L.A. TIMES (May 1, 2018, 3:00 AM), http://www.latimes.com/local/lanow/la-me-golden-state-cops-20180501-story.html.

15 Jouvenal, *supra* note 2.

16 Serna et al., *supra* note 14.

17 Kyle Swenson, *Undercover Cops Grabbed a DJ's Chewing Gum. It Helped Crack a Teacher's 1992 Murder, Police Say*, WASH. POST (June 26, 2018), https://www.washingtonpost.com/news/morning-mix/wp/2018/06/26/undercover-cops-grabbed-a-djs-chewing-gum-it-helped-crack-a-teachers-1992-murder-police-say/?utm_term=.7abdb34dabac; *April Tinsley: DNA Snares Man in Indiana Girl's 1988 Murder,* BBC NEWS (July 16, 2018), https://www.bbc.com/news/world-us-canada-44851825.

18 The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

19 Maryland v. King, 569 U.S. 435, 442 (2013).

20 Maggie Fox, *What You're Giving Away with Those Home DNA Tests: It's the Most Valuable Thing You Own*, NBC NEWS (Nov. 29, 2017, 6:46 AM), https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776.

21 *Id.*; *see also* Patrick Cain, *Privacy Risks Lurk in DNA Tests, Experts Warn*, GLOBAL NEWS (Aug. 15, 2016, 7:00 AM), https://globalnews.ca/news/2879276/privacy-risks-lurk-in-dna-tests-experts-warn/.

22 Fox, *supra* note 20.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

23 *Id.*; *see also* Cain, *supra* note 21.

24 Maryland v. King, 569 U.S. 435 (2013).

25 Carpenter v. United States, 138 S. Ct. 2206 (2018).

26 Byrd v. United States, 138 S. Ct. 1518 (2018).

27 U.S. CONST. amend. IV.

28 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Court has defined "searches" in two ways: (1) as a government intrusion on a person's reasonable expectation of privacy as defined in *Katz*, and (2) as a physical occupation of private property for purposes of gaining information as defined in *United States v. Jones*, 565 U.S. 400, 404-05 (2012). *Jones* explained, "The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.* As there is no evidence in the Golden State Killer case that government officials physically visited genealogical organizations to collect information, *Jones'* physical occupation test is beyond the scope of this article. For the same reason, the analysis of Fourth Amendment "seizures" is beyond the scope of this article.

29 *Katz*, 389 U.S. at 348.

30 *Id.*

31 *Id.*

32 *Id.* at 350-51.

33 *Id.* at 351.

34 *Id.* at 361 (Harlan, J., concurring).

35 Michigan v. Clifford, 464 U.S. 287, 292 (1984).

36 United States v. Dunn, 480 U.S. 294, 298 (1987).

37 Maryland v. Macon, 472 U.S. 463, 469 (1985).

38 Bond v. United States, 529 U.S. 334, 338-39 (2000).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

39 Smith v. Maryland, 442 U.S. 735, 739 (1979).

40 In a pertinent part, the Fourth Amendment provides, "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." U.S. CONST. amend. IV.

41 Riley v. California, 134 S. Ct. 2473, 2482 (2014).

42 Chimel v. California, 395 U.S. 752, 765 (1969).

43 *Id.* at 761.

44 *Id.*

45 Kentucky v. King, 563 U.S. 452, 459 (2011).

46 *Riley*, 134 S. Ct. at 2840-41.

47 *Id.* at 2495.

48 *Id.* at 2482.

49 *Id.*

50 Carpenter v. United States, 138 S. Ct. 2206, 2221, 201 L. Ed. 2d 507 (2018).

51 *Id.* at 2213. The *Carpenter* Court reiterated, "we have held that official intrusion into (a reasonable expectation of privacy) generally qualifies as a search and requires a warrant supported by probable cause." *Id.*

52 Agnello v. United States, 269 U.S. 20, 33 (1925).

53 Avi Selk, *The Most Disturbing Parts of the 171-page Warrant for the Golden States Killer Suspect*, WASH. POST (June 2, 2018), https://www.washingtonpost.com/news/post-nation/wp/2018/06/02/the-most-disturbing-parts-of-the-171-page-warrants-for-the-golden-state-killer-suspect/?utm_term=.d4870987d966. The search warrant affidavits for this case can be viewed at: http://www.sacda.org/files/9415/2789/1272/P_v_DeAngelo_Redacted_Search_Warrant_Final.pdf [hereinafter Search Warrant].

54 *Id.*

55 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

56 Sanchez et al., *supra* note 1.

57 Matthias Gafni, *Here's the 'Open Source' Genealogy Website that Helped Crack the Golden State Killer Case*, MERCURY NEWS (Apr. 26, 2018), https://www.mercurynews.com/2018/04/26/ancestry-23andme-deny-assisting-law-enforcement-in-east-area-rapist-case/.

58 *Id.*

59 *Id.*

60 *Id.*; Richard Winton, Tracey Lien, Paige St. John & Benjamin Oreskes, *The First Step in Finding Golden State Killer Suspect: Finding His Great-great-great-grandparents on Genealogy Site*, L.A. TIMES (Apr. 27, 2018), http://www.latimes.com/local/lanow/la-me-golden-state-dna-match-20180427-story.html.

61 Gafni, *supra* note 57.

62 Justin Jouvenal, Mark Berman, Drew Harwell & Tom Jackman, *Data on a Genealogy Site Led Police to the 'Golden State Killer' Suspect. Now Others Worry About a 'Treasure Trove of Data,'* WASH. POST (Apr. 27, 2018), https://www.washingtonpost.com/news/post-nation/wp/2018/04/27/data-on-a-genealogy-site-led-police-to-the-golden-state-killer-suspect-now-others-worry-about-a-treasure-trove-of-data/?utm_term=.ff16e1d38bab.

63 Zhang, *supra* note 3.

64 Emily Shapiro, *What to Know About the Privacy of Your DNA in Wake of 'Golden State Killer' Suspect's Arrest*, ABC NEWS (Apr. 30, 2018), https://abcnews.go.com/US/privacy-dna-wake-golden-state-killer-suspects-arrest/story?id=54777919.

65 *Id.*

66 Gina Kolata & Heather Murphy, *The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html.

67 Jouvenal et al., *supra* note 62. In contrast, "23andMe has more than 5 million customers, and Ancestry.com has 10 million." Kolata, *supra* note 66.

68 Gafni, *supra* note 57.

69 *Id.*

70 *Id.*

71 Ailsa Chang & Adhiti Bandlamudi, *Tactics Used To Find Golden State Killer Raise Privacy and Legal Questions*, NATIONAL PUBLIC RADIO (Apr. 27, 2018), https://www.npr.org/2018/04/27/606580162/tactics-used-to-find-golden-state-killer-raise-privacy-and-legal-questions.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

72 Winton, *supra* note 60. The discovery of this DNA sample was due to the diligence of a "meticulous pathologist" who had put "a duplicate evidence kit" in a freezer in 1980. Jouvenal, *supra* note 2. "Many other DNA samples from the case had been depleted over the years." *Id.*

73 Jouvenal, *supra* note 2.

74 *Id.*

75 Winton, *supra* note 60.

76 *Id.*; Jouvenal, *supra* note 2.

77 Jouvenal, *supra* note 2.

78 *Id.*

79 Ryan Lillis, *Here's the Inside Story of How Police Nabbed the East Area Rapist Suspect*, SACRAMENTO BEE (Apr. 29, 2018), http://www.sacbee.com/news/local/crime/article210003114.html.

80 *Id.*

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

85 Paige St. John et al., *DNA Lifted From Golden State Killer Suspect at Hobby Lobby Parking Lot Key to Cracking Case, Documents Show*, L.A. TIMES (June 1, 2018), http://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-deangelo-warrant-20180601-story.html.

86 *Id.*

87 *Id.*

88 *Id.*

89 Search Warrant, *supra* note 53, at 42.

90 Swenson, *supra* note 17.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

91 *Id.*

92 *Id.*

93 *Id.*

94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.* Investigators have also used forensic genealogy to identify victims of crime. Margaret Press and Colleen Fitzpatrick, co-founders of the DNA Doe Project, gave a name to a victim of a 37-year-old homicide case in four hours. Seth Augenstein, *Buck Skin Girl Case Break Is Success of New DNA Doe Project,* FORENSIC MAGAZINE (Apr. 16, 2018), https://www.forensicmag.com/news/2018/04/buck-skin-girl-case-break-success-new-dna-doe-project. In this case, which also relied on GEDmatch, Detective Steve Hickey of the Miami County Sheriff's Department stated this development created "an active homicide investigation." *Id.*

99 April Tinsley: DNA Snares Man in Indiana Girl's 1988 Murder, *supra* note 17.

100 *Id.*

101 *Id.*

102 *Id.*

103 *Id.*

104 *Id.*

105 *Id.*

106 *King*, 569 U.S. at 442.

107 *Id.*

108 *Id.* at 439.

109 *Id.* at 440, 444.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

110 *Id.* at 440.

111 *Id.* at 441, 443.

112 *Id.* at 443.

113 *Id.* at 444.

114 *Id.*

115 *Id.* at 441.

116 *Id.* at 444.

117 *Id.* at 444-45.

118 *Id.* at 445.

119 *Id.* at 465-66.

120 *Id.* at 447.

121 The Court explained, "[W]e balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." *Id.* at 448. *King* also noted, "This application of 'traditional standards of reasonableness' requires a court to weigh 'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy.'" *Id.* at 448.

122 *Id.* at 449-456. *King* concluded, "In the balance of reasonableness required by the Fourth Amendment, therefore, the Court must give great weight both to the significant government interest at stake in the identification of arrestees and to the unmatched potential of DNA identification to serve that interest." *Id.* at 461.

123 *Id.* at 461-464. *King* ruled, "The expectations of privacy of an individual taken into police custody "necessarily [are] of a diminished scope." *Id.* at 462.

124 *Id.* at 449-50.

125 *Id.* at 450.

126 *Id.*

127 *Id.* at 452.

128 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

129 *Id.* at 452-53.

130 *Id.* at 453.

131 *Id.* at 455.

132 *Id.* at 461.

133 *Id. King* described a buccal swab DNA sample as a "gentle rub along the inside of the cheek" that "does not break the skin." *Id.* at 463-64. The sample involved "virtually no risk, trauma, or pain." *Id.*

134 *Id.* at 464.

135 *Id.*

136 *Id.* at 442-43.

137 *Id.* at 464. Unfortunately, this information was outdated when the Court made its ruling, for scientists already knew even before the *King* opinion that "[S]pecific DNA once dismissed as junk plays an important role in brain development and might be involved in several devastating neurological diseases." Jeffrey Norris, *Brain Development Is Guided by Junk DNA that Isn't Really Junk*, UCSF (Apr. 15, 2013), https://www.ucsf.edu/news/2013/04/105126/brain-development-guided-junk-dna-isn%E2%C80%99t-really-junk. While the Norris article is dated April 15, 2013, the Court decided *King* on June 3, 2013. Any information of a genetic predisposition for a "devastating" neurological disease, in light of the possible consequences for such practical matters as insurance and employment, could rightly be seen as highly personal and sensitive.

138 *King*, 569 U.S. at 462.

139 *Id.*

140 *Id.* at 463.

141 *Id.*

142 *Id.* at 464-65.

143 *Id.* at 465.

144 *Id.* at 465-66.

145 *Id.* at 449

146 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

147 *Id.*

148 *Id.* at 449-50.

149 *Id.* at 452.

150 *Id.* at 452-53.

151 *Id.* at 453.

152 *Id.* at 462.

153 *Id.* at 463.

154 *Id.* at 441.

155 United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

156 *Id.* at 351.

157 *Id.*

158 *Jones*, 565 U.S. at 417.

159 United States v. Dionisio, 410 U.S. 1, 13-14 (1973).

160 *Id.* at 14.

161 United States v. Miller, 425 U.S. 435, 444 (1976).

162 *Id.* at 436.

163 *Id.* at 438, 440.

164 *Id.* at 443.

165 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

166 Smith v. Maryland, 442 U.S. 735 (1979).

167 *Id.* at 742.

168 *Id.* at 737, 744.

169 *Id.* at 743-44.

170 California v. Greenwood, 486 U.S. 35 (1988).

171 *Id.* at 37-38, 40.

172 *Id.* at 40.

173 *Id.*

174 *Id.* at 41.

175 *Carpenter v. United States*, 138 S. Ct. 2212 (2018).

176 *Id.* The level of suspicion needed to support the court orders was "specific and articulable facts showing that there are reasonable grounds to believe." *Id.* Such reasonable suspicion falls short of the Fourth Amendment requirement of probable cause for a warrant. U.S. CONST. amend. IV.

177 *Id.*

178 *Id.*

179 *Id.* at 2211.

180 *Id.*

181 *Id.* at 2211, 2212.

182 *Id.* at 2212.

183 *Id.*

184 *Id.* at 2216.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

185 *Id.*

186 *Id.*

187 *Id.*

188 *Id.*

189 *Id.*

190 *Id.*

191 *Id.* at 2219.

192 *Id.*

193 *Id.* at 2217.

194 *Id.* at 2218.

195 *Id.*

196 *Id.* at 2219.

197 *King*, 569 U.S. at 442.

198 Jouvenal et al., *supra* note 62.

199 Shapiro, *supra* note 64.

200 *Carpenter*, 138 S. Ct. at 2218.

201 *Id.*

202 *Id.* at 2223.

203 Susan Donaldson James, *Thrill-Seeking Gene Can Lead to More Sex Partners*, ABC NEWS (Dec. 6, 2010), https://abcnews.go.com/Health/scientists-discover-gene-responsible-cheating-promiscuous-sex-habits/story?id=12322891 ("[A]bout half of all people have a gene that makes them more vulnerable to promiscuity and cheating."). Julia Rosen, *About Half of Kids' Learning Ability Is in Their DNA, Study Says*, L.A. TIMES (July 11, 2014), http://www.latimes.com/science/sciencenow/la-sci-sn-math-reading-genes-20140711-story.html ("[A]pproximately half of False children's math and reading ability stemmed from their genetic makeup."). Melissa Hogenboom, *Two Genes*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Linked with Violent Crime, BBC NEWS (Oct. 28, 2014), https://www.bbc.com/news/science-environment-29760212 ("A genetic analysis of almost 900 offenders in Finland has revealed two genes associated with violent crime.").

204 *Carpenter*, 138 S. Ct. at 2219.

205 *Id.* at 2223.

206 *Id.* at 2212.

207 James Randerson, *What DNA Can Tell Us: Genes Alone Cannot Account for What a Person Is, But Even the Slightest Distinguishing Traits Between People Can be Attributed to Individual Genes*, THE GUARDIAN (Apr. 26, 2008), https://www.theguardian.com/science/2008/apr/27/genetics.cancer.

208 *Id.*

209 *Carpenter*, 138 S. Ct. at 2223.

210 *Id.* at 2218.

211 *Id.* at 2210.

212 *Id.* at 2218.

213 *Id.*; Jouvenal, *supra* note 2. Further, certain language in *Carpenter* indicated that the Court might find the very purpose for which the government visited a genealogical site to be concerning. In downplaying the intrusiveness of Smith's pen registers, *Carpenter* noted that such "telephone call logs reveal little in the way of 'identifying information.'" *Id.* at 19. The entire purpose of examining genealogical data in the Golden State Killer case was to identify the Golden State Killer suspect--to name an individual as perpetrator.

214 Dow Chemical Co. v. United States, 476 U.S. 227, 238 (1986).

215 Kyllo v. United States, 533 U.S. 27, 33-34 (2001).

216 *Carpenter*, 138 S. Ct. at 2216.

217 *Id.* at 2223.

218 United States v. Matlock, 415 U.S. 164, 170 (1974).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

219 *Id.* at 166.

220 *Id.* at 179 (Douglas, J., dissenting).

221 *Id.* at 166.

222 *Id.*

223 *Id.* at 166-67.

224 *Id.* at 167.

225 *Id.* at 170.

226 *Id.* at 171, n. 7.

227 *Id.*

228 *Id.*

229 *Id.* at 175-76.

230 *Id.* at 179 (Douglas, J., dissenting).

231 Georgia v. Randolph, 547 U.S. 103 (2006).

232 *Id.* at 107.

233 Specifically, the officer found "a section of a drinking straw with a powdery residue he suspected was cocaine." *Id.*

234 *Id.* at 106.

235 *Id.*

236 *Id.* at 111.

237 *Id.*

238 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Privacy Statement

Last Updated: June 8, 2022

What you should know about privacy at 23andMe

At 23andMe, Privacy is in our DNA.

This Privacy Statement applies to all websites owned and operated by 23andMe, including www.23andme.com (https://www.23andme.com/), and any other websites, pages, features, or content we own or operate, and to your use of the 23andMe mobile app and any related Services.

To keep things simple, we use the same terms here as in our Terms of Service (https://www.23andme.com/about/tos/). We'll let you know in this Privacy Statement if we have a new or different definition for a term. You should read our entire Privacy Statement, but if you only have a few minutes you can take a look at this summary (https://www.23andme.com/privacy/).

The information 23andMe collects

We try not to speak in legalese, but there are some useful definitions we use to describe data we collect in providing the Services to you.

When we say **Personal Information**, we use this as a general term to refer to the different data categories we describe in this section that personally identify you. Your Personal Information can be either:

- **Individual-level Information:** information about a single individual, such as their genotypes, diseases or other traits or characteristics.
- **De-identified Information:** information that has been stripped of identifying data such that an individual cannot reasonably be identified.

Here are the types of information we collect:

- **Registration Information:** information you provide during account registration or when purchasing the Services, such as a name, user ID, password, date of birth, billing address, shipping address, payment information (e.g., credit card), account authentication information, or contact information (e.g., email, phone number).
- **Genetic Information:** information regarding your genotype (e.g., the As, Ts, Cs, and Gs at particular locations in your DNA). Genetic Information includes the 23andMe genetic data and reports provided to you as part of our Services.
- **Sample Information:** information regarding any sample, such as a saliva sample, that you submit for processing to be analyzed to provide you with Genetic Information, laboratory values or other data provided through our Services.
- **Self-Reported Information:** information you provide to 23andMe regarding your disease conditions, health-related information, traits, ethnicity, family history, or anything else you provide to us within our Service(s).
- **User Content:** information, data, text, software, music, audio, photographs, graphics, video, messages, or other materials, other than Genetic Information and Self-Reported Information, generated by users of 23andMe Services and transmitted, whether publicly or privately, to or through 23andMe. For example, User Content includes comments posted on our Blog or messages you send through our Services.
- **Web-Behavior Information:** information on how you use our Services or about the way your devices use our Services is collected through log files, cookies, web beacons, and similar technologies (e.g., device information, device identifiers, IP address, browser type, domains, page views).

Aggregate Information is different from Personal Information

Aggregate Information is not Personal Information because Aggregate Information does not contain information about a specific individual. Aggregate Information is information about a group of people where names and contact information are stripped and the remaining data is combined with that of other individuals and is analyzed or evaluated as a whole, such that no specific individual may be reasonably identified.

How we collect information

- **You:** We collect information you provide to us when you request or purchase Services or information from us, register with us (including when you link your account on a third-party site or platform with your 23andMe account, such as via Google or Apple), participate in forums or other activities on our sites, features, and applications, respond to surveys, visit our physical properties, call our Customer Care support line, or otherwise interact with us using one or more devices. You may provide information in a variety of ways, including by typing or using voice commands.

- **Service Providers:** We may collect information through service providers who use a variety of technologies and tools, such as cookies, analytics tools, software development kits, application program interfaces, web beacons, pixels, and tags when you visit, use or interact with our Services. For more detail on how we collect and use Web-Behavior Information, please see our Cookie Policy (https://www.23andme.com/about/cookies/).
- **Other Third Parties:** We may receive information about you from other users, individuals, our corporate affiliates, or other third parties. For example, if someone gifts you a testing kit or Subscription, invites you to view their 23andMe Report, or otherwise refers you to 23andMe, we may collect information about you.

How we use your information

Now that we've covered the types of information we collect and how we collect it, let's review how we may use it. As a reminder, we do not sell information, and we will not use your Genetic Information for marketing or personalized advertising without your explicit consent. If you want to dig into the details of how we use your information, check out our How We Use Your Information page (https://www.23andme.com/legal/how-we-use-info/).

We use your information to:

- Provide our Services, including to develop, operate, improve, maintain, and safeguard our Services
- Analyze and measure trends and usage of the Services
- Communicate with you, this includes customer support, or to share information about our Services or other offers or information we think may be relevant to you
- Personalize or contextualize our Services to you
- Enhance the safety, integrity, and security of our Services, including prevention of fraud and other unauthorized or illegal activities on our Services
- Enforce, investigate, and report conduct violating our Terms of Service or other policies
- Conduct surveys or polls, and obtain testimonials or stories about you
- Comply with our legal, licensing, and regulatory obligations
- Conduct 23andMe Research (https://customercare.23andme.com/hc/en-us/sections/200565350-Research-and-Surveys) if you choose to participate

What 23andMe Research participation means for you

23andMe has an opt-in research program, meaning that for eligible customers, taking part in 23andMe Research is completely voluntary. Refer to the Main Research Consent (https://www.23andme.com/about/consent/) for information to help you make an informed choice about participating. Here are key points about 23andMe Research, how Research uses personal information, and other ways we safeguard your privacy.

Before explaining how Research uses Personal Information, let's cover a few basics:

What is 23andMe Research?

The purpose of 23andMe Research is to make new discoveries about genetics and other factors behind diseases and traits. "23andMe Research" means research activities performed by 23andMe, either independently or jointly with third parties, and overseen by an independent ethics review board (also called an Institutional Review Board or "IRB"). 23andMe Research may be sponsored by, conducted on behalf of, or in collaboration with third parties, including non-profit foundations, academic institutions or pharmaceutical companies. For more information on our academic collaborations, see Research (https://www.23andme.com/research/).

What if I *do not* want to participate in Research?

If you are eligible to participate in Research, you choose whether to participate or not, and you can change your mind any time. Customers never need to participate in Research to use 23andMe. Nothing changes about your core 23andMe experience if you do not participate in Research. We do not use your information for Research unless you choose to specifically participate in Research.

How does 23andMe protect my information in Research?

23andMe Research analyses are conducted with information that has been stripped of your identifying Registration Information.

If you choose to consent to the Main Research Consent (https://www.23andme.com/about/consent/)...

- Your de-identified Genetic Information and/or Self-Reported Information may be used for Research.
- We may use de-identified individual-level Genetic Information and Self-Reported Information internally at 23andMe for research purposes.
- We may share summaries of research results, which do not identify any particular individual, with qualified research collaborators and in scientific publications.
- We may inform you of research opportunities for which you may be eligible. We will not share individual-level Personal Information without your explicit consent. To change your preferences for these communications, go to your Account Settings (https://you.23andme.com/user/edit/preferences/).

Some participants choose to contribute in additional ways to Research. For example, you can choose to participate in Individual Level Data Sharing (https://www.23andme.com/about/individual-data-consent/), or additional study-specific agreement(s). Those consents are separate and, like the Main Research Consent, you can withdraw from them anytime. You should review those specific consents for the details. Take a look at your other Research consent documents (https://you.23andme.com/user/edit/research/).

Data sharing

We appreciate the level of trust you put into us. Here's how we do, and do not share your information.

Who we share with:

Service providers: Our service providers help us provide our Services and act on our behalf to get things done. We implement procedures and maintain contractual terms with each service provider to protect the confidentiality and security of your Personal Information. For example, some of the things we use service providers to help us with include: order fulfillment and shipping; processing and analyzing your samples (check out the How We Use Info page (https://www.23andme.com/legal/how-we-use-info/) to learn more!); sample storage (as we like to call it, "biobanking"); customer care support; cloud storage, IT, and security; marketing and analytics; and more.

Your sharing choices: You may direct us to share your Personal Information with friends, family members, doctors or other healthcare professionals, and/or any other individuals or entities who may or may not be using our Services, including through third party services such as social networks and third-party apps that connect to our Services. If you share your Personal Information with a third party, they may use your Personal Information differently than we do under this Privacy Statement. Please make such choices carefully and review the privacy policies of all other third parties involved.

