Cyber-Privacy and the Internet

Theodore Roosevelt Inn of Court

February 3, 2020

Program Participants:

- Elizabeth E. Schlissel, Esq.
- Thomas A. O'Rourke, Esq.
- Andrew M. Thaler, Esq.
- Ellen Tobin, Esq.
- Emma Bausert
- Kimberly E. Capuder
- Ron Eniclerico
- NallyAnn Scaturro

Welcome to the Jones' Family Dinner

Source: *Hindustan Times*

pennold • Follow
Saint Georges Hotel, London

pennold •Would you rather be overdressed or underdressed for an occasion?• I'm either in sweatpants and flats or a gown and platforms, covered in glitter. There is no in-between.

Taken by @keatonnchau on the way to hang out with @luisachristie and the @atlanticrecordsuk crew, to watch @avamax and @monetxchange perform at @heaven.nightclub. It was a lot of fun! There was even a cute dog I could pet backstage. Night made.
Outfit: lingerie by @malicelingerie, neck jewels @shopdalmata, hand piece @lorysunartistry, belt @tealecocothelabel, dress @asos.
Makeup: @fentybeauty lip paint, @meltcosmetics eyeshadows, @katvondbeauty highlighter,

14,696 likes

5 DAYS AGO

Add a comment...

Source: Socialbakers.com

What a data broker's profile on you might look like

Source: Privacy International

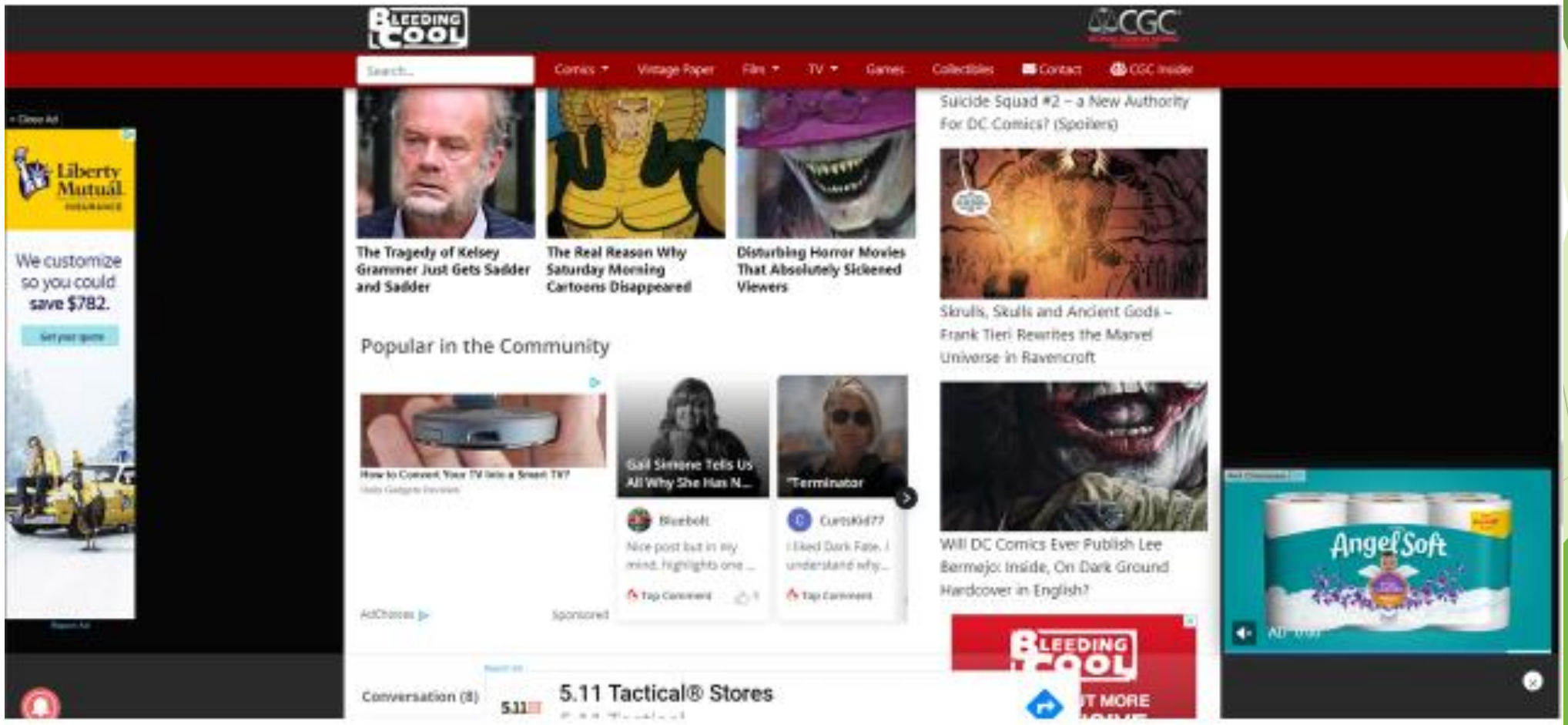
Data Brokers

You may not know them, but they know you

- Data brokers collect and collate information gathered from millions of Internet users
- Data collected includes browsing history, public records, purchasing history
- Tracking makes use of cookies - pieces of code that allow companies to track an individual's movements across various sites
- Information can be sold to advertisers, people search sites, or anyone else who wants to buy it

Sources: *Wired*, *Vice*

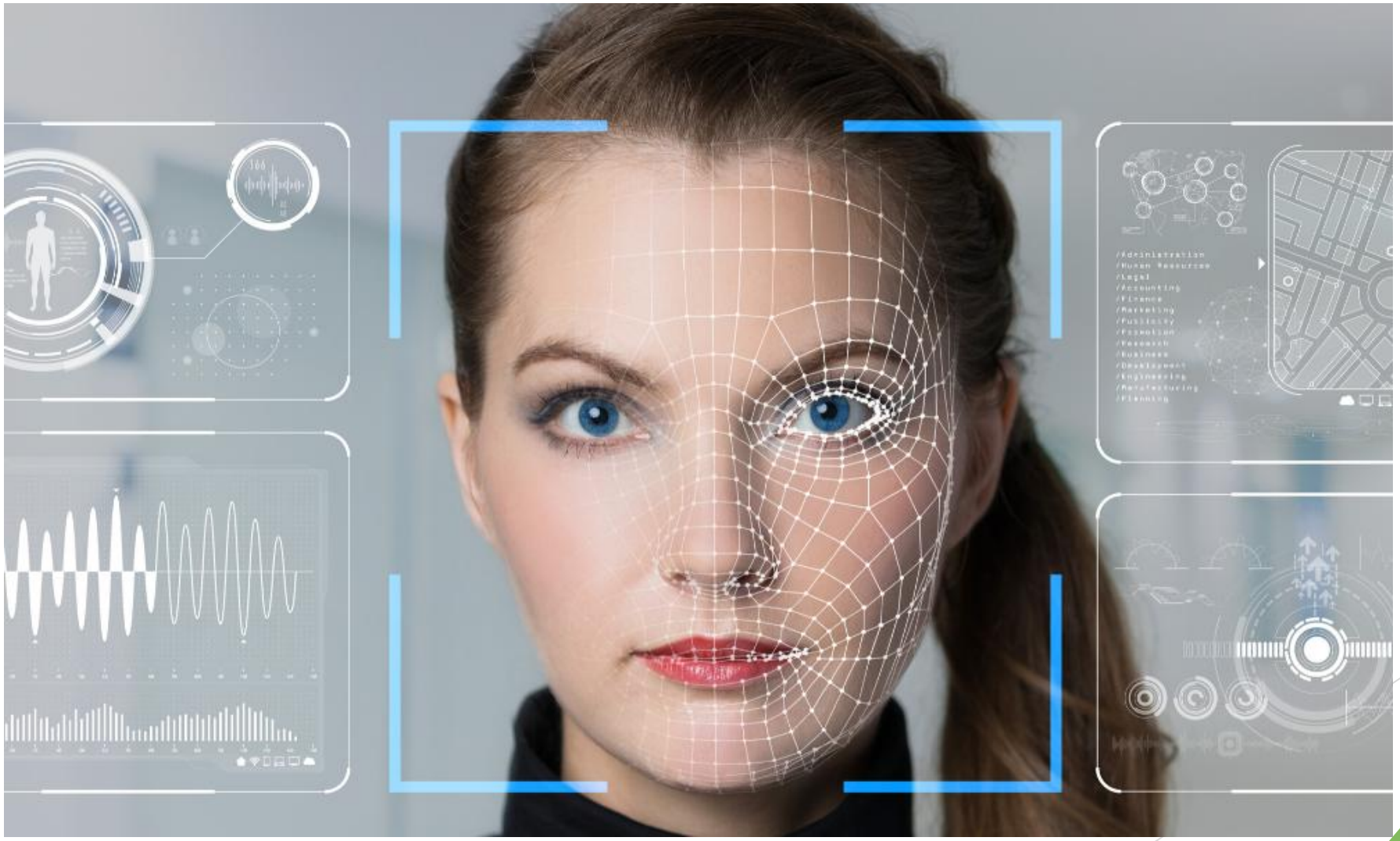
How many ads are on this screen?



