DELAWARE STATE BAR ASSOCIATION

CONTINUING LEGAL EDUCATION

TORTS AND SOCIAL MEDIA

LIVE SEMINAR AT DSBA WITH ZOOM OPTION

SPONSORED BY THE TORTS SECTION
OF THE DELAWARE STATE BAR ASSOCIATION

THURSDAY, NOVEMBER 3, 2022 | 12:30 P.M. – 1:30 P.M.

1.0 hour CLE credit in Enhanced Ethics for Delaware and Pennsylvania Attorneys

ABOUT THE PROGRAM

Join us for this seminar to look at how online conduct can lead towards lawsuits and how to deal with them. Online torts deal with the interactions between consumers, companies, and users all controlled by user agreements, but how do these contracts affect which jurisdictions law can be applied, where lawsuits can be filed, the remedies, and arbitration? During this seminar we will dive into what laws can be applied and how to address these cases, how intellectual property and probate law come into play, and how laws have evolved to address online property rights.

Topics: How Common Law can be applied to online tortious activity; Immunity under the Communication and Decency Act; Statutory Civil Remedies; Delaware State Laws: Civil Liability and Online Property Rights

PRESENTERS

Moderator

Margaret M. DiBianca, Esquire
Clark Hill PLC

Speakers

The Honorable
Danielle J. Brennan
Superior Court of the State of Delaware

Miranda D. Clifton, Esquire
Heckler & Frabizzio, P. A.

Joshua H. Meyeroff, Esquire
Morris James LLP

Visit https://www.dsba.org/event/torts-and-social-media/ 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

Margaret M. DiBianca, Esquire
Clark Hill PLC

Speakers

The Honorable Danielle J. Brennan
Superior Court of the State of Delaware

Miranda D. Clifton, Esquire
Heckler & Frabizzio, P. A.

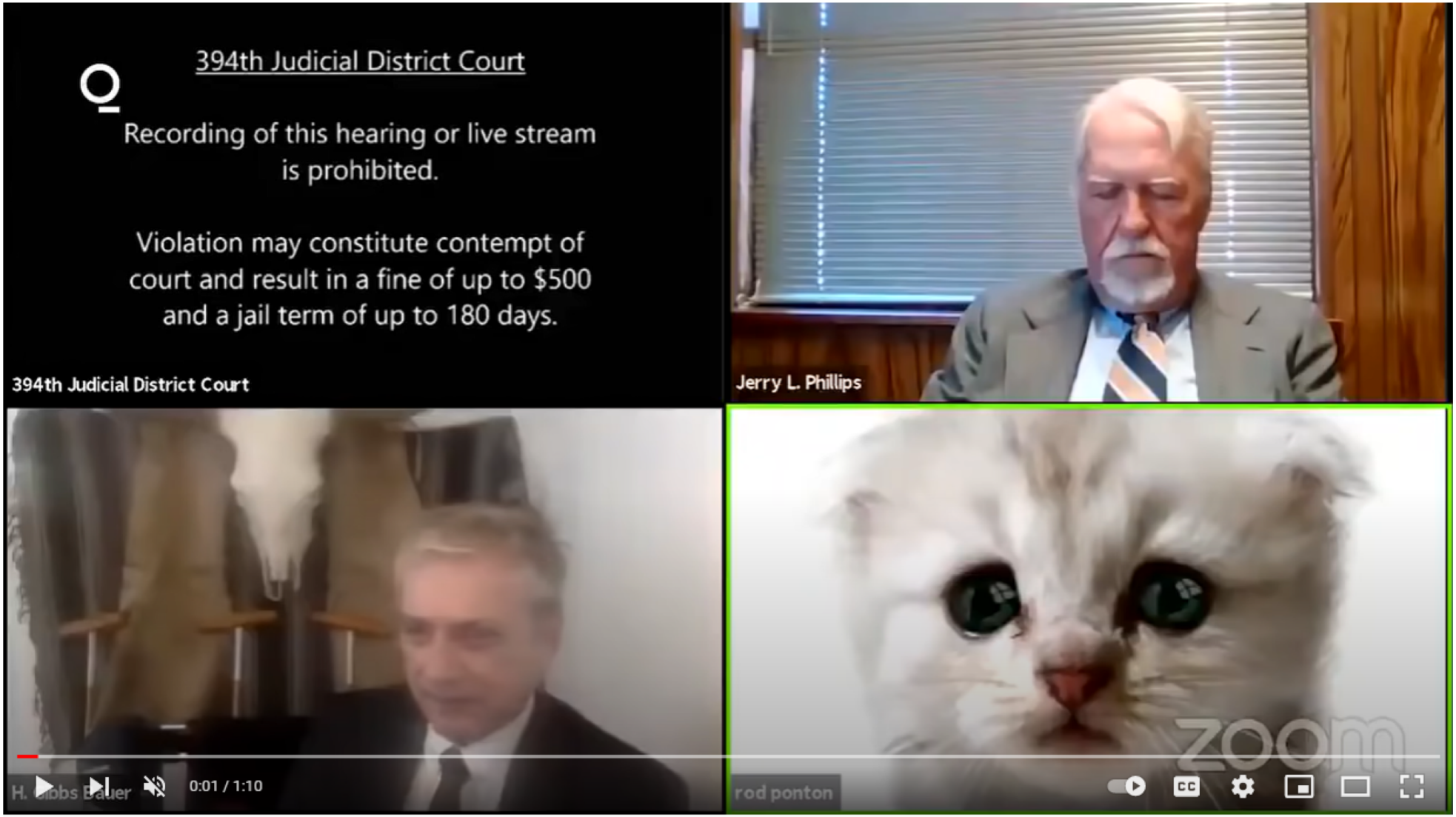
Joshua H. Meyeroff, Esquire
Morris James LLP