Commonly owned entities, affiliates and change of ownership: If we are involved in a bankruptcy, merger, acquisition, reorganization, or sale of assets, your Personal Information may be accessed, sold or transferred as part of that transaction and this Privacy Statement will apply to your Personal Information as transferred to the new entity. We may also disclose Personal Information about you to our corporate affiliates to help operate our services and our affiliates' services.

Third parties related to law, harm, and the public interest: We can't say it enough – 23andMe will not provide information to law enforcement or regulatory authorities unless required by law to comply with a valid court order, subpoena, or search warrant for Genetic or Personal Information. We require all law enforcement inquiries to follow a valid legal process, such as a court order or search warrant, and are prepared to exhaust available legal remedies to protect customer privacy. If we are compelled to disclose your Personal Information to law enforcement or regulatory authorities, we will try our best to provide you with prior notice, unless we are prohibited from doing so under the law.

23andMe will preserve and disclose any and all information if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary to: (a) comply with legal or regulatory process (such as a judicial proceeding, court order, or government inquiry) or obligations that 23andMe may owe pursuant to ethical and other professional rules, laws, and regulations; (b) enforce the 23andMe Terms of Service (https://www.23andme.com/about/tos/) and other policies; (c) respond to claims that any content violates the rights of third parties; or (d) protect the rights, property, or personal safety of 23andMe, its employees, officers, directors, contractors or other personnel, its users, and the public. Nothing in this Privacy Statement is intended to limit any legal defenses or objections that you may have to a third party's, including a government's, request to disclose your Personal Information.

Who we *DO NOT* share with:

You can rest assured, *we will not* voluntarily share your Personal Information with:

- Public databases
- Insurance companies or employers
- Law enforcement or regulatory authorities (Check out our track record on this promise in our Transparency Report (https://www.23andme.com/transparency-report/))

Your privacy settings and controls

It's your data, and we make it easy to make decisions and choices about it. Below are the types of controls you have in your Account Settings and we've listed what it means to opt-out or to opt-in:

Storing your sample

- Opt-out: No, I do not want my sample stored. If you choose to discard your sample, it will be securely destroyed after the lab completes its analysis, subject to laboratory legal and regulatory requirements. Note, a discard choice cannot be reversed.
- Opt-in: Yes, I want my sample stored. Learn more about Biobanking (https://www.23andme.com/about/biobanking/).

Viewing your health reports

- Opt-out: No, I do not want to receive my health reports.
- Opt-in: Yes, I do want to receive Genetic Health Risk and Carrier Status reports, as well as other reports (e.g., Pharmacogenetics reports) if available.

Sharing features

- Opt-out: No, I do not want to share my information with genetic relatives or other users via features like DNA Relatives or My Connections.
- Opt-in: Yes, I want to be able to share my information so I can discover genetic relatives or connect with others.

Communications preferences

- Opt-out: Please don't contact me for product or promotional purposes. In addition to changing your preferences via Account Settings or your device, you can also click the "unsubscribe" button at the bottom of promotional email communications.
- Opt-in: Yes, you can contact me (such as through email, in-product notifications, or push notifications) for product or promotional purposes.

Research participation

- Opt-out: I don't want to participate in 23andMe Research. If you experience difficulties changing your consent status in Account Settings, contact the Human Protections Administrator at hpa@23andMe.com. You can change your mind any time about your participation, however any Research involving your data that has already been performed or published prior to your withdrawal from 23andMe Research will not be reversed, undone, or withdrawn.
- Opt-in: Yes, I'd like to participate in 23andMe Research.

You can also:

Access & Download: You can access and download your Personal Information processed by 23andMe. Please note, if you lose access to your 23andMe Account, we require that you submit additional information to verify your identity before providing access or otherwise releasing information to you.

Correct Information: You can correct your Registration Information and modify Self-Reported Information entered into surveys.

Delete your Account: You can delete your 23andMe account within your Account Settings at any time. Upon account deletion, we will automatically opt you out of Research and discard your sample.

Keep in mind this process cannot be cancelled, undone, withdrawn, or reversed. For exact instructions, please read our Customer Care guidance (https://customercare.23andme.com/hc/en-us/articles/212170688-Requesting-23andMe-Account-Closure).

Other things to know about privacy

Security Measures

We implement physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information. Our team regularly reviews and improves our security practices to help ensure the integrity of our systems and your Personal Information. To learn more about our practices, please visit our Customer Care guidance (https://customercare.23andme.com/hc/en-us/articles/202907840-How-Is-My-Personal-Information-Protected).

Please recognize that protecting your Personal Information is also your responsibility. Be mindful of keeping your password and other authentication information safe from third parties, and immediately notify 23andMe of any unauthorized use of your login credentials. Your password is not visible to 23andMe staff, and we encourage you not to share your password with 23andMe or any third parties. 23andMe cannot secure Personal Information that you release on your own or that you request us to release.

Third Party Content and Integrations

Our Services may contain third party content, integrations or links to third party websites operated by organizations not affiliated with 23andMe. Through these integrations, you may be providing information to the third party as well as to 23andMe. Since we can only control our own Services, we are not responsible for how those third parties collect or use your information so please review the privacy policies of every third-party service that you visit or use, including those third parties you interact with through our Services.

State and Region-Specific Information

You may have specific privacy rights in your state or region. For example, in the United States, residents of California and other states (https://www.23andme.com/about/california-privacy/) have specific privacy rights, as well as 23andMe residents of the European Economic Area (EEA), the UK, Switzerland and other jurisdictions (https://www.23andme.com/legal/eu-privacy-notice/).

Legal Retention Requirements

23andMe and/or our contracted genotyping laboratory will retain your Genetic Information, date of birth, and sex as required for compliance with applicable legal obligations, including the federal Clinical Laboratory Improvement Amendments of 1988 (CLIA), California Business and Professions Code Section 1265 and College of American Pathologists (CAP) accreditation requirements. 23andMe will also retain limited information related to your account and data deletion request, including but not limited to, your email address, account deletion request identifier, communications related to inquiries or complaints and legal agreements for a limited period of time as required by law, contractual obligations, and/or as necessary for the establishment, exercise or defense of legal claims and for audit and compliance purposes.

Changes to this Privacy Statement

We may make changes to this Privacy Statement from time to time. We'll let you know about those changes here or by reaching out to you via email or some other contact method, such as through in-app notification, or on another website page or feature.

Contact Information

If you have questions about this Privacy Statement, or have a complaint or inquiry, please email 23andMe's Privacy Administrator at privacy@23andme.com (mailto:privacy@23andme.com), call us at 1.800.239.5230, or send a letter to:

Privacy Administrator
23andMe, Inc.
349 Oyster Pt. Blvd
South San Francisco CA 94080

Read the previous version of the document. (/legal/privacy/full-version/6.5/)

(https://www.facebook.com/23andMe/) (https://twitter.com/23andMe/) (https://www.youtube.com/user/23andMe) (https://www.instagram.com/23andMe) (https://www.linkedin.

© 2022 23andMe, Inc. All rights reserved.

23andMe Guide for Law Enforcement

This guide is intended for law enforcement authorities and government agencies in the United States seeking information relating to the accounts or users of 23andMe. Additional information is available in the applicable Terms of Service (/about/tos/) (TOS) and Privacy Statement. (/about/privacy/)

Services Provided By 23andMe

The 23andMe Personal Genetic Service is a direct-to-consumer genetic testing service that provides information and tools for individuals interested in learning about and exploring their DNA. Depending on where they live, customers who submit saliva samples using the 23andMe Personal Genetic Service saliva collection kit can access their Genetic Information through two different services:

- 23andMe Ancestry Service: customers have access to genealogical DNA test results and can opt-in to our DNA Relatives database.
- 23andMe Health + Ancestry Service: in addition to the Ancestry Service information, Health + Ancestry customers will also have access to Genetic Health Risks, Carrier Status, Wellness, and Trait reports.

Customers may purchase either the Ancestry Service or the Health + Ancestry Service.

Information 23andMe Collects

We collect user information in accordance with the applicable Terms of Service (TOS) and Privacy Statement.

We work with third-party companies to provide users with services on behalf of 23andMe, and in some cases these companies may have access to a limited amount of non-genetic user information. Specifically, our contracted lab has access to users' DNA samples and limited user information for processing purposes.

Under the federal Clinical Laboratory Improvement Amendments (CLIA) of 1988, 23andMe is required to provide the laboratory with the customer's sex and date of birth. No other Registration Information (such as name, address, email, phone number or other contact information) is provided to the laboratory. Samples and data are otherwise identifiable only by the unique barcode that is used to register a saliva collection kit tube.

Requests for 23andMe User Information

23andMe chooses to use all practical legal and administrative resources to resist requests from law enforcement, and we do not share customer data with any public databases, or with entities that may increase the risk of law enforcement access. In certain circumstances, however, 23andMe may be required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information.

23andMe requires valid legal process in order to consider producing information about our users. 23andMe will only review inquiries as defined in 18 USC § 2703(c)(2) related to a valid trial, grand jury or administrative subpoena, warrant, or order. Administrative subpoenas must be served on 23andMe by personal service just like subpoenas in a court setting. 23andMe will consider releasing additional account information or transactional information pertaining to an account only in response to a court order issued pursuant to 18 USC § 2703(d). In addition, 23andMe will only consider inquiries from a government agency with proper jurisdiction.

To date, 23andMe has never received a request to preserve information potentially relevant to legal proceedings pursuant to 18 USC § 2703(f). If we do receive a valid preservation request, we will preserve a temporary snapshot of the relevant records for 90 days, after which we will automatically remove the information from our servers unless we receive a renewed valid preservation request for an additional 90-day period.

If a 23andMe user completes a valid authorization to disclose their Genetic Information to law enforcement, then 23andMe will disclose the information identified in the authorization. 23andMe will not disclose any identifying information about the authorizing user's genetic relatives or connections that 23andMe holds unless those users also provide express, written consent.

23and Me publishes a Transparency Report (/transparency-report/) which contains details on all law enforcement requests for user information that we receive.

How to Request 23andMe User Information

23andMe responds to valid legal process issued in compliance with applicable law. When requesting user account information, please include:

- If available/known, the full name of the subject 23andMe account holder, and the email and/or mailing address associated with the account(s).

- Details about what specific information is requested (e.g., basic user information) and its relationship to the investigation. We are unable to process overly broad or vague requests.
- A valid official email address (e.g., name@agency.gov) so we may get back in touch with you upon receipt of your legal process.

Requests should be made in writing and should be submitted by certified mail, express courier, or in person at the addresses listed below; and an additional copy may be sent by email. We do not accept legal process by email or fax unless the request is an emergency request. Our contact information is available at the bottom of both this Guide and our Terms of Service (TOS). Written requests must be made on law enforcement letterhead and be signed by the responsib law enforcement officer.

Even if a law enforcement request for information meets the minimum requirements listed above, 23andMe will assess whether or not it is required by law to comply with the request, based on whether 23andMe is subject to personal jurisdiction in the requesting entity, the validity of the method of service, the relevance of the requested data, the specificity of the request, and other factors.

User Notification About Law Enforcement Requests

If 23andMe is required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information, we will notify the affected individual(s) through the contact information they have provided to us before we disclose this information to law enforcement, unless doing so would violate the law or a court order. We will give them a reasonable period of time to move to quash the subpoena before we answer it.

If law enforcement officials prevent this disclosure by submitting a Delayed Notice Order (DNO) pursuant to 18 U.S.C. § 2705(b) or equivalent state statute that is signed by a judge, we will delay notifying the user until the order expires. 23andMe retains sole discretion to not notify the user if doing so would create a risk of death or serious physical injury to an identifiable individual or group of individuals, and if we are legally permitted to do so. Under these circumstances, we will notify users of the law enforcement request once the emergency situation expires.

To date, 23andMe has not received a law enforcement request for information in the form of a National Security Letter (NSL) containing an indefinite non-disclosure provision. If 23andMe receives such a request in the future, 23andMe is committed to requesting judicial review of the order pursuant to the USA Freedom Act. Once the non-disclosure provision no longer applies, 23andMe will notify affected users about the order.

Use of 23andMe Personal Genetic Service for Law Enforcement Casework and Forensics

Use of the 23andMe Personal Genetic Service for casework and other criminal investigations falls outside the scope of our services intended use.

With respect to user information, while our Terms of Service (TOS) requires that participants provide 23andMe with true and accurate Registration Information, 23andMe cannot precisely authenticate or verify an individual's identity when they use or sign up for our service, and thus does not have the means to reliably connect any particular DNA sample or account to an individual. This means that 23andMe Personal Genetic Service has no chain of custody and is not considered a confirmatory test or proof in a legal context.

Submitting a saliva sample to 23andMe for processing requires that the person providing the sample, or their legal representative, has read and agreed to our TOS and our Privacy Statement. Those who wish to participate in the 23andMe service must guarantee that any sample they provide is either their own saliva or that of an individual for whom they have legal authorization to agree to the TOS on their behalf. Under our TOS, those who participate in 23andMe's services by submitting a saliva sample agree not to "use any information received through the Services to attempt to identify other customers, to contact other customers (other than through features for contacting other users such as DNA Relatives offered pursuant to the Services), or for any forensic use."

Therefore, it is a violation of our TOS for law enforcement officials to submit samples on behalf of a prisoner or someone in state custody who has been charged with a crime.

Additionally, the analysis that we provide can only be performed using a ~2ml saliva sample collected using our saliva kit. We cannot process samples or biospecimens collected in any other format.

Contact Information

For service of legal process, please contact 23andMe at the following address:

23andMe, Inc.
Attn: Legal Department, Law Enforcement Request
349 Oyster Point Blvd
South San Francisco, CA 94080
United States

Phone Number: (800) 239-5230 (tel:+01-800-239-5230)
Email Address: privacy@23andme.com (mailto:privacy@23andme.com)

23andMe

(/)

SERVICES

Health + Ancestry (/dna-health-ancestry/)

Ancestry + Traits (/dna-ancestry/)

23andMe+ Membership (/membership/)

Gifts (/gifts/)

COMPANY

Investors (https://investors.23andme.com/)

About Us (/about/)

Diversity, Equity & Inclusion (/diversity-equity-inclusion/)

Media Center (https://mediacenter.23andme.com)

Blog (https://blog.23andme.com/)

Genetics Learning Hub (/topics/)

Careers (/careers/)

Refer a Friend (https://refer.23andme.com/pub_footer_us)

Return Policy (https://customercare.23andme.com/hc/en-us/articles/202907780)

Customer Care (https://customercare.23andme.com/hc/en-us/)

FSA/HSA Eligibility (/fsa-hsa/)

Site Map (/sitemap/)

LEGAL

Important Test Info (/test-info/)

Terms of Service (/legal/terms-of-service/)

Privacy Statement (/legal/privacy/)

Data Protection (/gdpr/)

Family Considerations (https://customercare.23andme.com/hc/en-us/articles/202907980)

Research Consent (/about/consent/)

Individual Data Consent (/about/individual-data-consent/)

Biobanking Consent (/about/biobanking/)

Cookie Policy (/about/cookies/)

Ad Choices (/about/cookies/#5-what-are-my-privacy-options)

Patent Information (/patents/)

Report a Security Issue (/security-report/)

PARTNER WITH US

Medical Professionals (https://medical.23andme.com/)

Educators (https://education.23andme.com/)

Scientists (https://research.23andme.com/)

Therapeutics (https://therapeutics.23andme.com)

DOWNLOAD APP

Download on the App Store (https://itunes.apple.com/us/app/23andme/id952516687?ls=1&mt=8)

Download on Google play (https://play.google.com/store/apps/details?id=com.twentythreeandme.app&hl=en_US)

United States | Change

(https://www.facebook.com/23andMe/) (https://twitter.com/23andMe/) (https://www.youtube.com/user/23andMe) (https://www.instagram.com/23andMe) (https://www.linkedin.

© 2022 23andMe, Inc. All rights reserved.

Transparency Report

Respect for customer privacy and transparency are core principles that guide 23andMe's approach to responding to legal requests and maintaining customer trust. Unless required to do so by law, we will not release a customer's individual-level Personal Information to any third party without asking for and receiving that customer's explicit consent.

More specifically, we will closely scrutinize all law enforcement and regulatory requests and we will only comply with court orders, subpoenas, search warrants or other requests that we determine are legally valid.

The information we share in our Transparency Report is one of many ways we illustrate our commitment to keeping our customers informed and protecting their privacy.

About the Numbers

The statistics included in our Transparency Report reflect the following:

- The number of government requests for customer information we have received.
- The number of customers or accounts specified in requests we have received.
- The number of instances where data was produced (in whole or in part) without prior, explicit consent by the individual(s) specified in the request.

This report was first published in 2015, was last updated on October 14, 2022 and will continue to be updated on a quarterly basis. The information below reflects the cumulative number of requests received since this report was first published in 2015.

COUNTRY	DATA REQUESTS RECEIVED	NUMBER OF USERS / ACCOUNTS SPECIFIED	DATA PRODUCED (BY USER ACCOUNT)
TOTAL	11	15	0
United States	11	15	0

COUNTRY	DATA REQUESTS RECEIVED	NUMBER OF USERS / ACCOUNTS SPECIFIED	DATA PRODUCED (BY USER ACCOUNT)
Canada	0	0	0
The United Kingdom	0	0	0
The Netherlands	0	0	0
Sweden	0	0	0
Finland	0	0	0
Denmark	0	0	0
Ireland	0	0	0
Rest of World	0	0	0

National Security Requests

As of October 14, 2022, 23andMe has not received or been notified of a National Security Letter, an order under the Foreign Intelligence Surveillance Act, or any other classified request for user information pursuant to the national security laws of the United States or any other country.

Law Enforcement Resources

23andMe requires valid legal process to consider producing information about our customers. Law enforcement agencies should read 23andMe's **Guide for Law Enforcement** document prior to contacting 23andMe.

Gifts

COMPANY

Investors

About Us

Diversity, Equity & Inclusion

Media Center

Blog

Genetics Learning Hub

Careers

Refer a Friend

Return Policy

Customer Care

FSA/HSA Eligibility

Site Map

Data Protection

Family Considerations

Research Consent

Individual Data Consent

Biobanking Consent

Cookie Policy

Ad Choices

Patent Information

Report a Security Issue

PARTNER WITH US

Medical Professionals

Education

Scientists

Therapeutics

DOWNLOAD APP







United States | Change





© 2022 23andMe, Inc. All rights reserved.

Ancestry.com

Your Privacy

Language

Effective Date: 15 Aug 2022

Summary of Changes

This summary communicates the most recent changes to Ancestry's Privacy Statement and how the changes may impact you.

The updates to the Privacy Statement apply to your use of the Services (defined below) when you view, access, or otherwise use the Services. To fully understand the changes and terms that will govern your use of our Services, please read the Privacy Statement.

Specifically, the most recent changes include:

- The addition of language to comply with the California Privacy Rights Act of 2020 ("**CPRA**"), the Colorado Privacy Act ("**CPA**"), the Connecticut Data Privacy Act ("**CTDPA**"), the Virginia Consumer Data Protection Act ("**VCDPA**"), and the Australian Privacy Act 1988.
- The removal of references to AncestryHealth®.
- Updating, clarifying, and simplifying existing language.

At Ancestry®, your privacy is a top priority. Ancestry is committed to being a good steward of your Personal Information (defined below), handling it in a responsible manner, and securing it with administrative, technical, organizational and physical safeguards.

We believe in being honest, direct and transparent when it comes to your data. Ancestry follows three guiding principles when it comes to your privacy:

Transparency. We work hard to be transparent about what Personal Information we collect and process.

Simplicity. We try to use easy-to-understand language to describe our privacy practices to help you make informed choices.

Control. We give you control over the Personal Information you provide to us, including your DNA Data, and how it is used, shared, and retained.

Other Important Things for You To Understand When You Use Our Services

You maintain control of your DNA and DNA Data (defined below)—you can manage and delete it as described in this Privacy Statement.

You may discover unexpected facts about yourself or your family when using our services. Once discoveries are made, we can't undo them.

When you make new discoveries with us, you should feel confident and informed about how we use your Personal Information. Our full Privacy Statement is below. It covers all Ancestry websites, services, and mobile apps that link to this Privacy

Statement, including: Ancestry®, AncestryDNA®, Fold3®, Newspapers.com™, Archives®, We Remember®, and Find a Grave®.

US Customers only - The **US Resident Additional Privacy Statement** below contains additional details for US residents in California, Colorado, Connecticut, and Virginia.

Non-US Customers only - Ancestry Ireland Unlimited Company is the controller of your Personal Information and Section 8 below contains information on your rights.

Table of Contents

1. Introduction
2. Account Creation and Your Engagement with Ancestry Services
3. What Personal Information Does Ancestry Collect from You?
4. What Information Does Ancestry Collect Through Your Use of the Services?
5. Information We Collect from Other Sources
6. How Does Ancestry Use Your Personal Information?
7. What Information Do We Share, When Do We Share It, and Who Are the Recipients?
8. Your Rights and Choices Regarding Your Personal Information
9. What Are Our Retention Practices?
10. How Can I Delete My Personal Information?
11. Security
12. International Data Transfers
13. Changes to This Statement
14. Legal Bases Under EU General Data Protection Regulation for Processing Personal Information of EU Residents.
15. Identity and Contact Details of the Data Controller
16. US Resident Additional Privacy Statement (California, Colorado, Connecticut, and Virginia customers only)
17. Australian Additional Privacy Statement

1. Introduction

At Ancestry, we empower journeys of personal discovery to enrich lives. To provide and improve the websites, mobile applications, and services (collectively the "**Services**"), we collect, process, and store "**Personal Information**," which is information that can identify you directly or indirectly, as further described in Section 3, such as your name, email or address, or information that could reasonably be linked back to you, including your Genetic Information. This Privacy Statement describes our practices for collecting, storing and processing your Personal Information and the controls we provide you to manage it within our Services. In addition, our Cookie Policy describes our use of browser cookies and similar tracking technologies.

Please note: Information about deceased persons is not Personal Information under this Privacy Statement.

2. Account Creation and Your Engagement with Ancestry Services

The Personal Information contractually required to create an account with Ancestry is limited to your name, an email address, and a password. For Archives users only, billing information is also required for account creation.

By creating an account you are telling us that you understand Ancestry will collect, process, and share your Personal Information (including your Genetic Information if you have taken a DNA test) as described in this Privacy Statement.

Access to Ancestry content such as archival records to help you build a family tree or to our DNA features (ethnicity estimate, etc.) requires additional Personal Information, including payment and shipping details, and, for the DNA test, the test code, your assigned sex at birth, birth year, and Genetic Information extracted from your saliva sample.

At any time, you can request that Ancestry delete Personal Information you have uploaded into your account, such as a family tree or your Genetic Information. You can also delete your entire account. Please see Section 10 for specific details about deleting your Personal Information.

3. What Personal Information Does Ancestry Collect From You?

Categories:	**Account Information**

Description:

- Your name (required).
- An email address (required).
- A password that you create (required).
- A phone number - You may provide a phone number so we can (i) notify you of DNA test result status, (ii) notify you of other updates you agree to, (iii) assist you when you contact Ancestry Member Services, or (iv) allow you to enable multi-factor authentication. A phone number may be required for DNA test kit deliveries.
- Billing information.
- Certain Ancestry brands may support third-party sign-in services such as Facebook, Google and Apple that provide Ancestry your Personal Information, such as your name and email address, and profile photo. Please refer to our Cookie Policy to learn about how third parties use technology for analytics and targeting purposes and about the controls we provide you.

Categories: **Credit Card/Payment Information**

Description:

- Payment information, such as your credit card number, and your billing and shipping address(es), when you sign up for a free trial or make a purchase, such as an Ancestry subscription or a DNA test kit.

Categories: **DNA Kit Activation Information**

Description: When you activate a DNA test kit, we collect:

- Your DNA test kit code;
- Your assigned sex at birth; and,
- Your year of birth.

Categories: **Profile Information**

Description:

We collect the information that you provide when you create a user profile (for example, a profile image, your name, username, biography, age, location, and linked account usernames) and about you from your family tree. Your Ancestry user profile information is visible to other Users (defined in the Ancestry Terms and Conditions), so please consider limiting this information and using a username that is different from your real name to protect your privacy.

Categories: **Your Content**

Description:

We collect information when you voluntarily contribute to the Services, including Your Content (as defined in the Terms and Conditions.