Risks of Sharing Your Children's Information Online

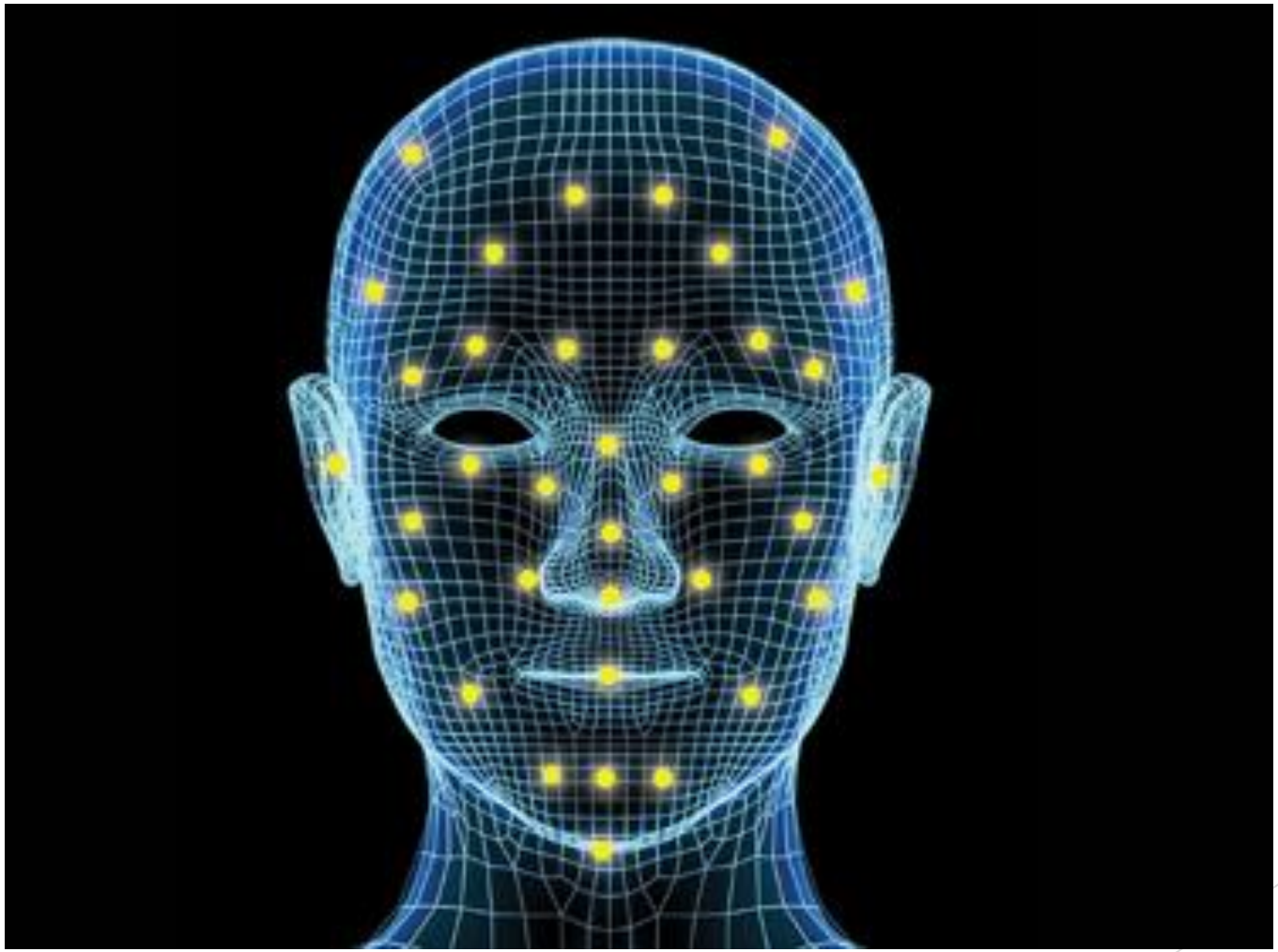
- Parents posting constant information regarding their children are exposing their children to risks of potential fraud and identify theft later in life.
- Data such as photographs, birthdays, places of birth, mother's maiden name, the names of pets, and sports teams they support will still be accessible to hackers once the child is an adult.
- Parents should take caution regarding what data they are putting on the internet about their children
  - "Sharenting" Now May Lead to Identity Theft Later, by Maghan Morovick Walbert