Torts & Social Media

DSBA 2022

AGENDA

- Risks of Social Media
- State Tort Laws
- Statutory Remedies
- Ethical Issues

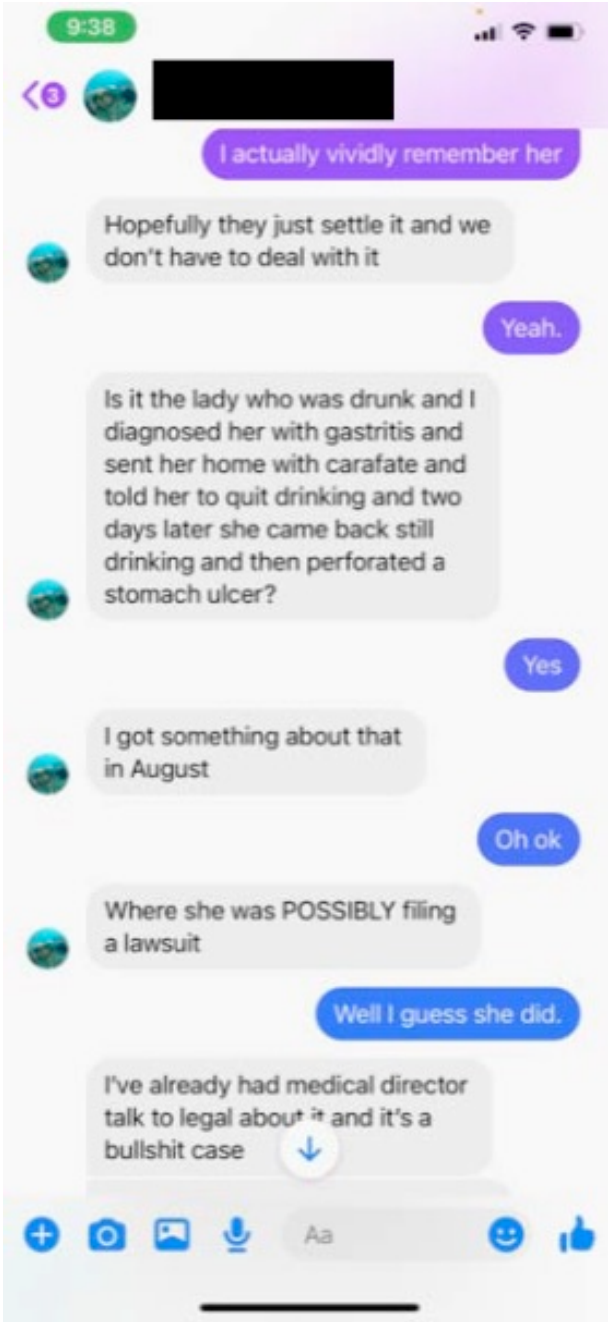

394th Judicial District Court
Recording of this hearing or live stream is prohibited.
Violation may constitute contempt of court and result in a fine of up to $500 and a jail term of up to 180 days.
394th Judicial District Court
Jerry L. Phillips
0:01 / 1:10
zoom
rod ponton