Categories: **Genetic Information**

Description: At our partner laboratories, we extract your DNA from your saliva and convert it into machine-readable biometric data (**"DNA Data"**) that we process to provide you with an ethnicity estimate and communities suggestions. We also process your DNA Data to provide you information about your degree of relatedness to other users in our DNA database and any genetic markers[?] associated with certain biological, physiological, or behavioral traits, such as hair thickness and eye color or traits associated with wellness.

Your DNA Data and any information derived from it such as ethnicity estimates, communities, traits, and genetic relative matches are Personal Information and referred to as **"Genetic Information"**.

A Note About Your DNA and Saliva: Neither your saliva nor the extracted DNA (together referred to as **"Biological Samples"**) are Personal Information under this Privacy Statement. Also, after our laboratory partner has processed your Biological Sample, you can consent to its storage in our bio bank for future testing at your option. Future testing may be done if you agree to our Informed Consent for Research or if you consent to other tests of your Biological Samples. If you do not consent to the storage of your Biological Sample, we will destroy your sample. Sections 8 and 10 below describe how you can control your Biological Samples. You may request that Ancestry destroy your Biological Samples by contacting Member Services. Note that we may destroy Biological Samples that do not meet our quality assurance requirements at our discretion.

Categories:	**Note About Health-Related Information**
Description:	Ancestry is not a covered entity under the Health Insurance Portability and Accountability Act ("**HIPAA**"), and as a result no data provided by you is subject to or protected by HIPAA.

Categories:	**Your Communications**
Description:	We host and maintain your communications with other Users through the communications features on our platform, and also collect your information when you communicate with Ancestry Member Services and support teams for our other Services, including audio and visual information (such as recordings of calls with Ancestry Member Services or information voluntarily shared when participating in consumer insights research).

Categories:	**Contests and Promotions**
Description:	We collect Personal Information when you voluntarily participate in contests and special promotions we run or sponsor, the details of which are provided upon entry.

Categories:	**Find a Grave Photos and Photo Volunteers**
Description:	Through Find a Grave, we collect metadata associated with digital photographs uploaded to the Find a Grave service, including location, date, and time the photo was taken. If you choose to be a photo volunteer for Find a Grave, you provide your location to us which you can change or remove at any time.

Categories:	**Other Protected Classifications and Sensitive Data**
Description:	We may collect information related to certain protected classifications such as gender or marital status.

For information on Personal Information processed by Ancestry relating to non-Ancestry users please click here.

4. What Information Does Ancestry Collect Through Your Use of the Services?

Categories:	**Computer and Mobile Device Information**
Description:	Ancestry collects information about how you access our Services, including the website you visited before and after Ancestry's site. We also collect the IP address where your computer, mobile device, or the proxy server that you use accesses the Internet, in addition to other technical information, such as: ◦ Your computer operating system; ◦ Your web browser; ◦ Your mobile device identifier provided by your mobile device operating system and your mobile operating system; and, ◦ The name of your internet service provider or mobile carrier. Ancestry may collect geolocation information from your device with your permission.

Categories:	**Information from Cookies and Similar Technologies**
Description:	Ancestry uses cookies and similar technologies as well as technical integrations with marketing and advertising partners as described in our Cookie Policy. Please refer to our Cookie Policy to learn about our practices and the controls we provide you.

Categories:	**Information Shared Through Social Media Features**
Description:	If you interact with social media through the Services, for example "Share," "Post," "Tweet," "Pin," or "Follow Us" links to sites such as Facebook, Twitter, Pinterest, Instagram, and YouTube, Ancestry will collect these interactions and whatever account information these services make available to us dependent on your privacy settings with that third party. Your interactions with these features are governed by the privacy statement of the applicable third-party company. You may have the option to sign-on to Ancestry services using your social networking account, such as a Google or Apple account. Where you give appropriate permissions, we will receive information about you from your social networking account that Ancestry will use to create your account and build your profile, such as your name, email address, and profile photo.

Categories:	**Information from Your Use of the Services**
Description:	We collect information about your use of the Services, such as when you search or access records or public family trees, which pages you view, links you click, or when you add people to your tree, etc., which we may use to infer details about you as a customer and your interests to provide a better experience through, for example, search suggestions.

5. Information We Collect from Other Sources

Categories:	**Information from Public and Historical Records**
Description:	Ancestry collects records from various sources, usually from official record sources, including newspapers, as well as birth, death, marriage, and census records, which may contain Personal Information relating to you. Public and historical records may also contain Personal Information relating to non-Ancestry users. These records are usually made available to Users as part of the Ancestry subscription Services.

Categories:	**Information from Third Parties**
Description:	We may also receive information about you from third parties. For example, we may supplement the data we collect with information licensed from third parties in order to personalize the Services and our offers to you. If you purchase a gift subscription or DNA kit as a gift, we will collect Personal Information, such as the recipient's name, shipping address, email address, and the necessary purchase information to complete the gift and notify the recipient.

6. How Does Ancestry Use Your Personal Information?

Categories:	**Personal Information (Generally)**
Description:	We use your Personal Information to provide, personalize, improve, update, and expand our Services. This includes: • Authenticating your access to the Services and improving Ancestry information security; • Processing your payments for subscriptions, AncestryDNA services and test kits, and other products and features; • Building new and improving existing Services; • Helping you create, and providing insights about, your family trees based on data in Ancestry's databases; • Issuing surveys and questionnaires for use in the Services, as well as facilitating product development and research initiatives; • Conducting scientific, statistical, and historical research; • Detecting and protecting against error, fraud, or other criminal or malicious activity; and, • Enforcing our Terms and Conditions.

Categories:	**Communications**
Description:	We use your Personal Information to communicate with you about the Services, such as when we: • Respond to your inquiries to Member Services; • Alert you to potential genetic relatives identified by DNA matching, or through our family history services (for example, "Ancestry Hints®" about potential ancestors in our database); • Alert you to records pertaining to people in your family tree or to whom you may be related; • Inform you of changes to Services or new Services; • Ask you to participate in Ancestry media productions, advertisements, consumer insights research, or testimonials; and, • Provide you with information or request action in response to technical, security, and other operational issues.

Categories:	**Market Products and Offers from Us or Our Business Partners**
Description:	We may use some Personal Information (for example, demographic information available from third-party sources or from parts of Ancestry (profile, trees, etc.)) to market our products and offers from us or our

business partners. This marketing includes advertising based on your interests.

Please note: Ancestry does not share your Genetic Information with third-party marketers, insurance companies, or employers, and we will not use your Genetic Information for marketing or personalized advertising without getting your explicit consent.

For marketing that you have consented to receive by email or SMS, you can control how we market to you by using the unsubscribe link in any marketing email you receive, by changing your communication settings, or by following the instructions in marketing communications you receive. Controls for Ancestry's related brands' are available through their settings and are listed here. For advertising on third-party platforms, we rely on our own legitimate interests as the legal basis (please see Section 7) and you should control your marketing preferences directly on those platforms.

Categories:	**Genetic Information**
Description:	Ancestry uses your Genetic Information for the following primary purposes: • Delivering ethnicity results, DNA matches (e.g., close or extended family or others to whom you may be related) from our database, and other information to help you and other users learn more about each other, potential family members, as well as your genetic relatives and family groups; • Connecting you with and helping you learn about your genetic relatives in our database through features such as DNA matching or other product features; • Providing you with other insights into what your DNA may reveal about traits, and wellness; • Providing relevant results to assist you in discovering common ancestors and other details about your family history, as well as helping you build your family tree or connect with friends and family; • Studying aggregated Genetic Information to better understand population and ethnicity-related health, wellness, aging, or physical conditions; • Conducting scientific, statistical, and historical research; and, • Improving features and functionality in our existing DNA-related products, enhancing the customer experience across Ancestry Services, improving the quality of our laboratory processes and technology, and building new products and services.

7. What Information Do We Share, When Do We Share It and Who Are the Recipients?

Ancestry does not share your individual Personal Information (including your Genetic Information) with third-parties except as described in this Privacy Statement or with your additional consent. We do not voluntarily share your information with law enforcement. Also, we will not share your Genetic Information with insurance companies, employers, or third-party marketers without your express consent.

Please note: Ancestry's US-specific disclosures can be found here. Ancestry does not sell your Personal Information.

The circumstances described below explain when sharing might occur:

Categories:	**Ancestry Companies**
Description:	We may share your information within the Ancestry group of companies listed here (the "**Ancestry Companies**") in order to provide and improve our Services. We transfer your Personal and Genetic Information between Ancestry's Ireland-based company and Ancestry's U.S.-based companies. For more information on this see Section 12 below.

Categories:	**Other Users or Others You May Choose to Share With**
Description:	As part of your use of the Services, you have the option to add or share information with all Users of the Service or through sharing features with particular Ancestry Users and even non-Ancestry users. You may have additional sharing options in some Services, for example AncestryDNA (see below). Information in your public profile(s) will be seen by all other Users, as will public family tree details (note that living people in your tree are only visible to you and people you share your tree with as "editor" or whom you authorize to be able to view your tree's living people). If you choose to view and be seen by your DNA matches, your DNA matches can see certain Personal Information, such as your username, how they might be related to you, whether you have linked a family tree

to your DNA, and either all or only shared (at your option) regions and communities. You may be offered other options for connecting with relatives or learning about familial connections.

You can share other DNA information, such as Traits, through the "compare" and other one-to-one sharing features.

If you share details of your family history or DNA experience outside the Services, you do so at your own risk.

Categories:	**Service Providers**
Description:	We work with other companies when providing and marketing the Services. As a result, these companies will have access to or otherwise process your data, including some of your Personal Information, in their systems. These companies are subject to contractual obligations governing privacy, data security, and confidentiality consistent with applicable laws. These companies and the Personal Information they may have access to include our: • Laboratory partners (such as your DNA); • DNA test shipping providers (such as name, shipping address, and phone number); • Payment processors (such as Payment Information); • Cloud services infrastructure providers (Ancestry's web and mobile services are cloud-based services; all your data resides with our cloud service vendors); • Biological sample storage facilities (such as Biological Sample and DNA test kit code); • Vendors that assist us in marketing and consumer research analytics, fraud prevention, and security (such as email address); • Communications infrastructure providers (such as name and email address); and, • Vendors that help us provide some Member Services functions, like phone support or survey tools (such as Account Information or name or email address)

Categories:	**Analytics and Advertising Partners**
Description:	We work with third-party partners for analytics and advertising purposes. By collecting and sharing certain Personal Information, these vendors help us to better personalize ads to match your interests. They also help us to measure the effectiveness of ad campaigns and are used to serve you with advertising that is more relevant to you.

Categories:	**Research Partners**
Description:	We share your Genetic Information with research partners only when you provide us with your express consent to do so through our Informed Consent to Research. Unless you agree to the Informed Consent to Research, your data will not be shared with these researchers. Research partners include commercial or non-profit organizations that conduct or support scientific research, the development of therapeutics, medical devices or related material to treat, diagnose or predict health conditions. In some circumstances, a research partner or Ancestry may have a financial interest in the research arrangement. A list of our research partners can be found here.

Categories:	**Law Enforcement**
Description:	Ancestry does not voluntarily provide data of any kind to governmental or judicial bodies or to law enforcement agencies. To provide our Users with the greatest protection under the law, we require all government agencies seeking access to Ancestry customers' data to follow valid legal process. We do not allow law enforcement to use Ancestry's services to investigate crimes or to identify human remains. If we are compelled to disclose your Personal Information to law enforcement, we will do our best to provide you with advance notice, unless we are prohibited under the law from doing so. Ancestry produces a Transparency Report where we list the number of valid law enforcement requests for user data across all our sites.

Categories:	**Other Legal or Regulatory Process**
Description:	We may share your Personal Information if we believe it is reasonably necessary to: • Comply with valid legal process (e.g., subpoenas, warrants); • Enforce or apply the Ancestry Terms and Conditions;

	◦ Protect the security or integrity of the Services; or ◦ Protect the rights, property, or safety of Ancestry, our employees, or Users.
Categories:	**If Ancestry is Acquired**
Description:	If Ancestry or its businesses are acquired or transferred (including in connection with bankruptcy or similar proceedings), we may share your Personal Information with the acquiring or receiving entity. The promises in this Privacy Statement will continue to apply to your Personal Information transferred to the new entity.
Categories:	**A Note About Aggregated Data**
Description:	Ancestry may disclose user information in an aggregated form as part of the Services or our marketing, or in scientific publications published by us or our research partners. For example, we might note the percentage of immigrants in a State that are from a particular geographic region or country. Such disclosure will never include Personal Information.

8. Your Rights and Choices Regarding Your Personal Information

All Users (as defined in our Terms and Conditions) may use our online tools to 1) request a report of what Personal Information they have provided to us, 2) download a copy of their DNA Data or download a copy of their family trees, and 3) delete their family trees, DNA test results or account.

Additionally, some data privacy laws, such as the EU's General Data Protection Regulation, provide people with specific rights regarding their Personal Information. For example:

Right of Access/To Know – You may have a right to request access to your Personal Information and to be provided with a copy of certain information including the categories of your Personal Information we collect and disclose. To request a copy, follow these step-by-step instructions. If you want a copy of your DNA Data, follow these step-by-step instructions. If you want a copy of your family trees, follow these step-by-step instructions.

Right of Rectification/Correction – You may have the right to request that we rectify or correct inaccurate Personal Information about you.

Right of Erasure/Deletion – You have the right, in certain cases, to request that we restrict (stop any active processing) or delete your Personal Information, provided there are valid grounds for doing so and subject to applicable law. See Section 10 for information on how to delete your Personal Information.

Right to Object – You may have the right to object to processing activities in our legitimate interests where such activities impact on your rights and freedoms as an individual. Also, when you consent to processing of your Personal Information for a specified purpose, you may withdraw your consent at any time and we will stop any further processing of your data for that purpose.

Right to Restriction – You have the right to request a restriction on our processing of your Personal Information, for example, where you believe that the processing is based on inaccurate data or not processed in a lawful manner.

Right to Data Portability – You may have the right to receive certain of your Personal Information in a format that can be transmitted to another data controller.

Right to Complain – You have the right to make a complaint to the Irish Data Protection Commission (Complaints handling, Investigations and Enforcement For Individuals | Data Protection Commissioner) or any other competent supervisory authority in the country of residence.

You can exercise these rights by using the tools described below or by contacting Ancestry. Details and options for accessing this information are listed below.

Categories:	**Ancestry**
Description:	You can access and update the Personal Information (such as your email address, username, profile information, etc.) that you provide to Ancestry at any time in the following sections of the privacy settings: Public Profile; Account Settings; Communications Settings; and, DNA Settings. To learn how to manage the privacy settings for any family trees you have created on Ancestry, you can visit your Tree Settings or click here.
Categories:	**Related Brands**

Description:	Ancestry strives to make it simple for you to manage your privacy across the Services. You can manage your privacy settings for our related brands here.

Categories:	**Mobile Apps**
Description:	You can also control your information using the settings available in our mobile applications, such as Ancestry, AncestryDNA, Find a Grave, and We Remember apps.

Categories:	**Advertising**
Description:	We use cookies and similar tracking technologies and integrations with third party marketing and advertising partners to collect data about your interests or behaviors to serve you targeted ads. You may change your settings as described in our Cookie Policy. For information on "Do Not Track" please see our Cookie Policy.

Categories:	**Family Tree Information Download**
Description:	Ancestry allows you to download your family tree information in the standard GEDCOM family tree file format in your Tree Settings. Learn how here.

Categories:	**Genetic Information Download**
Description:	You always have the option of downloading a file with your DNA Data. If you download your DNA Data, you do so at your own risk. Learn how here. For more information on what is included in your DNA Data download, go here.

9. What Are Our Retention Practices?

Ancestry Services are fundamentally premised on the notion that the personal voyage of self-discovery is not a one-time event and continues over lengthy periods of time—possibly lifetimes. Additionally, and with particular regard to our subscribers and DNA customers who pay fees or purchase subscriptions, the ongoing enhancement of our collections of historical records and DNA features provide benefits and insights to our Users over time. As a result, our retention practices reflect this ongoing value by retaining user accounts on our system until our Users inform us of their desire to delete their data or close their accounts.

Categories:	**Account and Profile**
Description:	Ancestry will retain the Personal Information you provide while creating your account and your profile until such time as you delete your account.

Categories:	**Family Tree**
Description:	Due to the multi-generational significance of family trees, Ancestry will retain your family tree data to provide you with continuous access, updated features, and the ability to enhance your family tree. Your family tree data is kept until you delete your family tree or your account.

Categories:	**DNA**
Description:	Ancestry retains your DNA Data to provide you with the features and functionality you purchased (or were gifted), including continuously updated features such as DNA matches, increasingly granular ethnicity estimates and improved regions and communities, as well as new other features based on your DNA Data. Your DNA Data is kept until you delete your DNA test results or your account. If you were a customer of AncestryHealth, our AncestryHealth laboratory partners are required to retain your DNA Data and test result for a period of at least seven years, or as required by state law and the Clinical Laboratory Improvements Act (CLIA) and the guidelines that apply to laboratories certified by the College of American Pathologists (CAP).

Categories:	**Related Brands**
Description:	Some of our related brands (Fold3, Newspapers.com™, Find a Grave, We Remember, or Archives) have their own account logins and will retain the Personal Information you provide while creating your account and your profile as needed to provide you with continuous and updated Services until such time as you ask us to delete it.

Categories:	**Usage Information**
Description:	We retain usage information (e.g., visits to sites) in a depersonalized or aggregated form. Once aggregated, this information ceases to be Personal Information and will not be subject to user deletion requests.

10. How Can I Delete My Personal Information?

You can delete your Personal Information from Ancestry at any time.

Categories:	**Personal Information**
Description:	You can delete your Personal Information from Ancestry by following these instructions. If you have shared information with other Users (for example, by making your family trees public or by sharing your DNA Results directly with other Users), Ancestry will not be able to remove any copies of information that other Users may have retained, which can only be removed by your contacting the other User and asking them to delete it. Please direct any request to remove information from linked archival records to the responsible archival entity. We will consider requests for removal of Personal Information from the searchable indexes of the records we hold on a case-by-case basis in accordance with law. For information on Personal Information processed by Ancestry relating to non-Ancestry users please click here.
Categories:	**Genetic**
Description:	**Please note**: If you request that Ancestry delete your DNA Data, we will delete all Genetic Information, including any derivative Genetic Information (ethnicity estimates, genetic relative matches, etc.) from our production, development, analytics, and research systems within 30 days. To request the destruction of your Biological Samples, you must contact Member Services. Please note that if you have agreed to our Informed Consent to Research, we will not be able to remove your Genetic Information from active or completed research projects, but we will not use it for any new research projects.
Categories:	**General**
Description:	Please note that there may be some latency in deleting your Personal Information from our backup systems after it has been deleted from our production, development, analytics, and research systems. Also, our laboratory partners may retain information they receive from us in order to comply with laws or regulations requiring retention of certain data, such as the Clinical Laboratory Improvements Amendments regulations administered by the U.S. Food and Drug Administration. Ancestry may also retain certain information as reasonably necessary to comply with our legal obligations (including law enforcement requests), resolve disputes, maintain security, prevent fraud and abuse, as well as to comply with tax, payment industry, securities, and clinical regulatory compliance requirements.
Categories:	**Related Brands**
Description:	To delete information from our related brands (Fold3, Newspapers.com™, Find a Grave, We Remember or Archives), you can contact us at the related brand and request that your Personal Information be deleted from that service. Some Services may also have an online request form accessible from that service's account settings menu and viewable here.

11. Security

Ancestry maintains a comprehensive information security program designed to protect our customers' Personal Information using administrative, physical, and technical safeguards.

The specific security measures used are based on the sensitivity of the Personal Information collected. We have measures in place to protect against inappropriate access, loss, misuse, or alteration of Personal Information (including Genetic Information) under our control.

The Ancestry Security Team regularly reviews our security and privacy practices and enhances them as necessary to help ensure the integrity of our systems and your Personal Information.

We use secure server software to encrypt Personal Information (including Genetic Information), and we only partner with security companies that meet and commit to our security standards. While we cannot guarantee that loss, misuse, or alteration of data will not occur, we use appropriate technical and organizational measures to prevent this.

It is also important for you to guard against unauthorized access to your Personal Information by maintaining strong passwords and protecting against the unauthorized use of your own computer or device.

12. International Data Transfers

We are a global business and will transfer your Personal Information to countries other than your own country, including but not limited to the United States, Ireland, the United Kingdom and France. Countries which are outside the EEA, Switzerland or the United Kingdom may not offer the same level of data protection as in your home country. When we transfer your Personal and Genetic Information between Ancestry's Ireland-based company and Ancestry's U.S.-based companies for processing in the United States, we rely on established transfer mechanisms such as Standard Contractual Clauses.

13. Changes to This Statement

We may modify this Privacy Statement at any time, but we will provide prominent advance notice of any material changes to this Statement, such as posting a notice through the Services, on our websites, or sending you an email, to provide you the opportunity to review the changes and choose whether to continue using the Services.

We will also notify you of non-material changes to this Statement as of their effective date by posting a notice through the Services, on our websites, or sending you an email.

If you object to any changes, you may delete your account as described in Section 10.

14. Legal Bases Under EU General Data Protection Regulation for Processing Personal Information of EU Residents.

Under EU and UK law, we are required to specify the purposes for which we process your Personal Information and the legal bases which we rely on to do this. Ancestry relies on a number of legal bases to collect and process your Personal Information and Genetic Information. You can view the details of our legal bases here.

15. Identity and Contact Details of the Data Controller

Customers in the United States

If you reside in the United States, Ancestry.com Operations, L.P. and Ancestry.com DNA, LLC, are responsible for the use of your data and for responding to any requests related to your Personal Information.

Groups:	**For Users Located in the United States**
Categories:	privacy@ancestry.com
Description:	Ancestry.com Operations, L.P. Attn: Privacy Office 153 Townsend Street, Suite 800 San Francisco, CA 94107

Groups:	**US State Privacy Requests**
Categories:	usprivacyrequests@ancestry.com
Description:	N/A

Groups:	**California Authorized Agent Support**
Categories:	thirdpartyauthorizationrequests@ancestry.com
Description:	N/A

Customers Outside the United States

If you reside outside the United States, Ancestry Ireland Unlimited Company is your data controller.

Users outside of the United States may contact the Irish Data Protection Commission, or your local Data Protection Authority.

Groups:	**For Users Located Outside of the United States**
Categories:	dpo@ancestry.com

Description:	Ancestry Ireland Unlimited Company Attn: Privacy Office 52-55 Sir John Rogerson's Quay Dublin D02 NA07 Ireland

For Ancestry Customers: Ancestry customers can reach us using these phone numbers, or you may submit questions using this web form.

Law Enforcement Requests: Requests for information from law enforcement bodies should follow Ancestry's Guide for Law Enforcement.

16. US Resident Additional Privacy Statement

Ancestry provides this US Resident Additional Privacy Statement (**"US Statement"**), applicable solely to California, Colorado, Connecticut, and Virginia residents, as a supplement to our Privacy Statement, to provide information as to how you may exercise your rights under the California Consumer Privacy Act of 2018 (**"CCPA"**) the California Privacy Rights Act of 2020 (**"CPRA"**), the Colorado Privacy Act (**"CPA"**), the Connecticut Data Privacy Act (**"CTDPA"**), and the Virginia Consumer Data Protection Act (**"VCDPA"**). This US Statement covers all Ancestry websites, services, and mobile apps that link to this US Statement, including: Ancestry®, AncestryDNA, Fold3, Newspapers.com™, Archives, We Remember, and Find a Grave (throughout, collectively, as applicable **"Ancestry" "we"** or **"our"**). It applies to the Personal Information (defined above) we collect from your use of our Services and through any other means by which you engage with us.