Facial Recognition Technology




OPEN 24 HOURS
A BRONX TALE
BROADWAY'S NEW HIT MUSICAL
The New York Times CRITICS' PICK
"A COMBINATION OF JERSEY BOYS & WEST SIDE STORY"
WHO'S BREAKINGBARRIERS?
Miles Regis
Painter | Technologist | Creator
#ARTISTS4EKF
See how we're breaking barriers at:
encourage-kids.org/artists
CATS
SHOTS FIRED
TONIGHT
FOX 5
SHARE AN ICE COLD Coke
TOSHIBA
TDK
4:44
McDonald's
ATM

Facial Recognition Technology



Cooler Screens

First Amendment Issues: Right of Freedom of Association and Right to Privacy

- Use of Facial Recognition Technology could:
  - Impinge upon the right to anonymous speech and association
  - Impinge upon the ability to associate freely and advocate for minority positions
  - Have a chilling effect on individual's behavior and lead to self-censorship

Fourth Amendment Issues:
Unlawful Search of a Place Where a Person Has a Reasonable Expectation of Privacy

- *Katz v. United States* (389 U.S.347 (1967)
  - Two part test:

    (1) whether the person exhibited an actual , subjective expectation of privacy; and

    (2) whether that expectation is one that society recognizes as reasonable

Relying on Katz, Supreme Court rules government violated Fourth Amendment when it received historical cell site location information (CSLI) without first obtaining a search warrant.
Carpenter v. United States (138 S.Ct.2206 (2018)

- Take away:
  - Law enforcement must now seek a search warrant for individual personal CSLI from phone companies in these specific situations: where no exigent circumstances exist and for date ranges of more than six days.
  - Individuals have an expectation of privacy in their information acquired in large quantities over a extended periods of time even when possessed by third parties.