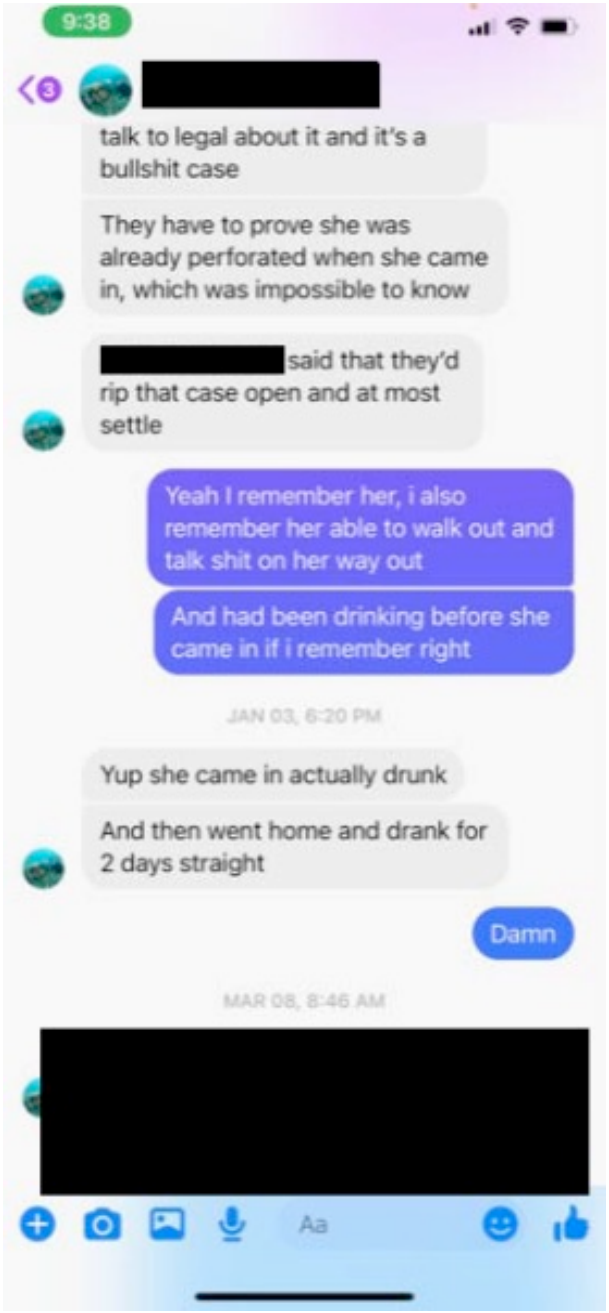

BBC NEWS
zoom

RISKS OF SOCIAL MEDIA

RISKS OF SOCIAL MEDIA

- Posting something online can be problematic with litigation
- Example: in a medical malpractice case, the plaintiff claimed that the care by a physician assistant (PA) in the emergency department was negligent and led to her below-the-knee amputation
- Defense was able to obtain experts to support the PA's care, but…


9:38
[redacted]
I actually vividly remember her
Hopefully they just settle it and we don't have to deal with it
Yeah.
Is it the lady who was drunk and I diagnosed her with gastritis and sent her home with carafate and told her to quit drinking and two days later she came back still drinking and then perforated a stomach ulcer?
Yes
I got something about that in August
Oh ok
Where she was POSSIBLY filing a lawsuit
Well I guess she did.
I've already had medical director talk to legal about it and it's a bullshit case
Aa


9:38
[redacted]
talk to legal about it and it's a bullshit case
They have to prove she was already perforated when she came in, which was impossible to know
[redacted] said that they'd rip that case open and at most settle
Yeah I remember her, i also remember her able to walk out and talk shit on her way out
And had been drinking before she came in if i remember right
JAN 03, 6:20 PM
Yup she came in actually drunk
And then went home and drank for 2 days straight
Damn
MAR 08, 8:46 AM
[redacted]
Aa

RISKS OF SOCIAL MEDIA (CONT'D)

- Facebook messages led to significant credibility issues
  - Made PA look uncaring
  - Made nurse look uncaring
- Led to settlement rather than risk trial