16.1 Categories of Personal Information

Ancestry collects, and has collected in the 12 months prior to the effective date of this US Statement, the following categories of Personal Information:

- Identifiers, such as name, username, postal address, unique personal identifier, online identifier, IP address, your mobile device identifier, email address, account name, driver's license.
- Personal information described in subdivision (e) of Section 1798.80 not covered by an existing category (physical characteristics or descriptions).
- Characteristics of protected classifications under applicable state or federal law, such as assigned sex at birth and year of birth. This also includes Your Content (as defined in our Terms and Conditions) you choose to share with us that is considered a legally protected class under applicable state or federal law.
- Commercial information, such as products or services purchased, obtained, or considered or other purchasing or consuming histories or tendencies.
- Biometric information, such as DNA Data (defined above).
- Internet usage information, such as your browsing history, search history, and information regarding your interaction with our sites and advertisements.
- Geolocation data, such as location of your device or computer and any metadata associated with digital photographs uploaded to Find a Grave, including the location, date, and time the photo was taken.
- Sensory data, such as audio, electronic, and visual information (e.g., audio or video recordings you upload, recordings of calls with Ancestry Member Services or information you voluntarily share when doing consumer insights research with us).
- Inferences derived from Personal Information, such as to suggest familial relationships and to create consumer profiles for the purposes of research, product development and marketing. Please note as stated in Section 16.7 below, we do not sell your Personal Information.
- Sensitive Personal Information, such as driver's license, account login information, racial or ethnic origin, and genetic data.

Note that some categories of information are collected only if you use certain of our Services.

16.2 Business Purposes

Ancestry uses the categories of Personal Information described in Section 16.1 for the following business purposes:

- Providing, personalizing, improving, updating, and expanding Ancestry's Services;
- Communicating to you about the Services;
- Helping to ensure security and integrity of the Services; and

- Marketing new products and offers from us or our business partners based on your interests.

16.3 Categories of Sources of Personal Information

Ancestry collects, and has collected in the 12 months prior to the effective date of this US Statement, categories of Personal Information described in Section 16.1 from the following categories of sources:

- You, our user/visitor—this source of Personal Information depends on your use of the Services, including when you submit Your Content (as defined in our Terms and Conditions);
- The Ancestry Companies (defined in Section 7);
- Public records;
- Historical records; and,
- Third parties.

16.4 Disclosure of Personal Information for Business Purposes

Ancestry shares, and has shared in the 12 months prior to the effective date of this US Statement, with the following categories of third parties the correlating categories of Personal Information for a business purpose:

Categories:	**Other Ancestry Users (if you shared your Personal Information on Ancestry)**
Description:	• Identifiers; • Categories of personal information described in Section 1798.80(e) of the California Civil Code; • Characteristics of protected classes under applicable state or federal law; and, • Biometric information.
Categories:	**Ancestry Companies**
Description:	• Identifiers; • Categories of personal information described in Section 1798.80(e) of the California Civil Code; • Characteristics of protected classes under applicable state or federal law; • Commercial information; • Biometric information (only between Ancestry and AncestryDNA); • Internet usage information; • Geolocation data; • Sensory data; and, • Inferences.
Categories:	**Service Providers**
Description:	• Identifiers and categories of personal information described in Section 1798.80(e) of the California Civil Code such as email address and unique personal identifiers generated by Ancestry (tube code); • Biometric information and characteristics of protected classes under applicable state or federal law (gender, birth date) are shared with our partner laboratories; • Commercial information; • Internet usage information; • Sensory data; and, • Inferences.
Categories:	**Research Partners**
Description:	Refer to the Informed Consent to Research for information on what is shared with research partners, which may include: • Identifiers; • Categories of personal information described in Section 1798.80(e) of the California Civil Code; • Characteristics of protected classes under applicable state or federal law; • Commercial information; • Biometric information (only between Ancestry and AncestryDNA);

	• Internet usage information; • Sensory data; and, • Inferences.
Categories:	Law Enforcement **or** Other Regulatory Bodies
Description:	We do not voluntarily share your Personal Information with law enforcement or regulatory bodies. We require a valid legal process as described in Section 7 above before we would provide any data to law enforcement. For information on what data has been shared, see our bi-annual Transparency Report.

16.5 Sharing and Advertising Preferences

Ancestry shares, and has shared in the 12 months prior to the effective date of this US Statement, with the following categories of third parties the correlating categories of Personal Information for targeted advertising:

Categories:	**Marketing and Advertising Partners**
Description:	• Identifiers; • Commercial information; • Internet usage information; • Inferences.

We use cookies and similar tracking technologies to share information with our service providers and third-party partners for a variety of reasons, including to measure, target, and serve advertisements as further described in this Privacy Statement.

You can learn more about our practices and the controls we provide you or opt out of certain types of such sharing by visiting our Cookie Policy. After January 1, 2023, please visit the "Do Not Sell or Share My Personal Information" link in the footer of our sites to change your preferences.

16.6 Exercising Your Rights.

16.6.1 Right to Know. You may have the right to request that we disclose what Personal Information we collect, use, disclose, share, or sell. This includes the right to request the categories of Personal Information we have collected about you, the categories of sources of Personal Information, the business purpose for collecting Personal Information, the categories of third parties with whom we share categories of Personal Information, and the specific pieces of Personal Information we have collected about you.

If you are submitting a request to know on your own behalf, there are two ways to make your request: online or by email.

To submit your request to know for Ancestry online, follow these step-by-step instructions on how to download your account data. Please note that this report will not include a copy of your DNA Data or family trees. If you want a copy of your family trees, follow these step-by-step instructions. If you want a copy of your DNA Data, follow these step-by-step instructions. Please note that if you download your DNA Data, you do so at your own risk.

To submit your request to know for our related brands (Fold3, Newspapers.com™, Find a Grave, We Remember or Archives), you can always contact us at the related brand and, for some Services, they may also have an online request form accessible from that service's account settings menu (contact information and link to online request form, if available, are here).

To email your request to know, email us at usprivacyrequests@ancestry.com. We are required to verify your identity before providing you with a copy of your data. We will require you to provide proof of identity and current address (e.g., you may be required to provide a copy of your government-issued ID, which will be used solely to verify your identity and address).

If you are an "Authorized Agent" pursuant to the CCPA/CPRA and are submitting a request to know on behalf of one of our users, see Section 16.6.3 below.

16.6.2 Right to Delete. You may have the right to request that we delete your Personal Information.

If you are submitting a request to delete on your own behalf, there are two ways to make your request: online or by email. Note that to delete your Personal Information, you must delete your account and that once an account deletion request is completed, this process is irreversible. Your information (including, but not limited to, family trees, records, photos, and DNA Data) will be permanently deleted.

To submit your request for deletion from Ancestry online, follow these step-by-step instructions on how to delete your account. To submit your request for deletion from our related brands (Fold3, Newspapers.com™, Find a Grave, We Remember or

Archives), you can always contact us at the related brand and, for some Services, they may also have an online request form accessible from that service's account settings menu (contact information and link to online request form, if available, are here).

To email your request to delete, email us at usprivacyrequests@ancestry.com. We are required to verify your identity before we delete your data. We will require you to provide proof of identity and current address (e.g., you may be required to provide a copy of your government-issued ID, which will be used solely to verify your identity and address).

If you are an "Authorized Agent" pursuant to the CCPA/CPRA and are submitting a request to know on behalf of one of our users, see Section 16.6.3 below.

16.6.3 Authorized Agents. California residents can use "authorized agents" to make requests to know and requests for deletion. To use an authorized agent, email us at thirdpartyauthorizationrequests@ancestry.com. Note that even if a consumer chooses to use an authorized agent for a request, the consumer will still need to work directly with us to provide item 3 below:

1. Proof that the authorized agent is registered with the Secretary of State to conduct business in California.
2. Signed permission from the consumer allowing the authorized agent to act on the consumer's behalf.
3. Verification of the consumer's identity (to be made directly by the consumer to us). We will require proof of identity and California address (e.g., a copy of your government-issued ID, which will be used solely to verify your identity and address).

Please note: The report will be delivered to the consumer via their Ancestry account. Also note that the report does not include a copy of the consumer's DNA Data or family trees. If the consumer wants to download their family trees or DNA Data, see Section 16.6.1 above.

16.6.4 Right to Appeal. If you are a Colorado, Connecticut, or Virginia resident and your request to know or delete your data is denied, you have the right to appeal. You can do so by contacting us at usprivacyrequests@ancestry.com.

16.7 Selling. Ancestry does not sell your Personal Information, and has not sold it in the 12 months prior to the effective date of this US Statement.

16.8 Sensitive Personal Information. We process sensitive personal information collected about you only to provide the Services, including to:

- Maintain the quality and safety of the Services;
- Improve the Services;
- Detect security incidents;
- Resist and prosecute malicious, deceptive, fraudulent, or illegal actions directed at Ancestry, and;
- Maintain or service accounts, provide customer service, process or fulfill orders and transactions, verify customer information, process payments, provide analytic services, and provide storage.

We may also process this sensitive personal information as needed to help ensure people's physical safety and as required by applicable law.

16.9 Non-discrimination. We will not discriminate against you for exercising any of your rights under applicable US privacy regulations.

16.10 California's Shine the Light Law. California Civil Code Section 1798.83, known as the "Shine the Light" law, permits Users who are California residents to request and obtain from us a list of what Personal Information (if any) we disclosed to third parties for their direct marketing purposes in the preceding calendar year and the names and addresses of those third parties. Requests may be made only once a year and are free of charge. Under Section 1798.83, Ancestry currently does not share any Personal Information with third parties for their own direct marketing purposes.

16.11 Annual Reporting. Click here to see our annual, global Right to Know/Subject Access and Right to Delete requests.

16.12 Contact Us. If you have questions about our US-related privacy policies or practices, please contact us at usprivacyrequests@ancestry.com.

17. Australian Resident Additional Privacy Statement

If the Australian Privacy Act 1988 (Cth) (Privacy Act) applies to the handling of your Personal Information, these clauses will also apply:

- Genetic Information is considered "sensitive information" as set out under the Privacy Act. We will collect, use or disclose sensitive information about you only as permitted by law, for example where we have received your consent to do so or the collection is required or authorized by law.

- In relation to Section 8 (Your Rights and Choices Regarding Your Personal Information), you may have the right to make a complaint to the relevant privacy or data protection regulator in your jurisdiction. However, if you have any questions or concerns about our handling of your Personal Information, or if you believe we have not complied with this Privacy Statement or the relevant privacy law in your jurisdiction, we would appreciate it if you contact us in the first instance using the details in Section 15 above. We will investigate the complaint and determine what action, if any, to take.

© 1997-2022 Ancestry

FamilyTreeDNA Privacy Statement

At FamilyTreeDNA, user privacy is an extremely high priority for us and something we have taken seriously for over 18 years. At FamilyTreeDNA, we handle your Personal Information with great care and implement safeguards to protect your data.

It is our goal to be transparent about the Personal Information you provide, including your DNA Data, as well as give you the control over how it is utilized, shared, and stored.

1. Introduction

Our Privacy Statement was created to help you better understand how we collect, use, store, process, share, and transfer your Information when operating our website, software, products, and other services (collectively the "Services"). This Privacy Statement outlines our practices and the controls we give you to manage your privacy within our Services and describes the privacy practices of the FamilyTreeDNA websites that link to this Statement.

2. Consent

Account creation requires that you purchase a DNA test or upload your Genetic Information. To create an account and access our Services, you must agree to the FamilyTreeDNA Terms of Service (/legal/terms-of-service) and this Privacy Statement by clicking "Accept Terms & Complete Purchase" on the checkout page.

By clicking "Accept Terms & Complete Purchase," you are telling us that you consent to FamilyTreeDNA collecting, processing, and sharing your Personal Information as described in this Privacy Statement and any other documents referenced in this Privacy Statement. If you are signing in to your account for the first time as a result of someone purchasing the kit on your behalf, you are agreeing to this Privacy Statement and our Terms of Service by use of the Service.

At any time, you can request that FamilyTreeDNA remove information you have uploaded into your account, such as your Genetic Information or a family tree. Please see Section 7 "Your options" for specific details about deleting your data.

3. The types of Information FamilyTreeDNA collects

A. **Information you provided directly to us and information related to our genetic testing services:**

i. **Personal Information:** Information that can help identify you. FamilyTreeDNA collects and stores the following types of personal information to provide you the Services:

a. **Account Information:** Information you provided about yourself when purchasing/and or registering our Services. This includes name, email, phone number, kit ID and password, billing and shipping address, and payment information.

b. **Genetic Information:** Readable DNA Data. After receiving your cheek swab in the return envelope included in your kit, we extract your DNA from your cheek swab in our in-house laboratory. From here, we convert your DNA into readable DNA Data.

c. **A note about your DNA sample:** Once our laboratory has produced your DNA Data, the samples are stored so that they can be attainable for future testing. Future testing may be done if you consent to future testing of your sample or if you otherwise agree to our Informed Consent for Research.

d. **Profile Information:** We gather the information you use to create a user profile. Depending on your share settings, this information may be seen by other FamilyTreeDNA users. This can include your sex, profile image, name, location, etc.

e. **User Provided Content:** All information you present about yourself or other individuals, living or deceased, when you voluntarily participate in the Services, Group Projects, or Forums. For example, User Provided Content includes any post or message you place on FamilyTreeDNA community forums.

f. **Self-Reported Information:** Information about yourself that you submit into forms, surveys, or features while signed in to your FamilyTreeDNA account. For example, family history information or ethnicity.

g. **Website Behavior Information:** Information on how you use the FamilyTreeDNA website obtained through cookies, log files, and web beacon technology. This may include information like browser type, domains, and page views.

h. **Additional User Information:** All information given to us when you answer online questionnaires or email surveys provided through the Services.

ii. **Communications with Customer Service:** When you contact our Customer Service center or correspond with us about our Service, we collect information to: track and respond to your query, investigate any breach of our policies or regulations, and analyze and improve our Services.

iii. **Aggregate Information:** Information that has been combined with that of other users and analyzed or assessed as a whole, such that no specific individual may be reasonably identified.

iv. **Pseudonymous Information:** Information that has been stripped of your Account Information and other identifying data, such that you cannot easily be identified as an individual to the public, and is instead only identifiable by a kit number or other alphanumeric sequences.

B. **Information FamilyTreeDNA collects through the use of the Services via tracking technology:**

i. **Web Behavior Information:** Information on how you use the FamilyTreeDNA website obtained through cookies, log files, and web beacon technology. We, as well as our third-party partners, use cookies and other technologies to help us identify you, personalize the Services and our offers to you, determine the success of marketing campaigns, provide security, evaluate Service usage, collect demographic information about users, and to deliver targeted advertising on our site and on other sites.

ii. **Computer and Mobile Device Information:** We receive certain information and store it in log files. This may include how you access our Services, including the website you visited before landing on FamilyTreeDNA, your exit page, your Internet protocol (IP) address, your web browser, your computer operating system, your Internet Service Provider (ISP) or the mobile device you use to access the Internet. This log information may be combined with other information we collect about you, such as your kit number or invoice number. We do this to better the services we offer you, and to improve marketing, analytics, and site functionality.

C. You may adjust your settings as described in our Cookie Policy if you do not want us to use data about your interests or behaviors to serve you targeted ads. For information on "Do Not Track," please see our Cookie Policy (/legal/cookie-policy).

D. Third parties that we partner with to display advertising based upon your Web browsing activity or that we use to allow particular features on our site use Flash Cookies to gather and store information.

E. Please see Section 5.G., below, to learn more about our third-party advertising partners.

F. **Google Analytics:** Google Analytics is used to perform many of the tasks listed above.

G. **Other Types of Information:** We are always working to strengthen our Services with new products, features, and applications that may result in the acquisition of new types of information. We will update our Privacy Statement as needed.

4. How does FamilyTreeDNA use your information

FamilyTreeDNA will use and share your personal information with third parties in the ways that are described in this Privacy Statement.

A. **FamilyTreeDNA uses your Personal Information to provide, personalize, analyze, and improve our Services:** These acts may include, in addition to other things not specifically mentioned, using your information in a manner consistent with other commitments in this Privacy Statement to:

   i. Open an account, processing payments for FamilyTreeDNA services and test kits, and communicate with you about the Services;

   ii. Process and deliver your genetic testing results;

   iii. Perform research & development, which may include, for example, conducting data analysis and research in order to develop new or enhance existing products and services, and performing quality control activities;

   iv. Dispense surveys and questionnaires to collect Additional User Information for use in the Services, as well as facilitating product development and research initiatives;

   v. Conduct analytics to improve our Services and track the usage of our Services;

   vi. Offer new products or services to users through emails and promotions;

   vii. Comply with the law and requests from government bodies; and

   viii. Carry out online marketing campaigns and targeted advertising, including utilizing third-party ads (subject to your cookie settings), and to measure the performance of our marketing and targeted advertising.

B. **FamilyTreeDNA uses your Genetic Information for the following primary purposes:** This may include, in addition to other things not specifically mentioned, using your information in a manner consistent with other commitments in this Privacy Statement to:

   i. Deliver DNA matches (e.g., close relatives or distant cousins) from our database, ethnicity results, and other information to assist you in learning more about yourself and your genetic relatives;

   ii. Connect you with your relatives in our database through features such as DNA matching or other product features;

   iii. Present you with other insights into what your DNA uncovers about traits, personal health and wellness;

   iv. Based on your DNA Data, invite you to participate in optional surveys;

   v. Provide relevant results to aid you in identifying common ancestors and other information about your family history, as well as helping you unite with family;

   vi. Examine aggregated Genetic Information to gain further understanding of population and ethnicity-related health and wellness

   vii. Perform statistical, scientific, and historical research;

   viii. Comply with requests from law enforcement or their authorized representatives that meet our Law Enforcement Guidelines (/legal/law-enforcement-guide);

   ix. Strengthen features and functionality in our existing DNA-related products, enhancing the customer experience across FamilyTreeDNA products, improving the quality of our laboratory technology and processes, and building new products and services, including services akin to personal health and wellness.

You may be able to adjust your preferences of having your information used for specific activities. See the below Section 5 to learn more.

We will seek additional consent from you before we collect and process Sensitive Information as part of your interaction with the Services.

5. How FamilyTreeDNA shares your information

FamilyTreeDNA does not share your individual Personal Information with third parties without your additional consent other than as described in this Privacy Statement. We will never share your Genetic Information with pharmaceutical or insurance companies, employers, or third-party marketers without your express consent. The circumstances described below explain when sharing might occur:

A. **FamilyTreeDNA users or others you may choose to share with:** Depending on your account settings, your FamilyTreeDNA Profile Information (see section 3.A.i.d) and your public family tree details, may be viewable to other FamilyTreeDNA users, including your DNA matches and matches whose accounts are managed by law enforcement (dependent on your matching preferences). If you consent to participate in matching and depending on your additional settings, some of your Genetic Information may be viewable to your DNA matches, including matches whose accounts are managed by law enforcement, as well as your mutual matches. You may review this information in the Learning Center and make adjustments in your Privacy & Sharing settings. In addition to the Personal Information mentioned in this section, Group Project Administrators of Group Projects you have chosen to join or Group Projects your matches have chosen to join, will be able to view certain DNA results (e.g., Y-DNA and mtDNA markers). Pseudonymized DNA marker information can also be shared publicly via any Group Project you chose to join. To change your settings, please go to the links below in Section 7.A.

   To share details of your family history or DNA information outside the Services, means to do so at your own risk.

B. **Information shared with commonly owned entities:** Some or all of your information may be shared with other companies under common ownership or control of FamilyTreeDNA, which may include our corporate parent, our subsidiaries, or any other subsidiaries owned by our corporate parent to provide you better service and improve user experience.

C. **Service Providers:** We use the services of other companies to help us provide the Services to you. As a result, these partner companies will have some of your information in their systems. Our partners act only at the direction of FamilyTreeDNA and are subject to contractual obligations governing data security and confidentiality consistent with this Privacy Statement and applicable laws. These partners include our DNA test shipping providers, credit card processors, cloud services infrastructure providers, and vendors that assist us in marketing, analytics, fraud prevention, and Member Support.

D. **For Legal or Regulatory Process:** We may use the information you have provided to us in order to comply with the law and requests from government bodies. This means that we may provide information that we collect from you if that information is relevant to a court subpoena or to a law enforcement authority or other government investigation, provided this is permissible under applicable data protection law.

   We may share your Personal Information if we believe it is reasonably necessary to:

   i. Enforce or apply the FamilyTreeDNA Terms and Conditions;

   ii. Comply with a valid legal process (e.g., subpoenas, warrants, etc.) and other requests from or on behalf of law enforcement that comply with our Law Enforcement Guidelines (/legal/law-enforcement-guide);

   iii. Protect the security or integrity of the Services; or

   iv. Protect the rights, safety, or property, of FamilyTreeDNA, our employees or users.

If compelled to disclose your Personal Information to law enforcement, we will do our best, unless prohibited by law, to provide you with notice.

E. **Investigative Genetic Genealogy Matching (IGGM):** For requests made by law enforcement and their authorized representatives that meet the requirements of our Law Enforcement Guidelines (/legal/law-enforcement-guide), FamilyTreeDNA may create limited access law enforcement accounts ("LE Accounts") which are permitted to upload genetic information to the database to identify the remains of a deceased individual or to identify the perpetrator of a homicide or sexual assault. FamilyTreeDNA will track Law Enforcement Accounts via an in-house identification system that will allow users to opt out of Investigative Genetic Genealogy Matching.

   Users will only be viewable to the law enforcement account if ALL of the following requirements are met:

   - The user has opted into matching
   - The user has not opted out of Investigative Genetic Genealogy Matching
   - The user and the law enforcement account have the same matching levels selected
   - The user is genetic relative (also referred to as a match or DNA relative) to the genetic file uploaded to the law enforcement account

   If a law enforcement account is a genetic relative and meets the above requirements, the information of yours that they will have access to is identical to that of your other matches. For further information on what Personal Information matches may see (/learn/ftdna/information-shared-with-matches/), please visit the Learning Center.

   Law enforcement accounts cannot join or participate in Group Projects. If you opt out of Investigative Genetic Genealogy Matching, law enforcement accounts will not be able to see you as a match or view any personal information viewable by matches. You have the ability to adjust your Investigative Genetic Genealogy Matching preferences at any time in your Privacy & Sharing settings located in your Account Settings.

   Please note, if you decline to participate in Investigative Genetic Genealogy Matching, we may still be required to share your Personal Information to comply with a valid legal process as described in Section 5.D. Investigative Genetic Genealogy Matching is only permitted with accounts set up by FamilyTreeDNA on behalf of law enforcement authorities and their authorized representatives. Any other use of the matching database for law enforcement purposes violates our Terms of Service (/legal/terms-of-service). Although FamilyTreeDNA relies on law enforcement officials and authorized representatives to identify themselves when requesting use of the site and FamilyTreeDNA has implemented controls to identify and prevent uses of the Services which violate our Terms of Service (/legal/terms-of-service), FamilyTreeDNA cannot guarantee that law enforcement officials and their authorized representatives follow the requirements stated in our Terms of Service (/legal/terms-of-service) and Law Enforcement Guidelines (/legal/law-enforcement-guide). Use of the Service for law enforcement purposes is a privilege, not a right. FamilyTreeDNA reserves the right to revoke law enforcement's account access for any reason without warning, including any use of the account for any law enforcement purpose not expressly agreed to by FamilyTreeDNA.

F. **If FamilyTreeDNA is acquired:** If FamilyTreeDNA or its businesses are acquired or transferred to another entity (in part or in whole and including in connection with any bankruptcy or similar proceedings), we will share your Personal Information with that entity. The promises in this Privacy Statement will apply to your Personal Information as transferred to the new entity.

G. **"Targeted Advertising" service providers:** We allow third-party advertising networks and providers to collect Web Behavior Information on our Service to help us to deliver targeted online advertisements to you. Using cookies and similar technologies (such as JavaScript, web beacons, device identifiers, location data, and clear gifs), they collect information about your browser's or

device's visits and usage patterns on our Services and on other websites over time. This helps us better personalize ads to match your interests and to measure the effectiveness of ad campaigns.

You may have the option to change your settings as described in our Cookie Policy if you do not wish us to use data about your interests or behaviors to serve you targeted ads. For information on "Do Not Track" please see our Cookie Policy (/legal/cookie-policy).

For more information about our marketing and advertising practices, please review our Cookie Policy (/legal/cookie-policy).

H. **Aggregate Information:** FamilyTreeDNA may show user information in an aggregated form as part of the Services or our marketing, or in scientific publications published by our research partners or us. Such disclosure will never include Personal Information

I. **Research Partners:** We do not share, trade, or barter your genetic information. If at any point in the future we change our policy in regards to research partners, we will ask for your express consent to share your Genetic Information with any research partner.

6. Using information for research with your consent

You have the choice to participate in future genetic research opportunities.

A. **Consent process for research:** Users wishing to participate in genetic research projects may indicate so and will be included in a candidate pool. If you become a potential candidate for a research project, you will be contacted to grant specific consent for every individual research project opportunity. Once given, consent cannot be revoked for research that has already occurred or is underway.