Facial Recognition Technology

Facial Recognition Technology

- **Legislation in various states and cities have banned and/or put limits on facial recognition technology.**
  - Ex: California bill A.B. 1215: Body Camera Accountability Act. It became effective January 1, 2020 and prevents California law enforcement agencies from adding or using FRT to body-worn cameras.

Facial Recognition Technology

- **What is it?**
  - Uses a database of photos to identify persons in security photos and videos
  - It does this by using biometrics to map features of faces, such as the distance between a person's eyes and the distance between their forehead and chin.
- **Where is it used?**
  - At airports, venues, shopping centers, unlocking your iPhone, automatic tagging of photos on Facebook, and by law enforcement.

Facial Recognition Technology

- **What are some of the issues? Why should we be concerned?**
  - Lack of federal regulations, inaccuracy, biases and misinformation.
  - Law enforcement agencies including the FBI and police departments in NYC, Chicago, Detroit and Orlando use Facial Recognition Technology. There are concerns about misidentifications, wrongful convictions, and invasion of privacy, in addition to First and Fourth Amendment concerns.
  - FRT is most accurate when the picture is stationary and head-on. However, changing features such as hair, facial hair, weight, and aging leads to inaccurate results. Additionally, research has found more inaccuracy when identifying people of certain demographics, such as those who are African American.

Facial Recognition Technology

Half of American adults – more than 117 million people – are in a law enforcement face recognition network, according to a report by the Center on Privacy & Technology at Georgetown Law. The study, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* found that one in four law enforcement agencies can access face recognition and that this use is almost completely unregulated. The study is available at ***ww.perpetuallineup.org***.

Georgetown Law Center on Privacy & Technology 10/18/16

American Civil Liberties Union in California released documents showing the Maryland Image Repository System, which lets police compare images of unidentified criminal suspects with millions of motor vehicle records using facial recognition, this was used to monitor protesters during the 2015 unrest and rioting in Baltimore.

Maryland's use of facial recognition software questioned by researchers, civil liberties advocates

(The Baltimore Sun 10/18/16)

Facial Recognition Technology

Approximately half of adult Americans' photographs are stored in facial recognition databases that can be accessed by the FBI, without their knowledge or consent, in the hunt for suspected criminals. About 80% of photos in the FBI's network are non-criminal entries, including pictures from driver's licenses and passports. The algorithms used to identify matches are inaccurate about 15% of the time, and are more likely to misidentify black people than white people.

The Guardian US edition (online article more than 2 years old) citing facts presented to House oversight committee

Facial Recognition Technology

- 80 percent of the photos that appear in the FBI's facial-recognition network are of non-criminals. Only 8 percent show known criminals.
  - *The Atlantic* 10/19/16 citing *Georgetown Law Center on Privacy & Technology Report*

Raise your hand if you have an Apple’s iPhone X series (or greater), Samsung’s Galaxy Note 8 and 9, Google Pixel 4, Motorola Moto G6, OnePlus 6, LG G7.

Facial Recognition & Smartphones

- Facial recognition uses the camera on your phone to analyze multiple parts of your face, like the placement of your eyes and width of your nose, to combine these features into a unique identification code.
- Chances of a random person being able to unlock your phone are 1 in 1 million. But that doesn't mean your image is safe from hackers or free from privacy concerns.
- It is estimated that over 1 Billion smartphones will use face scanning within the next two years.

All the Information Your Phone is Tracking

- Every place you've ever been – Location Services (Compass and GPS)
- Everything you've told Siri
- Your personal IDs, passcodes, and passwords.
- Every message you send
- How fast you're traveling (Accelerometer)
- All the information you give to Google
- All the information you give to your Apps
- Your heartrate
- How you hold your phone / how it is positioned in a three-dimensional space (Gyroscope)