ADMISSIBILITY OF SOCIAL MEDIA EVIDENCE AT TRIAL

- Social media evidence is admissible at trial so long as there is sufficient evidence that the posts/information are what the proponent claims that they are (*Parker v. State*, 85 A. 3d 682, 683 (Del. 2014)

ADMISSIBILITY

- *Parker v. State*, 85 A. 3d 682 (Del 2014): the defendant was charged with assault after fighting with another woman. The defendant claimed self-defense, but the State wanted to introduce Facebook messages she made after the altercation to undercut her self-defense argument
- The defendant objected to the admission of these posts on the bases that these were not authentic, but the trial court admitted them
- The Delaware Supreme Court affirmed and held that they were admissible
- The Supreme Court noted social media evidence is admissible so long as it can be verified (by things like witness testimony, corroborating evidence, distinctive characteristics, or evidence of the technical process or system that generated it

EMPLOYERS AND SOCIAL MEDIA

- Employers cannot monitor or intercept email unless the employer has first given a one-time written or electronic notice to the employee (19 Del. C. § 705)
- Provides for a civil penalty of $100 for each violation
- But…
  - EXCEPTION: when employer implements processed for computer system maintenance and/or protection, and for court-ordered actions.

EMPLOYERS AND SOCIAL MEDIA (CONT'D)

- 19 *Del. C*. § 709A: Delaware law prohibits employers from asking an applicant or employee to:
  - disclose username or password information to enable the employer to access the applicant's or employee's personal social media;
  - access personal social media in the presence of the employer;
  - use personal social media as a condition of employment;
  - divulge any personal social media, unless an exception applies; add a person, including the employer, to the list of contacts associated with the personal social media of the employee or applicant, or invite or accept an invitation from any person, including the employer, to join a group associated with such personal social media; or
  - alter the settings of an employee's or applicant's personal social media that affect a third party's ability to view its contents.

EMPLOYERS AND SOCIAL MEDIA (CONT'D)

- Employers are also prohibited from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee for refusing to comply with a demand for access that violated the above restrictions. BUT…
- Employers can access or require access to devices or services provided by the employer

EMPLOYERS AND SOCIAL MEDIA (CONT'D)

- For example, employers can:
  - exercise their rights under their personnel policies, federal or state law to require or request an employee to disclose their username, password, or social media "reasonably believed to be relevant" to an investigation of alleged employee misconduct or violation of applicable laws and regulations
  - Access, block, monitor, or review electronic data stored on an employer's network or on an electronic communications device supplied by or paid for by the employer
  - Screen applicants or employees, monitor or retain employee communications
  - Access, use, or view information about an applicant or employee available in the public domain

EMPLOYERS AND SOCIAL MEDIA (CONT'D)

- Likewise, an employer can investigate and punish conduct that is damaging to the employer or business. Employers can retain control over company accounts created for business purposes
- *Christian v. New Castle County Head Start*, 2018 WL _ (Del. Super. Ct. Feb. 16, 2018): Employee acknowledged her employer's social media policy prohibiting negative postings on social media about her employer, yet posted negative things. She was terminated, and both the Division of Unemployment Insurance and Superior Court agreed that this termination was appropriate. As a result, she was not entitled to unemployment benefits.

DESTRUCTION OF SOCIAL MEDIA

- There is no requirement to destroy social media postings as a general matter
- BUT: Delaware law requires a commercial entity to take reasonable steps to destroy social media postings that contain personal identifying information it possesses only if it seeks "permanently to dispose of records containing consumers' personal identifying information within its custody or control" (6 Del. C. § 5002C)
  - In other words, destruction of materials extends to digital media

BASES OF LIABILITY

- As a general rule, social media companies are protected from civil liability for social media posts
- Communications Decency Act, 47 U.S.C. Sec. 230
  - Providers of social media are not treated as the publisher of any information provided by another information content provider and are not liable for defamation posted on their sites
  - Law limits civil liability for actions taken in good faith to restrict access that the company believes to be objectionable
    - In other words, social media is not responsible for what its users post
  - Law requires computer service provider to notify its users of availability of parental control protections

BUT…

BASES OF LIABILITY (CONT'D)

- Communications Decency Act does not limit other state civil remedies, intellectual property laws, criminal laws, sex trafficking laws
- In Delaware, common law claims remain viable
  - Some examples include:
    - Invasion of privacy
    - Defamation
    - Harassment
    - Tortious interference with business relations
- Can pursue intellectual property violations
- Depending on the type of claim, one can file in Superior Court or Federal Court

WHAT HAPPENS TO MY SOCIAL MEDIA WHEN I DIE?