B. **If you no longer consent to FamilyTreeDNA Research:** Consent for future research can be revoked by notifying FamilyTreeDNA that you wish to be removed from the candidate pool or by declining invitations to participate in specific research projects. Removing yourself from the research candidate pool means that you will not receive any invitations to participate in research projects.

7. Your options and ability to access to your personal information

Subject to particular exceptions, you have a right to request access to your Personal Information and to be given a copy of certain information you provided in a portable format, as well as to seek to update, delete, or correct this information by using the tools described below or by contacting FamilyTreeDNA. Details and options for obtaining this information are below.

A. **Access to your account:** FamilyTreeDNA also provides privacy and security settings that allow you to control the visibility of your personal data to your matches and in any Group Project that you have joined. You have access to and may update the Personal Information (such as name, email address, profile information, etc.) that you provide to FamilyTreeDNA at any time in the following sections of the profile settings: Account Information (/my/account-information), Privacy & Sharing (/my/privacy-sharing), Project Preferences (/my/project-preferences), Genealogy (/my/genealogy), and Notification Preferences (/my/notification-preferences). To learn more about how to manage your privacy settings, click here (https://www.familytreedna.com/learn/user-guide/my-account/my-privacy-and-sharing-page/).

Testers have the option to assign a beneficiary to their account in the event that they become deceased. Only in the event that FamilyTreeDNA is notified about a deceased tester, will account information be shared with the specified beneficiary. In the case that a beneficiary is not specified and upon verification of the deceased user, ownership may default to FamilyTreeDNA. To learn more about managing beneficiary settings, you can click here (https://learn.familytreedna.com/user-guide/my-account/my-account-information-page/).

To learn more about managing privacy settings for family trees you have created on FamilyTreeDNA, you can click here (/my/privacy-sharing).

B. **Marketing Communications:** By creating an account, you are agreeing that we may send you promotional emails about our Services. You have the option to opt out of receiving specific messages or notifications from us by visiting your Notification Preferences (/my/notification-preferences) in your account. You also have the option to click "unsubscribe" at the bottom of promotional email communications. Please note that you may not opt out of receiving non-promotional messages regarding your account, such as Service-related emails or purchase confirmations.

C. **Genetic Information Download:** Your DNA Data belongs to you. You always have the option of downloading files with your DNA Data. Learn how here (https://www.familytreedna.com/learn/ftdna/how-to-access-and-download-your-raw-data-files/). For more information on what is included in your DNA Data downloads, go here (https://www.familytreedna.com/learn/ftdna/how-to-access-and-download-your-raw-data-files/).

D. **Information you choose to share with others:** FamilyTreeDNA gives you the ability to share information with other individuals who have FamilyTreeDNA accounts through (i) our community forums, (ii) relative finding features (e.g., "Matches"), (iii) Group Projects, and (iv) other sharing features. Please refer to settings in your profile. Some sharing may require you to opt in, but some features may require an opt out, such as Investigative Genetic Genealogy Matching. For example, we provide the ability to opt in to share your ethnicity results (myOrigins®) with your DNA Matches. Alternatively, if you have consented to participate in the DNA Matching Database, you may opt out or change the visibility of your profile information by visiting your Settings. Also, please note that certain types of your User Provided Content may be viewable by other FamilyTreeDNA users, and once posted, you may not be able to modify or delete certain content.

   You may choose to disclose your personal information to family members and/or friends and/or other individuals outside of our Services, including through third-party services such as social networks and third-party apps that connect to our website through our application programming interfaces ("API"). These third parties may use your personal information differently than we do under this Privacy Statement. Please make such choices carefully and review the privacy policies of all other third parties involved in the transaction.

   Personal information, once disclosed or shared, can be difficult to contain or retrieve. FamilyTreeDNA will have no liability or responsibility for any consequences that may result because you have released or shared personal information with others. If you have access to the personal information of a FamilyTreeDNA customer through an account you manage, we urge you to recognize your responsibility to protect the privacy of the person in the account. It is the responsibility of all users to share personal information and account access only with people they know and trust. Users managing multiple accounts should use caution in selecting profile settings.

E. **Participation in Group Projects**

   FamilyTreeDNA gives you the ability to participate in Group Projects and to share information with other Project Members and Group Project Administrators. Information that you have shared as part of your participation in a Group Project is shared at your own risk, and FamilyTreeDNA will not be obligated to remove any information or User Provided Content that may be made public as part of your participation.

   Group Projects may have public pages displaying pseudonymized member results so that members can share information more easily. This may include Group Project member results by kit number. Group Project pages may include participant surnames, oldest known ancestors, and their country of origin.

   Any changes you make to your permissions or privacy settings can experience a delay when updating on such public pages. For more information on Group Project participation, please see Group Project Participation Terms (/legal/terms/group-project-participation).

F. **How to leave a Group Project, delete your Personal Information, or close your FamilyTreeDNA account:**

i. **How to leave a Group Project:** You may leave a Group Project at any time by clicking the relevant "Leave" box(es) on your Project Preferences page or by sending an email to groups@familytreedna.com advising which project you wish to leave. We will comply with such requests within a reasonable timeframe and will send an email to the Group Project Administrator(s) requesting that they erase your public-facing information from any website maintained outside of FamilyTreeDNA as well as any of your data from their files. If you have posted information to a Group Project's forum, whether maintained by FamilyTreeDNA or elsewhere, or to any social media platform, Group Project Administrators will not have the ability to remove said posts.

ii. **How to delete your Personal Information:** Deleting your personal information from FamilyTreeDNA can be done in different ways through the settings linked above in section 7.A. of this document.

If you need support deleting the Personal Information you provided in your profile, please contact Customer Service (/contact).

If you have shared information through the Services, such as sharing your results directly with other Users or a Group Project Administrator, FamilyTreeDNA will not have the ability to delete any copies of information other FamilyTreeDNA members may have received, nor will FamilyTreeDNA be obligated to delete posts from the Activity feed.

iii. **How to delete your Genetic Information:** If you no longer wish for us to have your Genetic Information, please contact Customer Service (/contact) with your request, and we will remove all Genetic Information (DNA matches, ethnicity estimates, etc.) from your account (or profile) within a reasonable timeframe of your request.

To request the destruction of your swab samples, please contact Customer Service (/contact).

iv. **How to close your FamilyTreeDNA account:** You may request at any time to close your FamilyTreeDNA account and for your DNA test results and contact information to be deleted from FamilyTreeDNA. To close your account, please contact Customer Service (/contact).

As stated in any applicable Research Consent Document, however, Self-Reported Information and/or Genetic Information that you have already provided and for which you have given consent to use in FamilyTreeDNA Research cannot be deleted from ongoing or completed studies that use the information. However, your information will not be used for any future research projects.

We may retain limited information as reasonably necessary to resolve disputes, prevent fraud, comply with legal obligations, as well as to comply with accounting and audit purposes, and clinical regulatory compliance requirements.

FamilyTreeDNA acknowledges that individuals have the right to access the personal information that we maintain about them. An individual who seeks access or who seeks to correct, amend, or delete inaccurate or all data, should contact us at ombudsman@genebygene.com. If your request is for the removal of data, we will respond within a reasonable timeframe.

8. Important Information

A. **Privacy Shield:** FamilyTreeDNA has certified its compliance with both the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union (EU), European Economic Area (EEA), United Kingdom and Switzerland to the United States, respectively. FamilyTreeDNA is committed to subjecting all personal data received from the EU member countries, EEA, United Kingdom and Switzerland, in reliance on the Privacy Shield Frameworks, to the Framework's applicable Principles. If there is any conflict between the terms in this privacy policy and the

Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, listed under Gene By Gene, Ltd., please visit U.S. Department of Commerce's Privacy Shield List (https://www.privacyshield.gov/list).

FamilyTreeDNA's accountability for personal data that it receives under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. In particular, FamilyTreeDNA remains responsible and liable under the Privacy Shield Principles if third-party agents that it engages in processing the personal data on its behalf do so in a manner inconsistent with the Principles unless FamilyTreeDNA proves that it is not responsible for the event giving rise to the damage.

In compliance with the EU-US and Swiss-US Privacy Shield Principles, Gene by Gene commits to resolve complaints about your privacy and our collection or use of your personal information. Complaints regarding this privacy policy should first contact FamilyTreeDNA at:

Privacy Administrator
FamilyTreeDNA
1445 N Loop Suite 820
Houston, TX 77008
ombudsman@genebygene.com

FamilyTreeDNA has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://www.bbb.org/EU-privacy-shield/for-eu-consumers (https://www.bbb.org/EU-privacy-shield/for-eu-consumers) for more information and to file a complaint.

FamilyTreeDNA is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

Please note that if your complaint is not resolved through these channels, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

B. **Security:** FamilyTreeDNA places great importance on the security of all our customers' information. We have reasonable and adequate security measures in place to attempt to protect against the loss, misuse, or alteration of customer data under our control. For example, our security and privacy practices are periodically reviewed and enhanced as necessary and only authorized personnel have access to Personal Information. We use secure server software to encrypt financial information you input before it is sent to us and we only work with third parties who have met and commit to our security standard. While we cannot guarantee that loss, misuse or alteration of data will not occur, we use commercially reasonable efforts to prevent this.

C. **Business Transactions:** In the event that FamilyTreeDNA goes through a business transition such as a merger, acquisition by another company, or sale of all or a portion of its assets, your information will likely be among the assets transferred. In such a case, your information would remain subject to the promises made in any pre-existing Privacy Statement.

D. **Linked Websites:** FamilyTreeDNA provides links to third-party websites operated by organizations not affiliated with FamilyTreeDNA. FamilyTreeDNA does not disclose your information to organizations operating such linked third-party websites. FamilyTreeDNA does not review or endorse and is not responsible for the privacy practices of these organizations. We encourage you to read the Privacy Statements of each and every website that you visit. This Privacy Statement applies solely to information collected by FamilyTreeDNA.

E. **Children's Privacy:** FamilyTreeDNA is committed to protecting the privacy of children as well as adults. Neither FamilyTreeDNA nor any of its Services are designed for, intended to attract, or directed toward children under the age of 18. A parent or guardian, however, may collect a DNA sample from, create an

account for, and give information related to his or her child if they are between the age of 13 and 18. The guardian or parent assumes full responsibility for ensuring that the information that he/she shares with FamilyTreeDNA about his or her child is kept secure and that the information submitted is accurate.

F. **Changes to Privacy Statement:** We may choose to modify this Privacy Statement at any time. We will provide advance notice of any material changes to this Statement, such as sending you an email or posting a notice to allow you the opportunity to survey the changes and decide whether to continue using our Services.

   Non-material changes to this Statement will be notified as of their effective date by posting a notice through the Services on our website or by sending you an email. After notice of non-material changes, your continued use of our Services means that you consent to the updated Privacy Statement.

Read the previous version of this document. (/legal/privacy-statement/02242022) *Last updated 02/24/2022*

All Contents Copyright 2001-2022 Gene by Gene, Ltd.

rvice and Privacy Policy

Effective Date: December 30, 2021

We have updated these Terms of Service and Privacy Policy. Below is a summary of our updates:

- **Applicable privacy laws**: We made updates to include required disclosures in accordance with applicable privacy laws, including California's Genetic Information Privacy Act.
- **Payment terms:** For users who opt to use our paid services, we've updated our payment terms, including to account for our annual recurring payment plans (in addition to our monthly recurring payment plans).
- **Transparency**: We've made our terms more transparent and understandable for you. For example, we have updated the "DNA Data" section to include clarifying language regarding privacy settings consistent with the language on our DNA upload page. Note that we are not changing how your information is used or shared. Your opt-in and opt-out settings remain unchanged.
- **Location of servers**: We've updated our language to clarify that your personal data may, in the future, be hosted on EU servers in addition to U.S. servers.

By continuing to use GEDmatch, you consent to our Terms of Service and Privacy Policy. As always, you may stop using GEDmatch any time, and you may delete your information through the settings in your account.

As of December 9, 2019, GEDmatch is operated by Verogen, Inc. ("Verogen") following the acquisition by Verogen of the GEDmatch website.

Verogen respects your privacy and recognizes the importance of your personal information. We are committed to protecting your information through our compliance with these Terms of Service and Privacy Policy.

You may print a copy of these Terms and Service and Privacy Policy by clicking here. If you have a disability, you may access this policy in an alternative format by contacting GEDmatch@verogen.com.

This Privacy Policy describes our practices in connection with information we may collect through your use of our website (our 'Site'). By using our Site, you consent to our collection and use of the information described in this Privacy Policy.

GEDmatch Collection and Use of Information

When you register on GEDmatch, we collect your name, an optional alias, and email address to process your registration. Once you are registered, you can provide other personal information such as your sex, Y-DNA or mtDNA haplogroup, genetic sequence/information, Genealogy data, and/or Tier1 payment information. GEDmatch will only collect your personal information if you provide it to us voluntarily. If you are located outside the United States, you consent to the storage, processing, and transfer of your personal information outside your country.

In addition, we automatically collect certain information regarding visitors to our Site, including IP address, information about your equipment, browsing actions, and usage patterns. The information we collect automatically is statistical data and does not include personal information. We use this information solely for internal purposes, such as to improve our Site.

Our Site may use third party tools to help us understand, in aggregate, the age, gender and interests of Site visitors. These tools do not reveal to GEDmatch your name or other identifying information. GEDmatch does not combine the information collected through use of these tools with personally identifiable information. The information received from these tools is used only to improve our Site and the type of information displayed to Site visitors so we can better serve those interested in GEDmatch.

GEDmatch offers you opportunities to engage in forums that are designed to be visible to other users, including comments and postings. You should be aware that any personally identifiable information you choose to submit via these forums can be read,

We may disclose your Raw Data, personal information, and/or Genealogy Data if it is necessary to comply with a legal obligation such as a subpoena or warrant. We will attempt to alert you to this disclosure of your Raw Data, personal information, and/or Genealogy Data, unless notification is prohibited under law.

der the age of 13. GEDmatch does not knowingly collect any ved personal information from a child under 13 without verification of parental consent, we will delete that information.

GEDmatch purpose

GEDmatch exists to provide DNA and genealogy tools for comparison and research purposes. DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this Site agree that their information will be shared with other users.

Raw DNA Data Provided to GEDmatch

If you are a law enforcement officer or if you are working on behalf of a law enforcement officer, you agree you will not upload Raw Data to GEDmatch via the GEDmatch.com website; instead, please click here to upload Raw Data via the GEDmatch Pro portal to identify the perpetrator of a Violent Crime (where 'Violent Crime' is defined as murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault) or to identify human remains.

When you upload Raw Data to GEDmatch, you agree that the Raw Data is one of the following:

- Your DNA;
- DNA of a person for whom you are a legal guardian;
- DNA of a person who has granted you specific authorization to upload their DNA to GEDmatch;
- DNA of a person known by you to be deceased; or
- DNA obtained from an artifact (if and only if: (1) you have a reasonable belief that the Raw Data is DNA from a previous owner or user of the artifact rather than from a living individual; and (2) that previous owner or user of the artifact is known to you to be deceased).

By registering for GEDmatch and using the Site, you agree that you will not upload Raw Data that does not satisfy one of these categories. If you have previously uploaded Raw Data that does not satisfy one of these categories, you hereby agree that you will remove it immediately.

GEDmatch will not be responsible for any Raw Data provided to GEDmatch in violation of this Policy. Violators of this Policy will have their Raw Data or other personal information deleted without warning, their access will be blocked, and/or other remedial steps may be taken, including any legal action allowed under law.

Privacy

Although you may provide a real name for registration and data upload, you have the option of providing an alias for either login or data. If an alias has been provided, it will be displayed in place of the real name along with results. If DNA data you provide is linked to your Genealogy Data, and only one or the other uses an alias, it may be possible for users to see the real name in the linked data.

In today's world, there are real dangers of identity theft, credit fraud, etc. We try to strike a balance between these conflicting realities and the need to share information with other users. In the end, if you require absolute privacy and security, you agree that you will not provide your personal information, Raw Data, or Genealogy Data to GEDmatch. If you do not agree and you have already provided your personal information, Raw Data, or Genealogy Data, you agree to delete it immediately.

Security

Although GEDmatch has endeavored to create a secure and reliable Site for you, the confidentiality of any communication, material, or personal information provided to GEDmatch via the Site or email cannot be guaranteed.

The original Raw DNA and GEDCOM data you provide to GEDmatch is not kept in its original form. It is converted to a form that makes it more efficient for the software to perform searches and comparisons. The Genealogical Data is loaded into a relational database that might still be recognizable as text. The Raw DNA is converted to a compressed binary format in a process we call 'tokenization.' Although the Raw DNA is not encrypted in the usual sense of the word, it would be very difficult for a human to read it. Original uploaded files are deleted from the Site servers soon after they are processed and archived.

We encrypt your login password before putting it in our database. We cannot tell what your password is. However, there have been cases in the news of encrypted data being hacked and decoded. Be aware that may be a possibility on this or any other Site. We take measures to ensure that only registered users have access to your results, but those measures have not been and never will be perfect.

recovery plan. When a registered GEDmatch user deletes or requests deletion of Raw Data, Genealogy Data, and/or profile information, copies of that information stored in an archive copy will be deleted upon storage of an updated archive copy, no later than 30 days after the user request.

pplications. Additionally, state genetic data privacy laws require us to provide you with notice that your deidentified genetic or phenotypic information may be shared with or disclosed to third parties for research purposes in accordance with Part 46: Protection of Human Subjects (commencing with Section 46.101) of Title 45 of the Code of Federal Regulations. **However, please note that we will not share with or disclose to third parties your deidentified genetic or phenotypic information for research purposes pursuant to Part 46.**

Email addresses

Everybody who registers with the Site must provide a valid email address for the principal contact. It provides log-in verification and allows GEDmatch to contact them if necessary. It also provides a mechanism to verify your identity if you want to contact GEDmatch. You agree to keep your log-in information secure, and to keep your email address up to date.

Your email address and name (or alias, if provided) will be displayed along with any matches to your Raw Data or Genealogy Data. Some users obtain an email address separate from their primary email for this purpose.

You understand that any registered GEDmatch user using the tools available on the Site may gain access to the email address you provide.

Tier1 Payment Information

You may voluntarily obtain access to Tier1 tools on the Site for the recited amount (subject to change). You may provide a one-time payment of any amount, followed by a recurring amount as agreed to by you. By choosing a recurring pament plan, you acknowledge that such Tier1 tools have an initial and recurring payment feature and you accept responsibility for all recurring charges prior to cancellation. WE MAY SUBMIT PERIODIC CHARGES (I.E., MONTHLY OR ANNUALLY) TO CHARGE YOUR PAYMENT METHOD, EITHER DIRECTLY OR THROUGH OUR PAYMENT PROCESSORS WITHOUT FURTHER AUTHORIZATION FROM YOU, UNTIL YOU PROVIDE PRIOR NOTICE (RECEIPT OF WHICH IS CONFIRMED BY US) THAT YOU HAVE TERMINATED THIS AUTHORIZATION OR WISH TO CHANGE YOUR PAYMENT METHOD. SUCH NOTICE WILL NOT AFFECT CHARGES SUBMITTED BEFORE WE REASONABLY COULD ACT. TO TERMINATE YOUR AUTHORIZATION OR CHANGE YOUR PAYMENT METHOD, GO TO YOUR ACCOUNT SETTINGS OR VIEW THE INSTRUCTIONS FOR CANCELLING A RECURRING PAYMENT AVAILABLE IN THE GEDMATCH WIKI. Payments may also be provided by personal check to Verogen, Inc., Attn: Accounting Department, 11111 Flintkote Avenue, San Diego, CA 92121. You understand that your personal account information will be made available to Verogen when paying by personal check.

Unless you opt out of auto-renewal, which can be done through your account settings, any Tier1 tools you have signed up for on a Auto Renewal basis will be automatically extended for successive renewal periods of the same duration as the subscription term originally selected, at the then-current non-promotional rate. To change or resign your access to Tier1 tools at any time, go to account settings. If you terminate access to Tier1 tools, you may use your subscription until the end of your then-current term, and your subscription will not be renewed after your then-current term expires. However, you will not be eligible for a prorated refund of any portion of the subscription fee paid for the then-current subscription period. If you do not want to continue to be charged on a AUTO RENEWAL basis, you must cancel the applicable Paid Service through your account settings or terminate your account before the end of the recurring TERM. Paid Services cannot be terminated before the end of the period for which you have already paid, and except as expressly provided in these terms, GEDMATCH WILL NOT REFUND ANY FEES THAT YOU HAVE ALREADY PAID UNLESS GEDMATCH DETERMINES (IN ITS SOLE DISCRETION) THERE ARE UNUSUAL OR EXTENUATING CIRCUMSTANCES THAT WARRANT AN ISSUANCE OF A FULL OR PARTIAL REFUND.

Your non-termination or continued use of Tier1 tools reaffirms that we are authorized to charge your payment information for such Tier1 tools. We may submit those charges for payment and you will be responsible for such charges. This does not waive our right to seek payment directly from you. Your charges may be payable in advance, in arrears, per usage, or as otherwise described when you initially selected to use the Tier1 tools.

GEDCOMs

GEDCOMs (family trees) or other genealogy ('Genealogy Data') provided to GEDmatch remain the property of the person who uploaded it. When you upload your Genealogy Data, you will be provided a unique ID number for that GEDCOM. If you want your Genealogy Data removed from the Site, you may do so yourself by clicking on the 'Manage your resources' link on your home page. If you need assistance deleting a Genealogy Data, contact the Site administrator at GEDmatch@verogen.com.

Genealogy research requires the exchange of information. For that reason, all Genealogy Data provided to GEDmatch can be viewed, searched, and compared by any GEDmatch user.

[GED match]

Home How It Works Applications Education About Us Support

JOIN FOR FREE SIGN IN

individuals before uploading to GEDmatch by changing the name(s) of living individual(s) to 'LIVING'. Upon an upload of a GEDcom to GEDmatch we will automatically review and change the privacy setting for the Genealogy Data of individuals in your GEDcom to "HIDDEN" if we believe such individuals are alive based on birth or death dates. The owner of a GEDcom will see the Genealogy Data of all individuals in their GEDcom that are both alive and deceased; other users will only see the Genealogy Data of deceased individuals.

However, we cannot guarantee that your information will never be accessed by individuals other than GEDmatch users. If you require absolute security, you agree that you will not upload your Genealogy Data to GEDmatch. If you have already uploaded it, you agree to delete it immediately.

You will be given the opportunity to link your Genealogy Data with other DNA data you provide. This is a powerful tool and we encourage people to use it. It also provides a means of access to your Genealogy Data to people who may have no Genealogy Data of their own at GEDmatch. It will also enable identification of individuals within the provided Genealogy Data, even if the individuals are not identified in the Genealogy Data.

DNA Data

DNA data uploaded to GEDmatch.Com ('Raw Data') remains the property of the person who uploaded it. When you upload Raw Data, a kit number will be assigned at the end of the upload process and you will be prompted to select a privacy option for the DNA kit. This number is unique to the individual DNA upload, and will be used on the pages of this Site to identify your data, including being provided to anyone that shares DNA with the Raw Data. If you wish to contact the Site administrator regarding your data, you must provide the kit number associated with your data. A link or other means is provided within your GEDmatch account to remove your data from the Site. Alternatively, you can request deletion of your personal information at any time by contacting us at GEDmatch@verogen.com. It is possible that an old kit number may be reassigned to another user's uploaded data in the future if you delete your Raw Data.

No means are provided on the Site to make Raw DNA or other DNA data available for download.

There are 4 classes of privacy options for the DNA kit on this Site: 'Private', 'Research', 'opt-in' and 'opt-out'. You will be asked to select which category will apply when you upload DNA data. If you ever want to change the category, use the pencil icon link next to the kit number on your home page.

'Private' DNA kits will not be available for any matching comparisons with other people. No comparison results will be shown unless this privacy setting is changed by you later.
'Opt-in' We will compare your DNA kit to all other kits in the GEDmatch database to find your matching genetic relatives. Kits in the database include those submitted by users undertaking personal genetic genealogy research, adoptee searches, users (including law enforcement) attempting to identify unidentified human remains, and law enforcement attempting to identify perpetrators of violent crimes. Your kit WILL be compared with kits submitted by law enforcement to identify perpetrators of violent crimes. The operators of GEDmatch encourage everybody to select this option.
'Opt-out' We will compare your DNA kit to all other kits in the GEDmatch database to find your matching genetic relatives. Kits in the database include those submitted by users undertaking personal genetic genealogy research, adoptee searches, and users (including law enforcement) attempting to identify unidentified human remains. Your kit WILL NOT be compared with kits submitted by law enforcement to identify perpetrators of violent crimes.
'Research' DNA kits will not be shown in match result reports generated for other kits. Genealogy and Genetic Genealogy require the sharing of information. This option is provided primarily for artificially created research kits, but may be used for regular uploads if you have specific reasons for doing so.

By default, your Raw Data is not available to any user of the Site - not even you. However, you understand that anyone with the kit number for Raw Data can perform many or all of the same GEDmatch functions with that Raw Data that the provider of that Raw Data can perform.

There may be options where you may join a 'sharing pool' which has the potential for disclosing additional information about you or your data. If you choose to join a sharing pool, you should carefully read the conditions and disclaimers associated with that sharing pool. By joining the sharing pool, you are agreeing to abide by those conditions and disclaimers.

Use of Results

The nature of genealogy research requires the exchange of information. That use must also be tempered by respect for the rights and privacy of other individuals. Anybody found to be using this Site in ways not consistent with this principle of human decency will be subject to an immediate ban with all their data removed. Examples include, but are not specifically limited to, spam mailing lists or publishing other people's user names and kit numbers from match lists or other personal information without their permission. If relevant permission is not obtained from any applicable person, then any personal information (including, without limitation, user name

While the results presented on this Site are intended solely for genealogical research, we are unable to guarantee that users will not find other uses, including both current and new genealogical and non-genealogical uses. For example, some of these possible uses of Raw Data, personal information, and/or Genealogy Data by any registered user of GEDmatch include but are not limited to:

- Paternity and maternity testing;
- Discovery of unknown or unidentified children, parents, or siblings;
- Discovery of other genetic and genealogical relatives, including both known and unknown or unexpected genetic and genealogical relatives;
- Discovery of ethnic background;
- Discovery of a genetic relationship between parents;
- Discovery of biological sex;
- Discovery of medical information or physical traits;
- Obtaining an email address; and/or
- Familial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains.

You understand that future genealogical and non-genealogical uses may be developed, including uses that GEDmatch cannot predict or foresee. If you find any of these current or future uses unacceptable, do not provide Raw Data to GEDmatch, and remove any of your Raw Data already provided to this Site. It is our policy to never provide your Genealogy Data, Raw DNA, personal information, or email address to third parties, except as noted herein. You have the right to access the personal information that GEDmatch has collected about you. You may do the following at any time by contacting us at GEDmatch@verogen.com:

- Opt out of any future contacts from us;
- See what information we have about you, if any;
- Change, correct, or have us delete any information we have about you (including personal information, Raw Data, and Genealogy Data); and
- Express any concern you have about our use of your information.

Accuracy of Results

The analysis and comparison results presented on this Site are provided 'as is' and no representations are made regarding their accuracy or usability. Changes in software and analysis tools may be made from time to time that could change results from those previously provided. We do not make any promises about: (a) the functionality of the Site or the Site tools; or (b) the quality, accuracy, reliability, or availability of the Site, including about any personal information, Raw Data, or Genealogical Data provided to the Site. Any reliance you place on information found at the Site is strictly at your own risk. We disclaim all liability and responsibility arising from any reliance placed on such information by you and any other visitor to the Site, and by anyone who may be informed of any of its contents. The operators of this Site are not responsible for the consequences of using the information provided on this Site.

Termination of Service

Anybody wishing to have their provided Raw Data or Genealogy Data removed from the GEDmatch database may do so using the removal/deletion link or other means provided within your GEDmatch account. Alternatively, you can request deletion of your personal information at any time by contacting us at GEDmatch@verogen.com.

GEDmatch administrators reserve the right to remove any Raw Data, Genealogy Data, or personal information from the database, for any reason, at any time, either with or without notice. Any or all services at GEDmatch.Com may be terminated at any time, without notice, for any reason, at the sole discretion of the GEDmatch administrators.

Cookies

Cookies may be used by this Site to enable certain privacy and log-in capabilities. A cookie is a small file placed on your computer. You have the ability to delete cookie files from your computer at any time or avoid cookies by configuring your browser to reject them or to notify you when a cookie is being placed on your computer.

This Site may contain links to advertising placed by third party sites. Advertising by third party sites may be placing and reading cookies on your browser, or using web beacons to collect information, in the course of ads being served on this Site. We have no control over how third party sites may utilize cookies. If you feel that a third party site is engaging in unethical or illegal use of this capability, please notify us so that we may take appropriate action to remove that link.

Loss of data

GEDmatch operators will not be held responsible for the loss of Raw Data, whether as a result of mechanical failure, software malfunction, human error, or any other means.

possible that, in the future, GEDmatch will merge with, or operations will be transferred to other individuals or entities. If that happens, the operating personnel at GEDmatch will change. GEDmatch reserves the right to provide access to your data (including Raw Data, Genealogy Data, profile information, and other personal information) to those other individuals or entities, which may include people not currently involved in GEDmatch operations. This Policy will continue to apply to the Site until you receive notification of changes to

Home How It Works Applications Education About Us Support
JOIN FOR FREE SIGN IN

you will not provide your personal information, Raw Data, or information, Raw Data, or Genealogy Data, you agree to remove it from GEDmatch immediately.

Limitation of Liability

GEDmatch shall have no liability to you under this Policy, it being acknowledged and agreed that the Site is provided solely for your convenience. If the foregoing limitation of liability is found to be unenforceable, GEDmatch's liability to you for any cause of action arising from the Site or under this Policy will be limited to any amount paid by you to GEDmatch for the Site during the twelve (12) months preceding such cause of action. Notwithstanding anything to the contrary contained herein, this Policy shall not limit or exclude either party's liability for gross negligence or intentional misconduct of a party or its agents or employees, or for death or personal injury. The parties agree that the limitations on and exclusions of liability in this Policy were freely negotiated and are an integral part of the bargain, in that the Site would not have been available for the same price and under the same terms and conditions had such limitations on and exclusions of liability not been included in this Policy. Some states or jurisdictions do not allow the exclusion of certain warranties, so some of the above limitations may not apply to you. Further, some jurisdictions prohibit the exclusion or limitation of liability for consequential or incidental damages, so the above limitations may not apply to you.

Indemnification

You agree to indemnify, defend, and hold GEDmatch and any of their affiliates, any of their successors and assigns, and any of their respective officers, directors, employees, volunteers, contractors, consultants, agents, representatives, licensors, advertisers, suppliers, and service providers, harmless from any liability, loss, claim, and expense, including reasonable attorneys' fees, related to your violation of this Policy or use or misuse of the Site. We reserve the right, at our own expense, to assume the exclusive defense and control of any matter otherwise subject to indemnification by you, in which event you will cooperate with us in asserting any available defenses.

Legal Disclosures

In this section, we have included some legally required disclosures under U.S. state and EU/United Kingdom privacy laws. If there are any conflicts between this section and any other provision of these Terms of Service and Privacy Policy, the portion that is more protective of personal information in your country or state of residence shall control to the extent of such conflict. While these laws apply only to residents of the specified jurisdictions, all users have the ability to change, correct or delete their information through their account settings or by contacting us at GEDmatch@verogen.com.

Information for California Residents

Under the California Consumer Privacy Act 2018 ("CCPA"), California residents have certain rights regarding their data, including:

Access

You have the right to request certain information about our collection and use of your personal information over the past 12 months. In response, we will provide you with the following information:

- The categories of personal information that we have collected about you.
- The categories of sources from which that personal information was collected.
- The business or commercial purpose for collecting or selling your personal information.
- The categories of third parties with whom we have shared your personal information.
- The specific pieces of personal information that we have collected about you.

If we have disclosed your personal information to any third parties for a business purpose over the past 12 months, we will identify the categories of personal information shared with each category of third party recipient.

Deletion

You have the right to request that we delete the personal information that we have collected about you. Under the CCPA, this right is subject to certain exceptions: for example, we may need to retain your personal information to provide you with the GEDmatch services or complete a transaction or other action you have requested. If your deletion request is subject to one of these exceptions, we may deny your deletion request. If you have a GEDmatch account, you can also delete your information through your account settings.

Exercising Your Rights

To exercise the rights described above, you or your Authorized Agent (defined below) must send us a request that (1) provides sufficient information to allow us to verify that you are the person about whom we have collected personal information, and (2) describes your

Request. We will work to respond to your Valid Request within 45 days of receipt.

You may submit a Valid Request using the following methods:

- Call us at: 1 (833) 837-6436

You may also authorize an agent (an "Authorized Agent") to exercise your rights on your behalf. To do this, you must provide your Authorized Agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from your Authorized Agent when they make a request on your behalf. In order to prevent fraud or identity theft, it is our practice to confirm directly with you that a request from an Authorized Agent is legitimate.
We will not discriminate against you for exercising your rights under the CCPA.

We do not sell your information as we understand that term under the CCPA. However, we have incorporated cookies from certain third parties on the GEDmatch website. These cookies allow those third parties to receive certain information about your interaction with the website that is associated with your browser or device. To adjust or manage your cookies settings, please click "Manage Cookies" in the footer links at the bottom of this page. Please note that the GEDmatch website does not support "Do Not Track" requests sent from a browser at this time.

This chart details the categories of personal information that we collect and have collected over the past 12 months:

Category of Personal Information	Examples of Personal Information We Collect	How We Use It	Categories of Third Parties With Whom We Share this Personal Information:

		and log in to and use GEDmatch, to communicate with you (including to provide support and answer questions), to understand how our users interact with GEDmatch, and to improve our offerings. We also use this information in accordance with your specific opt-in/opt-out settings for law enforcement and research purposes, as described in more detail above.	
Profile or Contact Data	• First and last name • Alias • Email • Unique identifiers such as passwords		• Service Providers • Parties You Authorize, Access or Authenticate
Payment Data and Commercial Information About Your Transactions with Us	• Payment card type • Last 4 digits of payment card • Bank account number • Billing address, phone number, and email • Information on checks you send us • Information about Tier1 level subscriptions	To receive and process payment for the Tier1 version of GEDmatch, and to provide you with the GEDmatch service.	• Service Providers (specifically our payment processing partner, currently Chargebee)
Device/IP Data	• IP address • Device ID • Domain server • Type of device/operating system/browser used to access the GEDmatch services	To provide the GEDmatch services, to understand how our users interact with GEDmatch, and to improve our offerings.	• Service Providers (specifically our analytics partners)

purposes.

- **Restriction of Processing**: You can ask us to restrict further processing of your personal data.
- **Right to File Complaint**: You have the right to lodge a complaint about our practices with respect to your personal data with the supervisory authority of your country or EU Member State. A list of Supervisory Authorities is available

Transfers of Personal Data

The GEDmatch service is operated by Verogen, a company based in the United States. You acknowledge that any personal data you submit to, or that is collected by, the GEDmatch service is received by Verogen in the U.S. and will be hosted on U.S. servers or may, in the future, be hosted on EU servers operated by Verogen or its service providers. This is necessary for Verogen to be able to provide you with the GEDmatch services as requested by you and set forth in these Terms of Service and Privacy Policy. If you do not wish for your data to be processed and hosted in the U.S. or in the EU, please do not use the GEDmatch services. While Verogen receives or collects personal data directly from you as the EU or UK data subject, Verogen takes the protection of your personal data seriously and treats it in accordance with the obligations of the importer under the EU Commission Standard Contractual Clauses for Controller to Controller transfers of personal data (as updated from time to time by the EU Commission).

If you are located in the European Union or the United Kingdom, you may use the following information to contact our Data Protection Officer and our European Union-Based Member Representative:

- For our EU Representative, individuals and data protection supervisory authorities in the EU and the UK may contact our data protection representatives according to Articles 27 EU and UK GDPR:
  - EU Mail: DP-Dock GmbH, Attn: Verogen Inc., Ballindamm 39, 20095 Hamburg, Germany
  - UK Mail: DP Data Protection Services UK Ltd., Attn: Verogen Inc., 16 Great Queen Street, Covent Garden, London, WC2B 5AH, United Kingdom
  - Email: verogen@gdpr-rep.com
- For our Data Protection Officer:
  - Email: dpo@verogen.com

Data Retention

We retain personal information about you for as long as you have an open account with us or as otherwise necessary to provide you with the GEDmatch services. See the "Security" section about our retention and deletion of original uploaded files.

Updates to This Policy

We may update the GEDmatch.Com Terms of Service and Privacy Policy at any time. We will inform you of updates by posting an announcement on the Site. You agree to review the updated terms and policy, and by continuing to use the Site after we have posted a notice on the Site about the update, you accept the changes to the GEDmatch.Com Terms of Service and Privacy Policy.

Contact us:

Verogen Inc. is incorporated in the State of Delaware, USA
Email: GEDmatch@verogen.com
Phone: 1 (833) 837-6436
US Mail:
Verogen, Inc.
11111 Flintkote Avenue
San Diego, CA 92121

[GED match]

JOIN FOR FREE

SIGN IN

Applications

- One-to-Many DNA Comparison
- Admixture (Heritage)

Resources

- How It Works
- Education

About Us

- About Us
- Support
- Account Login

Copyright 2022 @ GED Match | Privacy Policy & Terms of Use | Manage Cookies

Web Analytics	webpage/source through which you accessed the services • Non-identifiable with the interaction between device or browser and the GEDmatch services	GEDmatch services, to understand how our users interact with GEDmatch, and to improve our offerings.	• Service Providers (specifically our analytics partners)
Consumer Demographic Data	• Gender	To provide the GEDmatch services, to understand how our users interact with GEDmatch, and to improve our offerings.	• Service Providers • Parties You Authorize, Access or Authenticate
Biometric Data	• Y-DNA or mtDNA haplogroup • Genetic sequence/information • Genealogy data	To provide the GEDmatch services, and in accordance with your specific opt-in/opt-out settings.	• Service Providers • Parties You Authorize, Access or Authenticate
Other Identifying Information that You Voluntarily Choose to Provide	• Identifying information in emails or letters you send us	To provide the GEDmatch services, to understand how our users interact with GEDmatch, and to improve our offerings.	• Service Providers

In addition to the specific uses described above, we also use personal information for fraud protection, security and debugging purposes, and we may use and share personal information for meeting legal requirements and enforcing legal terms, as described in more detail above.

Other California Resident Rights
Under California Civil Code Sections 1798.83-1798.84, California residents are entitled to contact us to prevent disclosure of personal information to third parties for such third parties' direct marketing purposes; in order to submit such a request, please contact us at GEDmatch@verogen.com.

If you are a resident of California, you have a right to file a complaint alleging a violation under the GIPA with California's Attorney General or other applicable state officials. To file a complaint alleging a violation under the GIPA, please contact:

- California's Attorney General:
  - Webform: https://oag.ca.gov/contact/consumer-complaint-against-business-or-company

If applicable, you may also file a complaint alleging a violation under the GIPA by contacting the applicable state officials listed below:

- County counsel authorized by agreement with the district attorney in actions involving violation of a county ordinance;
- City attorney of a city having a population in excess of 750,000;
- City attorney in a city and county (for example, city attorneys listed at: https://www.cdaa.org/city-attorney-roster); or
- City having a full-time city prosecutor, in the name of the people of the State of California.

JOIN FOR FREE SIGN IN Applications Support

Information for Nevada Residents

If you are a resident of Nevada, you have the right to opt-out of the sale of certain personal information to third parties who intend to license or sell that personal information. Please note that we do not currently sell your personal information as sales are defined in Nevada Revised Statutes Chapter 603A.

Information for European Union and United Kingdom Residents

If you are a resident of the European Union ("EU"), United Kingdom, Lichtenstein, Norway or Iceland, you may have additional rights under the EU General Data Protection Regulation (the "GDPR") or the United Kingdom Data Protection Act with respect to your personal data, as outlined below.

For this section, we use the terms "personal data" and "processing" as they are defined in the GDPR, but "personal data" generally means information that can be used to individually identify a person, and "processing" generally covers actions that can be performed in connection with data such as collection, use, storage and disclosure. Verogen will be the controller of your personal data processed in connection with the GEDmatch services.

Personal Data We Collect

The "GEDmatch Collection and Use of Information" section and the chart above detail the personal data that we collect.

Personal Data of Children

We do not knowingly collect or solicit personal data from children under 16 years of age; if you are a child under the age of 16, please do not attempt to register for or otherwise use GEDmatch or send us any personal data. If we learn we have collected personal data from a child under 16 years of age, we will delete that information as quickly as possible. If you believe that a child under 16 years of age may have provided personal data to us, please contact us at GEDmatch@verogen.com.

Personal Data Use and Processing Grounds

We will only process your personal data if we have a lawful basis for doing so. We process your personal data as a matter of contractual necessity to provide you with the GEDmatch services. For example, we need your contact information in order to enable your account, provide support and communicate with you, your payment information to provide you with the Tier1 level of services if selected by you, and, at your option, your DNA and genealogical data so that you can use the GEDmatch services for genealogical purposes. We also process your personal data when we believe it furthers the legitimate interests of us or third parties. For example, we process your device ID and we generate web analytics in order to understand how our users use GEDmatch, so that we can improve GEDmatch for everyone. In some cases, we process personal data based on the consent you expressly grant to us at the time we collect such data. For example, your personal data will only be processed for law enforcement and/or research access when you expressly opt in, as described in more detail above. When we process personal data based on your consent, it will be expressly indicated to you at the point and time of collection. From time to time we may also need to process personal data to comply with a legal obligation, if it is necessary to protect the vital interests of you or other data subjects, or if it is necessary for a task carried out in the public interest.

EU Data Subject Rights

You have certain rights with respect to your personal data, including those set forth below. For more information about these rights, or to submit a request, please email us at GEDmatch@verogen.com. Please note that in some circumstances, we may not be able to fully comply with your request, such as if it is frivolous or extremely impractical, if it jeopardizes the rights of others, or if it is not required by law, but in those circumstances, we will still respond to notify you of such a decision. In some cases, we may also need you to provide us with additional information, which may include personal data, if necessary to verify your identity and the nature of your request.

- **Access**: You can request more information about the personal data we hold about you and request a copy of such personal data. If you are an account holder, you can also access certain of your personal data by logging on to your account.
- **Rectification**: If you believe that any personal data we are holding about you is incorrect or incomplete, you can request that we correct or supplement such data. You can also correct some of this information directly by logging on to your account.
- **Erasure**: You can request that we erase some or all of your personal data from our systems.
- **Withdrawal of Consent**: If we are processing your personal data based on your consent (as indicated at the time of collection of such data), you have the right to withdraw your consent at any time.

Manolakos, Alexandra 10/24/2022
For Educational Use Only

30 Geo. Mason U. Civ. Rts. L.J. 177

George Mason University Civil Rights Law Journal
Spring, 2020

Comment

Jennie F. O'Hara[a1]

Copyright © 2020 by George Mason University Civil Rights Law Journal Association; Jennie F. O'Hara

23, ME, AND THE POLICE: THE FOURTH AMENDMENT IMPLICATIONS OF FAMILIAL DNA SEARCHING

INTRODUCTION

On April 24, 2018, a seventy-two-year-old man was escorted out of his Citrus Heights, California home in handcuffs.[1] This man, Joseph DeAngelo--now infamously known as the Golden State Killer--will likely spend what remains of his life in prison, finally paying for the rapes and gruesome murders of dozens of victims throughout the state of California in the 1970s and 80s.[2] DeAngelo's crimes had gone unsolved for over four decades, until savvy police investigators--still invested after all of that time--decided to experiment with a newly conceived investigatory technique: familial DNA searching.[3] Using this method, investigators were able to track down DeAngelo by matching DNA he had discarded at the scene of his crimes with the DNA of his distant relative, uploaded to a genealogy website.[4]

From this anecdotal scenario, it is simple to assume that familial DNA searching by police investigators can yield immeasurable positive outcomes. Although this may be true, it is also easy to imagine the myriad of ways in which law enforcement could weaponize this ***178** level of intrusion against the privacy rights of American citizens. Under the current Fourth Amendment framework, few safeguards are in place that would effectively protect the privacy rights of individuals who actively participate in public genealogy websites.[5] Furthermore, any existing state regulatory protections are sparse and highly varied.[6] In order for both law enforcement and the general public to benefit from the possibilities and potential advantages of familial DNA searching in criminal investigations, the government must implement uniform regulations.[7]

This Comment will suggest the implementation of federal legislation specifically designed to provide strict standards concerning familial DNA searching in criminal investigations. First, this Comment will discuss background concepts and information pertinent to the current framework of the Fourth Amendment as well as the modern use of DNA evidence generally. Specifically, Part I will discuss in detail the Golden State Killer case and investigation, including the use of familial DNA searching that led to DeAngelo's arrest. Part II will provide a historical overview of the use of DNA analysis in police investigation, including its current utility as an investigative tool. Part III will provide a general overview of Fourth Amendment jurisprudence, defining the scope of the law regarding search and seizure. Part IV will address the business operations of several popular genealogy websites, delving particularly into the privacy and general use disclosures supplied to people who utilize the websites' services. Part IV will also analyze the current landscape of federal regulation with regard to familial DNA testing of genealogy websites. Finally, Part V will conclude the background section by focusing on Colorado's familial DNA searching regulations and policies, as the leading state in terms of this technology.

Next, this Comment will analyze the Fourth Amendment implications surrounding the use of genetic information in the Golden State Killer investigation under the current regulatory scheme. This Comment will then apply the same facts to the Colorado model's framework to determine its effectiveness in real-world scenarios. Finally, this Comment concludes that it is necessary

for Congress to enact further *179 legislation to regulate the use of private individual genetic information at the federal level, and specifically suggests federal implementation of the Colorado model.

BACKGROUND

I. THE GOLDEN STATE KILLER

In the early morning hours of June 18, 1976, a twenty-three-year-old woman lay on the floor of her Rancho Cordova, California bedroom with her hands bound behind her back. [8] Despite her bindings, she was able to reach her telephone and call the police, to whom she recounted her horrific ordeal in vivid detail. [9] She stated that she awoke to a man "about five nine, moderately muscular, wearing a navy blue, short-sleeved T-shirt and gray canvas gloves" standing in the doorway of her bedroom, wearing a tight white ski mask to disguise his face. [10] This man went on to rape her before ransacking her home and fleeing the scene. [11] Investigators soon discovered that this man was careful and calculated in the planning and execution of his crimes. [12] They also discovered that he was incredibly cautious not to reveal his identity to his victims. [13]

This man's meticulous nature would prove effective, as this fateful night would go down in infamy as the beginning of his horrifying rampage throughout California over the next decade. [14] What began in 1972 as home invasions quickly turned into rapes, which became violent rapes and tortures, and, eventually, murders. [15] Because of the multi-jurisdictional nature of his crimes throughout California, investigators were initially unaware that they were perpetrated by a single offender. [16] This allowed the offender to commit his crimes undetected *180 from 1972 to 1986 before inexplicably vanishing into thin air. [17] The elusive villain stalking California homes received many monikers during that span of time, including--"The Cordova Cat Burglar," "The Visalia Ransacker," "The East Area Rapist," and "The Original Night Stalker." [18] Decades later, after forty-two years, investigators across the state would finally learn that all of these widespread atrocities were the work of a single man: Joseph DeAngelo, the Golden State Killer. [19]

The last known crime attributed to the individual who would become the Golden State Killer occurred in 1986, an era of infantile forensic DNA technology. [20] Although the killer had "left his DNA all over the place" [21] at each crime scene, forensic analysts at the time did not possess the necessary technology to yield any viable leads. [22] It was not until 2011, after years of failed attempts, that police were able to use the DNA left at the crime scenes to create a general profile of the killer. [23] Nevertheless, this profile was not a match with any of the known felons in the Combined DNA Index System (CODIS), the Federal Bureau of Investigation's (FBI) DNA database. [24]

However, many who studied and investigated this case in great detail still believed that pursuing DNA evidence was the best way to "get out of the maze of the Golden State Killer." [25] One such individual was Michelle McNamara, the late author of the novel, *I'll Be Gone in the Dark: One Woman's Obsessive Search for the Golden State Killer*. [26] After McNamara suddenly passed away while writing this novel, her assistants and fellow researchers used compilations of her notes, research, and hard drives to continue her diligent work. [27] In *181 those notes, McNamara stated that she believed one potentially fruitful path for DNA analysis was through familial DNA searching. [28] Her notes recognized that although CODIS could not match the crime scene DNA to the Golden State Killer himself, if a member of the perpetrator's family happened to be in the system, police could potentially see a match in trace DNA markers shared by close family members. [29] Even though this line of inquiry rendered no useful results at that initial stage, after just a few more years of dedicated research into the field of DNA technology, this idea would ultimately prove to be the key to solving the case. [30]

On April 24, 2018, just shy of forty-two years after the Golden State Killer's first attack, police in Citrus Heights--a suburb of Sacramento, California--arrested seventy-two-year-old Joseph DeAngelo in his home. [31] Under a familial DNA-driven line of inquiry, California law enforcement had developed a new tactic--familial searching through a "no-frills" site used by amateur

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

genealogists called GEDmatch.com (GEDmatch).[32] Authorities began using GEDmatch, a public genealogical database used to search for relatives and ancestors online, after the traditional route of searching through state and federally run criminal DNA databases did not yield results.[33] According to longtime Contra Costa County District Attorney investigator Paul Holes, after authorities uploaded the Golden State Killer DNA profile to the site, they were able to obtain an extended list detailing the extent to which the DNA uploaded by various individuals on GEDmatch resembled the DNA of the killer--the closer the match in DNA sequences, the more closely related the individuals are.[34] Because GEDmatch users willingly upload their DNA profiles to the site for public use, authorities did not need a court order to access the familial data.[35]

From these results, Chief Deputy District Attorney Steve Grippi stated that police were able to "zero in on DeAngelo" using a DNA ***182** profile uploaded by a distant relative.[36] Once authorities had a small pool of possible suspects derived from the public GEDmatch profiles, investigators used the results to explore these family trees and find men who were roughly the right age and height, and were living in California when the crimes occurred.[37] From this point, police were able to hone in on DeAngelo.[38] Specifically, investigators obtained samples of DeAngelo's DNA from his car door handle while he shopped at a local craft store, as well as from a tissue discarded in his trash.[39] Finally, after decades of tireless searching by authorities across the state of California, the Golden State Killer had a name and a face.