- Delaware has not adopted the Revised Uniform Fiduciary Access to Digital Assets Act; instead, it has adopted the Fiduciary Access to Digital Assets and Digital Accounts Act (12 Del. C. §§ 5001-5007)
  - Similar in that it grants a fiduciary access to a decedent's digital assets
  - Permits a fiduciary to manage those assets
  - Custodian who relies on the fiduciary's written notice in good faith is protected
- Many states have adopted the Revised Uniform Fiduciary Access to Digital Assets Act, which likewise allows a fiduciary to manage the decedent's or incapacitated person's digital assets
  - The act restricts the fiduciary's access to email, text messages, and social media accounts unless the original user consented in a formal record, like a will or trust

TORTS

INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

- Online Application
- "Cyber Bullying"
- *Fischer v. Maloney*, the New York Court of Appeals adopted the tort of intentional infliction of emotional distress from the Second Restatement of Torts, which reads:
  - One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress

IIED

- Delaware:
  - Negligent Infliction of Emotional Distress (*Robb v. Pennsylvania RR Co.*, 210 A.2d 709 (Del. 1965))
  - Plaintiff has to be:
    - in the "immediate area of physical danger" and
    - suffered "physical consequences"
- Situations conceivable where it can be applied in DE in online situations

DEFAMATION ONLINE

- Problems with Anonymous Posters
  - Subpoena ISP
  - First Amendment Concerns – fear of chilling free speech if subpoenas can readily be issued
  - DE Supreme Court: *John Doe No. 1 v. Cahill*, 884 A2d 451, that the good-faith standard is not sufficient to protect legitimate Internet communications and that actual proof of some violation of law will be required before a subpoena is issued.
  - This holding is for Public Figures
  - Set standard for Delaware courts to apply "when faced with a public figure plaintiff's discovery request that seeks to unmask the identity of an anonymous defendant who has posted allegedly defamatory material on the internet."
    - After considering various options for such a standard, the court decided to require "a showing of prima facie evidence sufficient to withstand a motion for summary judgment."
    - Unsure if "good faith" standard would be OK if NOT a public figure

DEFAMATION ONLINE

- Problems with Anonymous Posters
  - Subpoena ISP
  - First Amendment Concerns – fear of chilling free speech if subpoenas can readily be issued

DEFAMATION ONLINE

- DE Supreme Court: *John Doe No. 1 v. Cahill*, 884 A2d 451, that the good-faith standard is not sufficient to protect legitimate Internet communications and that actual proof of some violation of law will be required before a subpoena is issued.
- This holding is for Public Figures
- Set standard for Delaware courts to apply "when faced with a public figure plaintiff's discovery request that seeks to unmask the identity of an anonymous defendant who has posted allegedly defamatory material on the internet."
  - After considering various options for such a standard, the court decided to require "a showing of prima facie evidence sufficient to withstand a motion for summary judgment."
  - Unsure if "good faith" standard would be OK if NOT a public figure

CAHILL CONT'D

- In Delaware, those wishing to challenge online communications will now have two hurdles to surmount. First, they must satisfy the new standard for obtaining a subpoena to identify the anonymous poster; and second, they must satisfy a court that the material posted would be interpreted as constituting fact rather than opinion.
- Supreme Court ruled summarily that "no reasonable person could have interpreted these statements as being anything other than opinion." (note: did not remand case for trial court determination)

DE ANTI-SLAPP LAW

- SLAPP =“Strategic Lawsuits Against Public Participation”
- DEL. CODE ANN. tit. 10, §§ 8136 – 8138 (1992)
- Statements made by an applicant, permittee, or related person regarding a government licensing, permitting, or other decision, are protected.
- Under DEL. CODE ANN. tit. 10, § 8138, a SLAPP defendant may recover compensatory and punitive damages, in addition to fees and costs, upon an additional demonstration that the SLAPP was commenced or continued for the purpose of harassing, intimidating, punishing, or otherwise maliciously inhibiting, the free exercise of speech, petition or association rights.