When news sources began to report that law enforcement used a public genealogy website to solve a murder investigation, the public's reaction to this revelation was mixed, at best.[40] A large portion of the populace seemed to have been unaware that the information uploaded to databases such as GEDmatch "could later be used to incriminate a relative."[41] As Joel Winston, a New Jersey consumer protection lawyer and former deputy state attorney general, opined, "DNA databases are relatively new, but nobody thinks they'll ever be used in [that] manner."[42] Potential ethical concerns aside, scholars and law enforcement alike have been left to wonder about the legality of using DNA samples from genealogy companies to investigate crimes. State privacy laws may carry some weight, but they are often rebutted because most, if not all, DNA samples supplied to genealogy websites are voluntarily submitted.[43] Because of the inherent infringement these searches have on individual privacy, however, it is imperative to consider the Fourth Amendment implications of this policy.

*183 II. HISTORY OF THE USE OF DNA EVIDENCE IN POLICE INVESTIGATIONS

A. *British Development of the Method*

The use of DNA evidence in its modern form did not arise publicly in the court system until 1986 when Dr. Alec Jeffreys, a geneticist at the University of Leicester, United Kingdom, proposed the radical idea that his recently developed method of genetic testing could be used to apprehend criminals.[44] Jeffreys discovered his method accidentally--the result of a failed attempt at studying the progression of illness through family lineage--when he attached DNA that he had extracted from human cells to photographic film and allowed the film to develop.[45] Each developed film reel bore the image of a unique sequence of bars, which Jeffreys soon realized allowed him to distinguish between the DNA patterns of different individuals with extraordinary precision.[46] Initially, Jeffreys' technique was used as a means to establish the paternity of various children in British immigration disputes.[47] However, police officers soon requested Jeffreys' assistance in identifying the perpetrator behind the rape and murder of two teenage girls in the village of Narborough, Leicestershire, who had managed to evade capture for over two years.[48] After a local teenage boy named Richard Buckland confessed to the crimes, but shortly thereafter recanted, Jeffreys was tasked with comparing the blood and semen the killer left at the crime scenes with a sample of Buckland's DNA.[49] Jeffreys' method led to Buckland's exoneration, as the results confirmed that although the two girls were killed by the same man, that man was not Buckland.[50]

This setback did not hinder police enthusiasm to find the killer, however, and investigators continued pursuing the possibilities Jeffreys' innovative method offered.[51] Police began collecting voluntary ***184** blood samples from men throughout the neighborhood, and eventually amassed a database of over 5,000 samples.[52] However, this too yielded no direct match.[53] It

was not until August 1987, over a year since the second victim's body was discovered, that a local man notified police that he had overheard another man in a pub discussing how he had supplied a blood sample on behalf of a workmate named Colin Pitchfork.[54] Police quickly brought Pitchfork in for questioning, and he confessed immediately to the rape and murder of the two young women.[55] For the first time in recorded history, DNA testing had led to the successful conviction of a murderer.[56]

B. ***DNA Evidence in the United States***

Dr. Jeffreys' innovative new technique quickly made its way to the United States and began weaving its way into the lexicon of criminal investigative techniques. In 1987, a DNA test was able to confirm that a blood sample extracted from Tommie[57] Lee Andrews perfectly matched traces of semen left at the scene of a rape, leading to America's first DNA-based conviction.[58]

Initially, the admissibility of evidence gained through DNA testing was not frequently disputed in court.[59] However, as prosecutors more widely used the practice as a means to secure convictions, defense attorneys began to question the admissibility of DNA evidence in criminal trials, because they doubted the validity of the techniques used to produce DNA profiles.[60] In 1989, one of the first public challenges against using DNA evidence came before the New York State Supreme Court, Appellate Division, in *People v. Castro*, when the court considered the admissibility of a DNA identification ***185** test that would prove that blood found on the defendant's watch belonged to the victim of a murder, tying him directly to the crime.[61] At that time, no appellate court in the state had ruled on the admissibility of DNA evidence in criminal trials, so the court turned to standards for determining the admissibility of new scientific evidence articulated by the U.S. District Court for the District of Columbia in *Frye v. United States* and by the New York Court of Appeals in *People v. Middleton*.[62] The court found that DNA tests satisfied the rule set forth in *Frye*, stating that "the test is not whether a particular procedure is unanimously indorsed [sic] by the scientific community, but whether it is generally acceptable as reliable."[63] In making this determination, the *Castro* court developed a three-prong analysis to aid in its final decision: (1) "Is there a theory, which is generally accepted in the scientific community, which supports the conclusion that DNA forensic testing can produce reliable results?"; (2) "Are there techniques or experiments that currently exist that are capable of producing reliable results in DNA identification and which are generally accepted in the scientific community?"; and (3) "Did the testing laboratory perform the accepted scientific techniques in analyzing the forensic samples in this particular case?"[64] The court was able to discuss the first two prongs with relative ease, concluding first that "[t]here is general scientific acceptance of the theory underlying DNA identification," and second that "DNA forensic identification techniques and experiments are generally accepted in the scientific community and can produce reliable results."[65] Therefore, the court largely decided the case upon consideration of the third prong, holding that "[a] pretrial hearing should be conducted to determine if the testing laboratory substantially performed the scientifically accepted tests and techniques, yielding sufficiently reliable results to be admissible as a question of fact for the jury."[66]

With a clear standard for the admissibility of DNA evidence in court proceedings in place, police and prosecutors were then free to ***186** develop and utilize the technology within the ever-evolving criminal justice system.[67] In 1989, the Virginia Division of Forensic Sciences became the first state crime laboratory to implement a policy of DNA testing in all of its criminal investigations.[68] The following year, the Virginia General Assembly passed the first state law requiring all individuals with felony convictions to submit DNA samples for inclusion in a state DNA database.[69]

The constitutionality of this state database quickly came into question before the Fourth Circuit in *Jones v. Murray*, one of the earliest cases considering this issue.[70] In *Jones*, the court upheld the constitutionality of Virginia's DNA database system, holding:

> Considering the inmates' questionable claim of privacy to protect their identification and the minimal intrusion resulting from taking a small sample of blood, the Commonwealth's interest in combatting and deterring felony recidivism justifies the involuntary taking of the sample and the creation of the DNA data bank as reasonable in the context of the Fourth Amendment.[71]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Manolakos, Alexandra 10/24/2022
For Educational Use Only

Following this favorable decision, each of the other forty-nine states began developing their own DNA database systems--and all fifty states actively maintain their systems through the present day. [72] However, the various state laws creating and regulating the databases are largely inconsistent with one another. [73] For example, four state laws require DNA samples from only those defendants convicted of a felony, while at least eight other states require certain individuals convicted of misdemeanor offenses to also supply DNA samples. [74] Additionally, states inconsistently regulate the procedures through which law enforcement may access the databases. [75] While most states allow for the automatic search of their databases in assistance of criminal ***187** investigations, some others are much stricter, allowing police to search the databases only in regard to violent crimes. [76]

In 1990, in an effort to provide a remedy for this inconsistency, the FBI developed CODIS, a streamlined, nationwide database that law enforcement from any state could access. [77] Initially developed as a pilot program implemented in fourteen state and local crime laboratories within the United States, CODIS is now utilized by over ninety crime laboratories across fifty countries. [78] CODIS enables crime laboratories at the federal, state, and local levels to communicate and share information and DNA samples to facilitate effective criminal investigation. [79] In 1994, the DNA Identification Act [80] established the National DNA Index System (NDIS), a national database containing all of the DNA profiles supplied by the federal, state, and local crime laboratories participating in CODIS. [81] Officially implemented in 1998, the NDIS actively participates with all fifty U.S. states, the District of Columbia, and Puerto Rico. [82] The establishment of the NDIS also helped to resolve the inconsistencies resulting from state-by-state laws surrounding access to DNA databases. [83] According to the FBI, "[i]f a state has signed the Memorandum of Understanding ... to participate in NDIS, that state has agreed to comply with the Federal DNA Identification Act, including the limited access requirements." [84]

*188 III. FOURTH AMENDMENT JURISPRUDENCE

A. *Development of Traditional Fourth Amendment Analysis*

The Fourth Amendment to the United States Constitution guarantees:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. [85]

Before the Supreme Court's landmark decision in *Katz v. United States* in 1967, courts tended to limit the extension of Fourth Amendment protection to instances in which law enforcement *physically* trespassed on private property to complete a search or seizure, framing the Amendment to focus mainly on property rights. [86] The Supreme Court rejected this viewpoint in *Katz*, holding that the Fourth Amendment "protects people, not places." [87] Specifically, the Court stated, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." [88] The Court has upheld that the reasonableness of an expectation of privacy depends on two factors: (1) the individual must have manifested a subjective expectation of privacy in the object of the challenged search; and (2) society must be willing to recognize that expectation of privacy as reasonable. [89] In *Katz*, the Court found that an individual manifests a subjective expectation of privacy in the objects and locations which he seeks to preserve as private. [90] Therefore, if the individual has displayed a reasonable expectation of privacy, the Court will evaluate "whether ***189** the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment." [91]

Because the *Katz* reasonableness standard inherently allows for some case-by-case variation in analysis, the definition of a search or seizure can vary for the purposes of Fourth Amendment protection. [92] However, the Supreme Court has concretely provided that a "search" occurs when an individual manifests a subjective expectation of privacy in something, which society is willing to recognize as reasonable, and that item is observed visually, or by the use of sense-enhancing technology not in general public use. [93] The Court has also stated that a "seizure" occurs "when [an] officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen." [94] Returning to the significance of the reasonableness consideration, the Court clarified this point to include that "the police can be said to have seized an individual only if, in view of all the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave." [95]

As previously mentioned, the Fourth Amendment has historically been inextricably linked with property rights. [96] Despite the extension of this point beyond strict property in *Katz*, a trespass analysis is still often invoked in consideration of constitutional protection under the Fourth Amendment. For example, in *United States v. Jones*, [97] the Court ruled in favor of a defendant who had a GPS tracker placed on his vehicle by the government, specifically citing the Fourth Amendment language that notes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." [98] The Court reasoned that a person's vehicle is undoubtedly an "effect" as covered under this clause and, therefore, the government's "installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search." [99] This theory is directly ***190** derived from property law, as the Court noted that there was no doubt "that such a physical intrusion would have been considered a 'search' within the [original] meaning of the Fourth Amendment." [100]

B. *Exceptions*

Various exceptions to the reasonable expectation of privacy requirement for constitutional protection have arisen throughout the span of Fourth Amendment jurisprudence. One notable exception, the abandonment principle, also derives from the Fourth Amendment's traditional focus on property law. [101] As articulated by the Third Circuit in *United States v. Harrison*, "a person can lose his reasonable expectation of privacy in his real property if he abandons it." [102] Whether the owner has abandoned his reasonable expectation of privacy in his property is a determination that "must be made from an objective viewpoint, and proof of intent to abandon must be established by clear and unequivocal evidence." [103] To determine this, the court will look to "the totality of the facts and circumstances." [104] The Supreme Court has extended this principle to trash left on the curb outside an individual's home in *California v. Greenwood*, holding that because trash is sufficiently exposed to public view, it cannot rise to the level of Fourth Amendment protection. [105] Discarded items will only rise to the level of constitutional protection if the manner in which those items were discarded nevertheless constitutes an expectation of privacy that society is prepared to accept as objectively reasonable. [106] With regard to seizures of physical DNA evidence abandoned by a perpetrator at the scene of a crime, scholars have explained that there is no need to afford any constitutional protection to such evidence, because where there is no suspect in mind, there is no Fourth Amendment right to protect. [107] State courts have also articulated this ***191** standard. For example, in *State v. Athan*, police used a suspect's saliva left on an envelope to identify him. [108] There, the Supreme Court of Washington held that "[t]he analysis of DNA obtained without forcible compulsion and analyzed by the government for comparison to evidence found at a crime scene is not a search under the Fourth Amendment." [109]

Another prominent exception to the reasonable expectation of privacy requirement has been referred to as the third-party doctrine, which largely stems from inferences derived from the abandonment principle. The Supreme Court articulated this doctrine in *Smith v. Maryland* when it ruled that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." [110] In *Carpenter v. United States*, the Supreme Court explained that "[t]he third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another." [111] However, the "diminished privacy interests" associated with the third-party doctrine do "not mean that the Fourth

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Amendment falls out of the picture entirely." [112] Instead, courts should consider "the nature of the particular documents sought to determine whether there is a legitimate expectation of privacy concerning their contents." [113]

IV. USER AGREEMENTS AND CURRENT FEDERAL REGULATIONS OF POPULAR GENEALOGY WEBSITES

The use of genealogy websites by the general public has skyrocketed in recent history. In fact, genealogy is currently the second most popular hobby in the United States, with genealogy websites being the second most frequently visited category of internet sites. [114] Despite genealogy websites' growing popularity, it is unclear whether individuals who willingly upload their DNA to these various services are fully ***192** informed of how their information may be stored and used in the future. [115] For example, following the news surrounding the Golden State Killer case, GEDmatch was forced to release a statement specifying that users' genetic information, though primarily used to find distant relatives, *might* be used for other purposes, as it is not considered private under the third-party doctrine. [116]

Each genealogy website provides the public with information pertaining to their privacy policies and legal obligations with varying degrees of specificity and detail. [117] These measures largely are disclosed to indemnify the companies from legal action if personal user data is released to third parties. [118] Privacy policies also are disclosed to inform the public at large to which federal regulations these websites and the data stored therein are subject. [119] Each of the three genealogy websites discussed in this Comment vary in terms of the information provided in their privacy statements and terms of service in some respects, but there is some significant overlap with regard to federal statutes.

A. *23andMe*

23andMe, a popular genealogy website, says in its privacy security statement that the company "believes genetic information, as well as the systems put in place to protect it, deserve the highest level of security." [120] For this reason, 23andMe affirms that it will not give personal user data to any third party under any circumstances without explicit user consent, unless a valid warrant mandates the disclosure. ***193** [121] 23andMe explicitly promises its users that it will not provide private user information to "law enforcement or regulatory authorities unless required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information." [122]

The average 23andMe user may find it difficult at first glance to find any relevant statutory constraints on legal liability for the website. In fact, users must first navigate through five separate web pages on 23andMe's website to find the company's "Guide for Law Enforcement" to understand the statutory underpinnings of 23andMe's privacy policy. [123] Although clearly not labeled to attract the attention of the typical user, this guide details to law enforcement all of the necessary steps they must take and the constraints they must overcome before the company will release private user data. [124] This page begins by stating that, "23andMe will only review inquiries as defined in 18 U.S.C. § 2703(c)(2) related to a valid trial, grand jury subpoena, warrant or order." [125] This subsection of the U.S. Code--under the general heading "Required disclosure of customer communications or records" [126] --requires the mandatory disclosure to law enforcement of certain records concerning electronic communications or remote computing services. [127] Under 18 U.S.C. § 2703(c)(2), providers of electronic communication or remote computing services must disclose the name, address, records of session times and durations, length of service, types of services utilized, subscriber number, and means and source of payment for the service to government entities upon a valid request. [128]

Additionally, the Guide for Law Enforcement states that 23andMe will consider releasing additional user information outside of the aforementioned statutory categories if they are prompted to do ***194** so under a court order issued pursuant to 18 U.S.C. § 2703(d). [129] In relevant part, this subsection states that a court may issue such an order "only if the governmental entity

Manolakos, Alexandra 10/24/2022
For Educational Use Only

offers specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought are relevant and material to an ongoing criminal investigation." [130] The webpage then cites to 18 U.S.C. § 2703(f) to note that the company has never received a request to preserve information potentially relevant to legal proceedings pursuant to that subsection. [131] 18 U.S.C. § 2703(f) mandates that certain material requested under court order must be preserved for a ninety-day period. [132] Finally, 23andMe states that it will make every effort to notify a user if law enforcement has requested his personal data from the company, unless it is forbidden to do so by a Delayed Notice Order under 18 U.S.C. § 2705(b). [133] This statute states that a governmental entity, under certain circumstances, may apply for a "court order commanding a provider of electronic communications service[s] or remote computing service[s] ... not to notify any other person of the existence of the warrant, subpoena, or court order [directed to them]." [134]

B. *Ancestry DNA*

The Ancestry DNA Guide for Law Enforcement contains the exact same protections and statutory constraints stated by 23andMe except that it does not mention 18 U.S.C. § 2703(f). [135] Therefore, under these two companies, users can expect that their personal data and information will be protected from third-party inquiry except under the extreme circumstance of a valid court order in criminal investigations. This language and statutory scheme is consistent with the Fourth Amendment's protection against unreasonable searches and seizures without a proper warrant issued "upon probable cause, ***195** supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." [136]

Ancestry DNA cites three governing privacy principles: transparency, simplicity, and control. [137] Ancestry DNA also ensures that there are "measures in place to protect against inappropriate access, loss, misuse, or alteration of personal information under [its] control," although it does not clarify what specific "measures" are in place. [138] Additionally, Ancestry DNA offers the assurance that if law enforcement compels it to disclose any user's personal information, its first priority will be to provide the user with advance notice so long as it is permissible under law. [139] Ancestry DNA further provides all visitors--whether they have signed up to use their service or not--with access to an annual transparency report disclosing all law enforcement requests for user data over the preceding year. [140] The 2018 report revealed that Ancestry DNA responded to seven out of a total of ten valid law enforcement requests in that year, all of which were related to investigations of credit card misuse or identity theft. [141] In sum, Ancestry DNA and 23andMe both prioritize user privacy, at least as far as they are legally permitted to do so.

C. *GEDmatch*

GEDmatch's privacy policy paints a wholly different picture of privacy than those articulated by both 23andMe and Ancestry DNA. [142] Unlike the more professional-looking 23andMe and Ancestry DNA websites, GEDmatch provides only a low-tech and minimalist user interface. Its terms of service and privacy policy pages were initially updated in May 2018, one month after the Golden State Killer case was solved. [143] Although much of the initial language of this page ***196** espouses a heightened importance in the protection of individual privacy, the true nature of the website is revealed under a heading titled "GEDmatch Purpose." [144] This section reads:

> GEDmatch exists to provide DNA and genealogy tools for comparison and research purposes. It is supported entirely by users, volunteers, and researchers. DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this Site agree that their information will be shared with other users.

Therefore, unlike the typical legal protections enjoyed by users of more regulated websites, like 23andMe and Ancestry DNA, users of GEDmatch can expect that fellow users, any member of the general public, and even law enforcement may access the genetic information they have freely uploaded to the site.

GEDmatch, conversely, does not claim any statutory protection over its genetic content. GEDmatch brands itself largely as a public forum, rather than strictly a genealogy service. [145] Although it cites no statutory authority, GEDmatch does first establish that it "may disclose [users'] raw data, personal information, and/or genealogy data if it is necessary to comply with a legal obligation such as a subpoena or warrant." [146] The site even offers some possible alternative uses beyond simple genealogy research that users may access--including "familial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains." [147]

Further, GEDmatch's policy was recently updated on December 9, 2019, following the company's acquisition by Verogen, Inc. [148] The revised policy reflects a shift in the company's branding practices in the wake of the Golden State Killer investigation. Specifically, the policy now includes four options for users when uploading their DNA profiles to the website: "Private," "Public + opt-in," "Public + opt-out," and "Research." [149] Notably, the "Public + opt-out" option allows users to upload their DNA profiles for public comparison by ***197** other general users, but hides those profiles from users with profiles identified as having been uploaded "for Law Enforcement purposes." [150] Nevertheless, in this most recent revision, GEDmatch still fails to cite statutory authority for its policies, and retains portions of its policy notifying users of the inherent public nature of its product.

This policy stands in stark contrast to those outlined in the previous two websites. GEDmatch attempts to make it explicitly clear to users that the company is in no way responsible for breaches of information that is publicly accessible on its site. Under this scheme, the website functions largely like a social media platform, in which a majority of user data is voluntarily uploaded under the understanding that it can be freely accessed for any and all purposes.

V. THE COLORADO MODEL

In 2009, Colorado began to formally implement a policy of statewide familial DNA searching in criminal investigations, making it the first state in the U.S. to formally recognize familial DNA as an investigative resource. [151] Since then, Colorado's policy has become the gold standard for state familial DNA searching, with many states following suit in modeling their own policies after it. [152] Colorado has developed and proliferated its own familial DNA searching software, which is regularly tested and retested to ensure accuracy of results. [153] As of 2017, this software has been shared with local police departments in six additional states and has the capability of being fully downloaded and usable within an hour. [154] Users begin by uploading DNA profile data from the crime scene into the software's database. [155] The software then calculates ratios indicating the likelihood of familial relatedness between samples for all profiles in the system. [156] The software is also capable of organizing this data by familial relationship-- such as parent-child, siblings, etc.--as well as race. [157] Finally, ***198** based on the previously mentioned likelihood ratios, the software will export a table which displays the top selected profiles derived from comparison to the inputted DNA. [158]

There is no specific state legislation in Colorado that either explicitly prohibits or allows the use of familial DNA searches in criminal investigations, because the policy did not originate in the state legislature. [159] The policy of familial DNA searching was first proposed in the state by the Colorado Bureau of Investigations (CBI) and governed by the "CBI DNA Familial Search Policy." [160] After the CBI developed this policy, the state Attorney General approved and put it into effect state-wide in October of 2009. [161] The CBI policy defines familial DNA searching as "a deliberate search for biologically-related relatives of a contributor of an evidentiary profile conducted with specialized (non-CODIS) software designed for this purpose." [162] Because of the obvious privacy concerns and implications the new policy would surely elicit, the CBI was careful to implement incredibly specific and detailed procedures for state law enforcement to follow with each initial familial DNA search request. [163]

First, the request must originate from one of two sources: (1) "analysts within the [CBI or Denver PD Crime] lab identify cases they think are good candidates for [familial DNA searching] and go to their lab director requesting permission;" or (2) directly from a law enforcement agency. [164] Requests under either circumstance must meet a number of strict criteria. [165] First, not only must the case have already undergone a CODIS search with no results, but the lab must also be confident that the law enforcement agency has fully exhausted *all* alternative investigative leads. [166] Second, the request is subject to the professional opinion of the lab staff before familial DNA searching can be approved. [167] In this determination, lab staff will consider a number of factors, including "public safety implications, the age of the case, and the types of evidence available" to ensure that the case is ***199** sufficiently compelling to justify the significant monetary and time expenditure of familial DNA search analysis. [168] In circumstances where the request comes directly from law enforcement, lab staff will meet with the officers to fully inform them of the familial DNA search process. [169] After all relevant information has been shared with the officers, they are required to sign a form indicating their understanding of the procedure and relevant factors surrounding it before any analysis can commence. [170] This form also indicates a commitment from the officers that if a match or lead is discovered through familial DNA searching, officers must continue their investigation of the case so as to not have wasted lab resources. [171] This penultimate step in the process has been cited by both law enforcement entities as well as the Denver PD Crime Lab as one of the most integral parts of the request policy--the formal agreement between parties to take and maintain responsibility of the case so that neither party feels as though their time, finances, or energy is wasted. [172] Finally, the prosecutor of each case will be added to the formal familial DNA searching process to ensure the proper follow-up of any leads produced, continuing the chain of responsibility. [173] Ultimately, the crime lab's director makes the final decision of whether a familial DNA search will be conducted on any given case. [174]

ANALYSIS

This section sets forth a model framework based on the Colorado Model which, if implemented through federal legislation, would provide a uniform request and analysis process for investigative use of familial DNA searching that would afford heightened protections of the privacy rights of individuals. Specifically, this Part will first provide a comprehensive analysis of the Fourth Amendment implications in the Golden State Killer case under current legal standards. Then, this Part will apply these same facts to the processes and procedures of the Colorado Model. Finally, this Part will discuss the differing outcomes ***200** of these two methods and ultimately conclude that the Colorado Model provides for a more streamlined, thorough, and uniform request system. Federal implementation of the Colorado Model would, therefore, provide for greater constitutional privacy protections for individuals while also improving upon the current process of familial DNA searching.

I. FOURTH AMENDMENT IMPLICATIONS IN THE GOLDEN STATE KILLER INVESTIGATION & PENDING TRIAL

Under the current regulatory scheme surrounding the Fourth Amendment, it is unlikely that any significant constitutional impediments will arise in Joseph DeAngelo's upcoming trial. Assuming, *arguendo*, DeAngelo does assert a constitutional claim, the court will likely begin its analysis by determining whether DeAngelo had a reasonable expectation of privacy in the DNA he shed at the initial crime scene or the more recent DNA he shed on his car door handle and in his trash. [175] Under the abandonment standards articulated in *Greenwood* and *Athan*, the inquiry would likely end at this preliminary juncture. [176] Under *Athan*, as well as under conventional wisdom in police investigations, DeAngelo has no reasonable expectation of privacy in the DNA left in the commission of his original crimes and collected during the course of routine police investigation. [177] Further, in addition to the abandoned DNA later collected by police from a tissue discarded in his trash, the DNA retrieved from the handle of his car--parked in a public parking lot-- would not survive Fourth Amendment scrutiny because both were discarded and subject to public view, therefore constituting a lower manifest privacy interest. [178] Because all three of these samples do not meet the objective reasonableness standard from the perspective of society, DeAngelo could have no reasonable expectation of privacy that would afford him Fourth Amendment protection. [179]

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

Manolakos, Alexandra 10/24/2022
For Educational Use Only

***201** However, it is also important to view this constitutional question from the perspective of the innocent distant family member whose DNA led to the capture and arrest of the perpetrator. This inquiry is much murkier in the Fourth Amendment context. Assuredly, if the DNA had been uploaded to one of the more secure websites, such as 23andMe or Ancestry DNA, the question of reasonableness of the objective expectation of privacy would be more clear based on the safeguards promised in their privacy statements. [180] However, given the objectively lower standard articulated by GEDmatch, there is a significant likelihood that a court would find no Fourth Amendment violation resulting from the police action here. [181] Fourth Amendment protection extends to intrusions of constitutionally protected areas unless the technology used to conduct the search was in general public use. [182] GEDmatch is well within public use as it is marketed as an open-source database in which "information will be shared with other users." [183] The website's very nature facilitates public use, and no user who willingly shares personal data with such a public forum can reasonably expect such data to remain confidential. GEDmatch makes no secret that users may find numerous other uses for the data uploaded to the website and therefore openly employs a "participate at your own risk" policy. Under current Fourth Amendment precedent, there is likely no chance that a court would uphold a constitutional claim purported by the willing GEDmatch user in this case.

II. APPLICATION OF THE COLORADO MODEL TO THE GOLDEN STATE KILLER INVESTIGATION

Unlike the application of Fourth Amendment analysis, the Colorado standard, if applied strictly, could produce vastly different results in the DeAngelo case. Under the Colorado framework, the request for familial DNA searching in this case would come from the policy's second stated source category--directly from law enforcement. [184] Under a federally mandated Colorado-style policy, California state investigators handling the Golden State Killer case could submit a formal ***202** request for familial DNA search analysis of the DNA retrieved from the crime scene. Then, this request would be tested under the strict Colorado criteria. First, law enforcement officials must verify to the crime lab that the DNA had already been put through a CODIS search and yielded no results. [185] As previously discussed, the DNA profile yielded by police using the crime scene DNA left behind by the Golden State Killer was not a match with any of the known felons in the CODIS database. [186] Next, the crime lab would determine whether law enforcement had exhausted all other possible leads. [187] Here, it is clear that after nearly forty years of deliberate investigation, all possible leads had been thoroughly examined. After passing this initial inquiry, the request would then be subject to the professional evaluation of the crime lab analysts. [188] The Golden State Killer case, having gone cold after a period of nearly forty years, is clearly of a significant public interest in terms of safety implications. [189] Under a cost-benefit analysis of the necessity for familial DNA searching in this case, any rational crime lab would undoubtedly move forward, given the sheer amount of lives lost and compassion for the families still suffering. Thereafter, the crime lab analysts would meet with representatives from the California law enforcement agencies who submitted the formal request to fully apprise them of the nature of familial DNA searching and to garner a contractual obligation to continue the investigation if results are successfully yielded. [190] Finally, if a prosecutor had been assigned at that point, she too would be added to this agreement so that all parties share in accountability for the resources expended. [191] Under this scenario, the same results would be produced as would be under the current framework. Even so, the positive implications stemming from the strict scrutiny and accountability standards employed in the Colorado model cannot be diminished. Under these standards, there is an assurance of thoroughness, attention to detail, and accountability, thus ensuring the protection of the rights of all parties involved to the fullest extent possible.

*203 III. THE IMPERATIVE NEED FOR COMPREHENSIVE FEDERAL REGULATION

It is clear from this analysis that no current federal regulations effectively protect the privacy rights of individuals with regard to familial DNA searching in the same comprehensive manner as the Colorado Model. As demonstrated, a simple Fourth Amendment analysis will often fail to extend to such specific instances as those presented here, so long as the DNA collected and tested is publicly available. Additionally, the statutes cited by both 23andMe and Ancestry DNA serve as insufficient guidance for the intricacies involved in DNA retrieval and analysis. The federal legislation contained in 18 U.S.C. § 2703 too broadly covers inquiries with regard to "required disclosures of customer communications or records" in a "remote computing" setting. [192] This incredibly wide-sweeping language is intended to touch upon a variety of web-based communications and

does not inherently evoke any cognizant relation for genealogy websites or familial DNA searching. However, the sheer lack of federal guidance or legislation is not surprising given the relative recency and popularity of such services. As the court stated in *United States v. Jones*, "dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes." [193] With this change in popular attitude must come a change in law.

Specific federal legislation aimed at familial DNA searching would provide a uniformity in the request and analysis process that affords heightened protections of the privacy rights of individuals. Instead of allowing for variances in state-implemented policies, cohesive federal regulations would work directly with existing technology, such as CODIS, to produce the most efficient and accurate results. Federal implementation of the Colorado Model would accomplish these objectives. As previously stated, the Colorado familial DNA searching policy has served as a pioneer for other state policies across the country. [194] The FBI could easily implement the process of carrying out this policy in the same way the CBI conducts it within Colorado. Using the highly sophisticated crime labs already in regular use ***204** within the FBI, analysts could begin implementing the Colorado Model's strict scrutiny standards to requests received from all over the country immediately upon adoption. These standards, applied at the federal level, would more closely align with the goals and purposes of the Fourth Amendment, and would provide the necessary vetting and consideration needed before permitting the encroachment upon those rights. In addition to this enhanced Fourth Amendment protection, this policy would produce more efficient and accurate results through familial DNA searching, allowing federal agents to successfully solve more crimes like the Golden State Killer case.

CONCLUSION

The right to privacy is an integral tenant of the freedoms guaranteed to American citizens in the Constitution. However, the current legal restrictions pertaining to familial DNA searching through genealogy websites provide for little substantive protection of this right. Under the current framework, virtually all law enforcement requests for familial DNA data will survive a constitutional challenge in court, as most samples are submitted voluntarily, and police necessity typically takes precedence over arbitrary and attenuated privacy claims in voluntarily uploaded DNA profiles. Additionally, the current standard does not require any formal process by which police must exhaust other options, nor does it require a cost-benefit analysis of privacy concerns. Therefore, the present system places police necessity--arbitrary or otherwise-- above the individual privacy rights of American citizens. The Colorado Model, conversely, maintains a viable option for police access for familial DNA data, while keeping in mind the sanctity of an individual's right to privacy. By requiring proof of police exhaustion of alternative methods, as well as a thorough interest-balancing analysis, this model would lead to greater police accountability while providing a clear and formulaic process for familial DNA requests. Federal implementation of the Colorado Model would provide a clear and uniform federal standard for familial DNA searching. This proposal would provide a viable solution to the inherent privacy concerns that arise from the growing use of genealogy websites for investigatory purposes. A solution such as this will only become more necessary as public genealogy technology continues to expand. Otherwise, an individual's right to privacy as it currently exists will diminish as it is forced to adapt to police demands.

Footnotes

a1 George Mason University Antonin Scalia Law School, J.D. expected, 2020. This Comment is dedicated in memory of Michelle McNamara, whose tireless search for justice was integral in the Golden State Killer's ultimate apprehension.

1 Juan Carlos Guerrero, *TIMELINE: A Look Back at the Golden State Killer's Crime Spree that Lasted a Decade*, ABC7 (May 23, 2018), https://abc7news.com/timeline-looking-back-at-golden-state-killer-crimes/3391867/.

2 *See* Michelle McNamara, *In the Footsteps of a Killer*, L.A. MAG. (Feb. 27, 2013), https://www.lamag.com/longform/in-the-footsteps-of-a-killer/.

3 Laurel Wamsley, *In Hunt for Golden State Killer, Investigators Uploaded His DNA To Genealogy Site*, NPR (Apr. 27, 2018, 7:31 PM), https://www.npr.org/sections/thetwo-way/2018/04/27/606624218/in-hunt-for-golden-state-killer-investigators-uploaded-his-dna-to-genealogy-site.

4 *Id.*; *see also* Melody Gutierrez, *Golden State Killer Suspect's DNA Taken from Car as he Shopped at Hobby Lobby*, S.F. CHRON. (June 2, 2018, 10:51 AM), https://www.sfchronicle.com/crime/article/Golden-State-Killer-suspect-s-DNA-taken-from-12961700.php.

5 *See* Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767, 779-81 (1999).

6 *See id.*

7 *Id.* at 781-82.

8 MICHELLE MCNAMARA, I'LL BE GONE IN THE DARK: ONE WOMAN'S OBSESSIVE SEARCH FOR THE GOLDEN STATE KILLER 52-53 (Harper Perennial 2019) (2018).

9 *Id.*

10 *Id.* at 53.

11 *Id.*

12 *Id.* at 54.

13 *See generally id.*

14 *See* Guerrero, *supra* note 1.

15 Emily Shapiro, *Inside the Timeline of Crimes by the 'Golden State Killer'*, ABCNEWS (Apr. 26, 2018, 1:34 PM), https://abcnews.go.com/US/inside-timeline-crimes-golden-state-killer/story?id=54744307.

16 MCNAMARA, *supra* note 8, at 4.

17 *See id.* at 328.

18 Joseph Serna & Benjamin Oreskes, *Why did it Take so Long to Arrest the Golden State Killer Suspect? Interagency Rivalries, Old Technology, Errors and Bad Luck*, L.A. TIMES (May 25, 2018, 4:35 PM), http://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-case-20180525-story.html#.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

19 *Id.* The offender has come to be known as "The Golden State Killer," first coined by author Michelle McNamara in a 2013 Los Angeles Magazine article. *See* McNamara, *supra* note 2.

20 Wamsley, *supra* note 3.

21 *Id.*

22 *See id.*

23 MCNAMARA, *supra* note 8, at 144-45; *see also* Wamsley, *supra* note 3.

24 MCNAMARA, *supra* note 8, at 144-45, 302; *see also* Wamsley, *supra* note 3.

25 *See* MCNAMARA, *supra* note 8, at 306.

26 *See generally id.*

27 *Id.* at 283.

28 *See id.* at 286-87, 306.

29 *Id.* at 309.

30 *See* Gutierrez, *supra* note 4.

31 *See* Guerrero, *supra* note 1.

32 *See* Wamsley, *supra* note 3.

33 *Id.*

34 Erik Ortiz, *Golden State Killer Suspect's Capture Sparks DNA Site Privacy Fears*, NBCNEWS (Apr. 27, 2018, 1:49 PM), https://www.nbcnews.com/news/us-news/golden-state-killer-suspect-s-capture-sparks-dna-site-privacy-n869661.

35 *See* Wamsley, *supra* note 3.

36 *Id.*

37 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

38 *See* Ortiz, *supra* note 34.

39 *See* Gutierrez, *supra* note 4.

40 *Privacy Concerns After Public Genealogy Database used to ID "Golden State Killer" Suspect*, CBSNEWS (Apr. 27, 2018), https://www.cbsnews.com/news/privacy-concerns-after-public-genealogy-database-used-to-id-golden-state-killer-suspect/.

41 *Id.*

42 Ortiz, *supra* note 34.

43 *Id.*

44 *See* Ian Cobain, *Killer Breakthrough--the Day DNA Evidence First Nailed a Murderer*, THE GUARDIAN (June 2, 2016, 10:25 AM), https://www.theguardian.com/uk-news/2016/jun/07/killer-dna-evidence-genetic-profiling-criminal-investigation.

45 *Id.*

46 *Id.*

47 *Id.*

48 *Id.*

49 *Id.*

50 *See* Cobain, *supra* note 44.

51 *Id.*

52 *Id.*

53 *Id.*

54 *Id.*

55 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

56 *See* Cobain, *supra* note 44.

57 Some sources spell Mr. Tommie Lee Andrews' name as "Tommy." *Compare* Andrews v. State, 533 So. 2d 841 (Fla. Dist. Ct. App. 1988) ("Tommie Lee Andrews"), *with* Roger Roy, *DNA Test Gets a Chance in Orange Rape Trial*, THE ORLANDO SENTINEL, Oct. 21, 1987, at A1 ("Tommy Lee Andrews").

58 *See* Karen Cormier at al., *Evolution of DNA Evidence for Crime Solving--A Judicial and Legislative History*, 2 FORENSIC MAG., no. 4 (2005), http://tools.thermofisher.com/content/sfs/brochures/cms_042067.pdf.

59 *Id.*

60 *Id.*

61 People v. Castro, 545 N.Y.S.2d 985 (N.Y. App. Div. 1989).

62 *Id.* at 986 (first citing Frye v. United States, 293 F. 1013 (D.C. Cir. 1923) (discussing the admissibility of blood pressure monitoring to determine honesty during questioning); then citing People v. Middleton, 429 N.E.2d 100 (N.Y. 1981) (discussing the admissibility of bite mark evidence)).

63 *Castro*, 545 N.Y.S.2d at 986-87 (quoting *Middleton*, 429 N.E.2d at 103).

64 *Id.* at 987.

65 *Id.* at 999.

66 *Id.*

67 *See* Hibbert, *supra* note 5, at 774.

68 *Id.*

69 *Id.*

70 Jones v. Murray, 962 F.2d 302, 303 (4th Cir. 1992).

71 *Id.* at 310-11.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

72 *See* Hibbert, *supra* note 5, at 775.

73 *Id.* at 779.

74 *Id.* at 776.

75 *See id.* at 779.

76 *Id.*

77 FED. BUREAU OF INVESTIGATION, *Combined DNA Index System (CODIS)*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis#CODIS-and%20NDIS%C20Fact%20Sheet (last visited Oct. 18, 2019) [hereinafter FED. BUREAU OF INVESTIGATION, *CODIS*].

78 *Id.*

79 *Id.*

80 34 U.S.C. § 12592 (2019).

81 FED. BUREAU OF INVESTIGATION, *CODIS*, *supra* note 77.

82 *Id.*

83 *Id.*

84 FED. BUREAU OF INVESTIGATION, *Frequently Asked Questions on CODIS and NDIS*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Oct. 18, 2019) [hereinafter FED. BUREAU OF INVESTIGATION, *CODIS and NDIS FAQs*]. The FBI's Memorandum of Understanding is a mandatory agreement for participation in the NDIS, "documenting their agreement to abide by the DNA Identification Act requirements as well as record-keeping and other operational procedures governing the uploading of DNA data, expungements, CODIS users, audits, etc." *Id.*

85 U.S. CONST. amend. IV.

86 *See* Katz v. United States, 389 U.S. 347, 352-53 (1967).

87 *Id.* at 351.

88 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

89 *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)).

90 *See* *Katz*, 389 U.S. at 351.

91 *See* Oliver v. United States, 466 U.S. 170, 182-83 (1984).

92 *See* *Katz*, 389 U.S. at 357.

93 *See* Kyllo v. United States, 533 U.S. 27, 34 (2011).

94 *See* Michigan v. Chesternut, 486 U.S. 567, 573 (1988) (quoting Terry v. Ohio, 392 U.S. 1, 19 n. 16 (1968)).

95 *See id.* (quoting United States v. Mendenhall, 446 U.S. 544, 555 (1980)).

96 *See* *Katz*, 389 U.S. at 352-53.

97 United States v. Jones, 565 U.S. 400 (2012).

98 *Id.* at 404.

99 *Id.*

100 *See id.* at 404-05.

101 John P. Ludington, Annotation, *Search and Seizure: What Constitutes Abandonment of Personal Property Within Rule that Search and Seizure of Abandoned Property is not Unreasonable--modern cases*, 40 A.L.R. 4th 381 (1985).

102 United States v. Harrison, 689 F.3d 301, 307 (3d Cir. 2012).

103 *Id.*

104 *Id.*

105 *See* California v. Greenwood, 486 U.S. 35, 40 (1988).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

106 *Id.* at 39-40.

107 Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. L. REV. 857, 859 n.10 (2006).

108 State v. Athan, 158 P.3d 27, 37 (Wash. 2007).

109 *Id.*

110 Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

111 Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

112 *Id.* (quoting Riley v. California, 573 U.S. 373, 392 (2014)).

113 *Id.* (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

114 Gregory Rodriguez, *How Genealogy Became Almost as Popular as Porn*, TIME (May 30, 2014), http://time.com/133811/how-genealogy-became-almost-as-popular-as-porn/. In this article, Time Magazine points out that the most popular hobby in the United States is gardening, and the most popular category of website visited is pornography. *Id.*

115 CBSNEWS, *supra* note 40.

116 *See id.*

117 *See generally Privacy and Data Protection*, 23ANDME, https://www.23andme.com/privacy/ (last visited Oct. 18, 2019) [hereinafter *Privacy*, 23ANDME]; *see also Your Privacy*, ANCESTRY, https://www.ancestry.com/cs/legal/privacystatement (last visited Oct. 18, 2019) [hereinafter *Your Privacy*, ANCESTRY]; *see also Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last visited Jan. 21, 2020) [hereinafter *Privacy Policy*, GEDMATCH].

118 *See, e.g., Ancestry International Terms and Conditions*, ANCESTRY, https://www.ancestry.com/cs/legal/row-terms-and-conditions-en (last visited Nov. 21, 2019).

119 *E.g.*, Marcus Moretti & Michael Naughton, *Why Privacy Policies are so Inscrutable*, THE ATLANTIC (Sep. 4, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/.

120 *Privacy*, 23ANDME, *supra* note 117.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

121 *Privacy Highlights*, 23ANDME, https://www.23andme.com/about/privacy/ (last updated Sept. 30, 2019) [hereinafter *Privacy Highlights*, 23ANDME].

122 *Id.*

123 *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ (last visited Oct. 18, 2019). To reach this page, a user must navigate from the 23andMe homepage, to the "Privacy and Data Protection" page through a tab, then through a link on that page to the "Privacy Statement" page, then through a link on that page to the "Transparency Report" page, then finally through a link on that page to the "Guide for Law Enforcement."

124 *Id.*

125 *Id.*

126 18 U.S.C. § 2703 (2019).

127 18 U.S.C. § 2703(c) (2019).

128 *See* 18 U.S.C. § 2703(c)(2)(A)-(F) (2019).

129 *23andMe Guide for Law Enforcement, supra* note 123.

130 18 U.S.C. § 2703(d) (2019).

131 *23andMe Guide for Law Enforcement, supra* note 123.

132 18 U.S.C. § 2703(f) (2019).

133 *23andMe Guide for Law Enforcement, supra* note 123.

134 18 U.S.C. § 2705(b) (2019).

135 *See Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement (last visited Oct. 18, 2019).

136 U.S. CONST. amend. IV.

137 *Your Privacy*, ANCESTRY, *supra* note 117.

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

138 *Id.*

139 *Id.*

140 *Ancestry 2018 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency (last visited Jan 22, 2020).

141 *Compare id., with Ancestry 2017 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency-2017 (last visited Jan. 20, 2020). The 2017 report revealed that Ancestry DNA responded to thirty-one out of a total thirty-four valid law enforcement requests in 2017, all of which were related to investigations of credit card misuse or identity theft.

142 *Privacy Policy*, GEDMATCH, *supra* note 117.

143 *Id.*

144 *Id.*

145 *Id.*

146 *Id.*

147 *Id.*

148 *Privacy Policy*, GEDMATCH, *supra* note 117.

149 *Id.*

150 *Id.*

151 MICHAEL B. FIELD, ET AL., NAT'L CRIMINAL REFERENCE SERV., STUDY OF FAMILIAL DNA SEARCHING POLICIES AND PRACTICES: CASE STUDY BRIEF SERIES 3 (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251081.pdf.

152 *Id.*

153 *Id.* at 5.

154 *Id.*

155 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

156 *Id.* at 6.

157 FIELD, ET AL., *supra* note 151, at 6.

158 *Id.*

159 *Id.*

160 *Id.*

161 *Id.*

162 *Id.*

163 FIELD, ET AL., *supra* note 151, at 7-9.

164 *Id.* at 7.

165 *Id.*

166 *Id.*

167 *Id.*

168 *Id.*

169 FIELD, ET AL., *supra* note 151, at 7.

170 *Id.*

171 *Id.*

172 *Id.*

173 *Id.*

174 *Id.*

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

175 *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

176 *See* California v. Greenwood, 486 U.S. 35, 39-40 (1988); State v. Athan, 158 P.3d 27, 37 (Wash. 2007).

177 *Athan*, 158 P.3d at 37.

178 *Greenwood*, 486 U.S. at 39-40; United States v. Harrison, 689 F.3d 301, 307 (3d Cir. 2012).

179 *Greenwood*, 486 U.S. at 39-40.

180 *Ancestry Guide for Law Enforcement, supra* note 135; *Privacy*, 23ANDME, *supra* note 117.

181 *See Privacy Policy*, GEDMATCH, *supra* note 117.

182 Kyllo v. United States, 533 U.S. 27, 34 (2011).

183 *Privacy Policy*, GEDMATCH, *supra* note 117.

184 FIELD, ET AL., *supra* note 151.

185 *Id.*

186 *See* MCNAMARA, *supra* note 8, at 302; *see also* Wamsley, *supra* note 3.

187 FIELD, ET AL., *supra* note 151.

188 *Id.*

189 *Id.*

190 *Id.*

191 *Id.*

192 18 U.S.C. § 2703(c) (2019).

 © 2022 Thomson Reuters. No claim to original U.S. Government Works.

193 United States v. Jones, 565 U.S. 400, 427 (2012).

194 FIELD, ET AL., *supra* note 151.

30 GMUCRLJ 177

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.