LITIGATION

- In *Agar v. Judy,* C.A. No. 9541-VCL (Del. Ch. Jan. 19), a rare case involving resort to a Delaware statute's legislative history, Vice Chancellor Laster held that Delaware's anti-SLAPP statute is to be construed narrowly so as to be applicable only to public petition and participation in land use proceedings, and is not a broad legal protection against defamation claims.

DELAWARE ONLINE PRIVACY AND PROTECTION ACT (DOPPA)

- Title 6 of the Delaware Code, Chapter 12, Sections 1201C-1206C
- Three areas of compliance:
  - (1) advertising to children;
  - (2) conspicuous posting of a compliant privacy policy; and
  - (3) enhancing the privacy protections of users of digital books ("e-books").

DELAWARE ONLINE PRIVACY AND PROTECTION ACT (DOPPA)

- Website and app operators that direct their services to children must ensure that they do not advertise or market certain enumerated content that are considered by the law to be inappropriate for children's viewing, such as:
  - alcohol,
  - tobacco,
  - firearms,
  - pornography, and a host of other categories delineated by the law.

DELAWARE ONLINE PRIVACY AND PROTECTION ACT (DOPPA)

- In seeking to regulate sites that are directed to children, the Delaware law compliments the federal Children's Online Privacy Protection Act ("COPPA").
- However, DOPPA has a wider reach, as it defines children as anyone under the age of 18, while the federal law regulates online content directed to those under 13.

NEGLIGENCE ACTIONS

- DOPPA violations prosecuted by DDOJ, however civil applications
- Violation *per se* negligence?

TRESPASS AND CONVERSION ONLINE APPLICATION?

- Both trespass to chattel and conversion deal with wrongfully interfering with a person's personal property.
- Both are intentional torts that refer to a wrongful, intentional interference with the possession of someone's personal property. Trespass to chattels and conversion deal only with personal property. They do not apply to the interference of real property or any interest in land
- Conversion occurs when a person uses or alters a piece of personal property belonging to someone else without the owner's consent. The degree of interference for conversion must be so serious that the tortfeasor may be required to pay the full value of the property. Trespass to Chattel can occur when less than the full value of the property is taken
- Delaware Supreme Court decisional law regarding INTANGIBLE property – can it apply? So far? No.
- Applied in cyber hacking situations; Identity theft

NEGLIGENCE, TOO?

- It depends.
- Cyber Hacking? Possibly
  - Standing has been biggest issue so far
- Other Scenarios?
  - Anti-SLAPP?
  - DOPPA?

STATUTORY REMEDIES

OVERVIEW

- Digital Millennium Copyright Act (DMCA) – 1998
- Online Copyright Infringement Liability Limitation Act (OCILLA)
- The Computer Fraud and Abuse Act (CFAA) – 1986 Amendment

DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA) - 1998

- Designed to Protect Copyright Holders from online theft, specifically from the unlawful reproduction or distribution of their works
- Covers music, movies, text and anything that is copyrighted.
- Essentially criminalizes pirating.

ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION ACT (OCILLA)

- Federal Law that creates a conditional "safe harbor" for online service providers (OSP) including internet service providers (ISP) and other internet intermediaries by shielding them for their own acts of copyright infringement or secondary liability for the infringing acts of others
- Passed as part of the DMCA.
- Still must meet conditions.

CONDITIONS FOR OCILLA

To qualify, the online service provider must:

1. Not receive a financial benefit directly attributable to the infringing activity
2. Not be aware of the presence of the infringing material or know any facts or circumstances that would make infringing material apparent
3. Upon receiving notice from copyright owners or their agents, act expeditiously to remove or disable access to the purported infringing material

THE COMPUTER FRAUD AND ABUSE ACT (CFAA) – 1986 AMENDMENT

- Amended 1989, 1994, 1996, 2001, 2002 and 2008
- Addresses Hacking. The law prohibits accessing a computer without authorization or in excess of authorization.
- Expands existing tort law to intangible property
- Also limits federal jurisdiction to cases "with a compelling federal interest…where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature"

LEGAL ETHICS


Add as Friend


TikTok

Robert L. McKenna III

EDUCATION

BAR ADMISSIONS

MEMBERSHIPS

COMMUNITY INVOLVEMENT

HONORS AND AWARDS

Robert L. McKenna III

Senior Partner