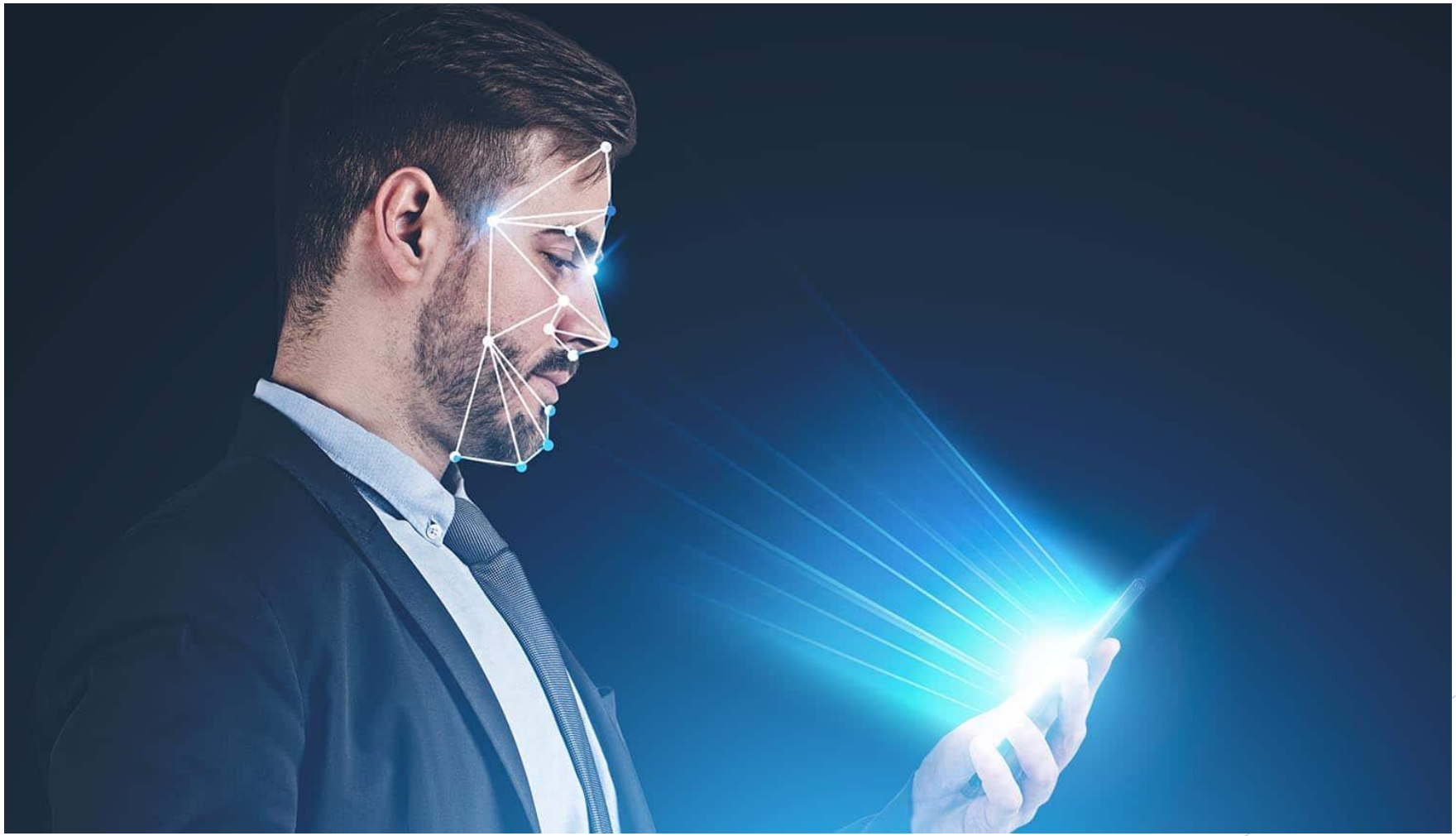
Facial Recognition Used to ID Suspects

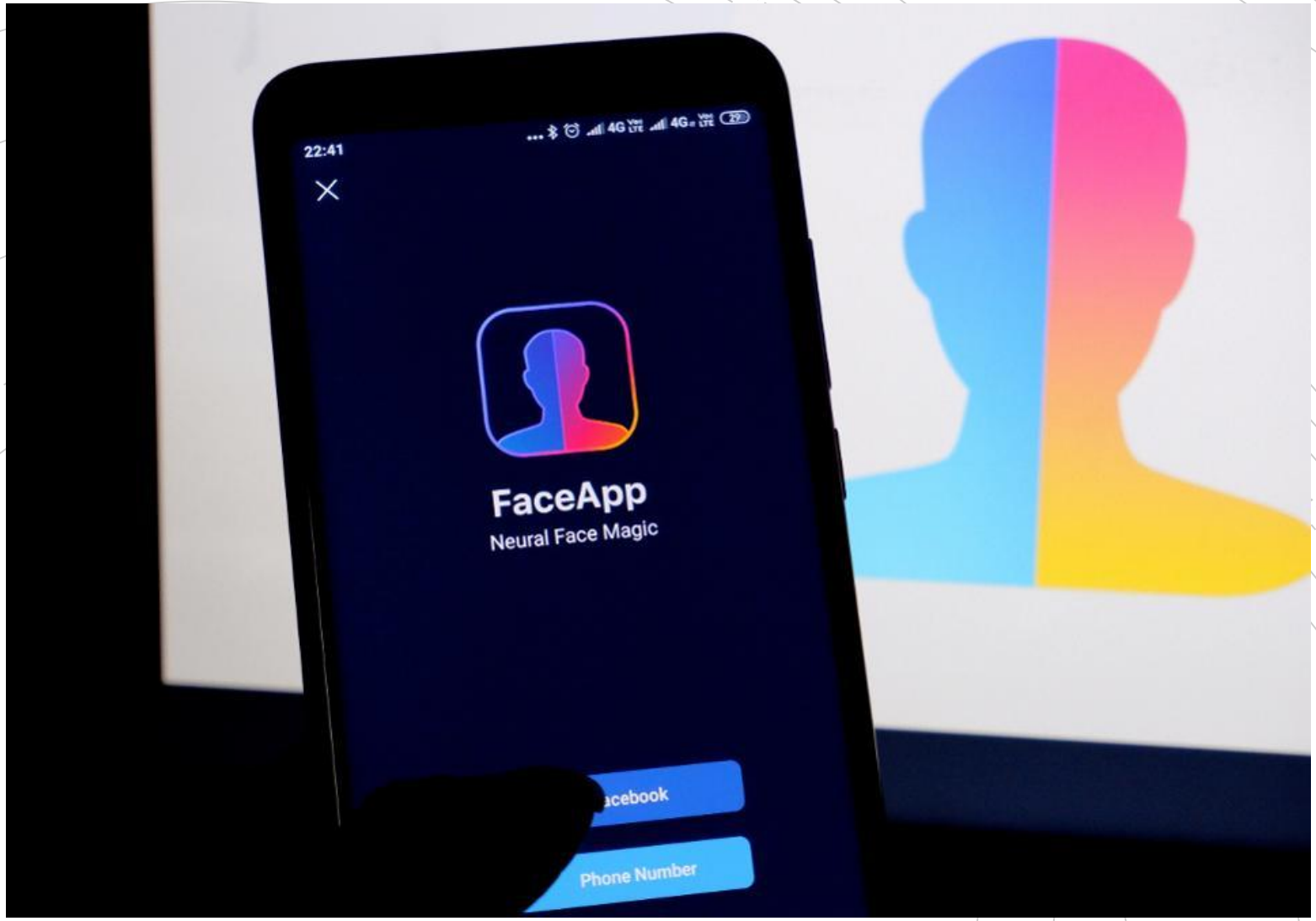
Query:

- What is the proper balance between need for information and the right to privacy?

- How will courts shape FRT and other technology in the future?

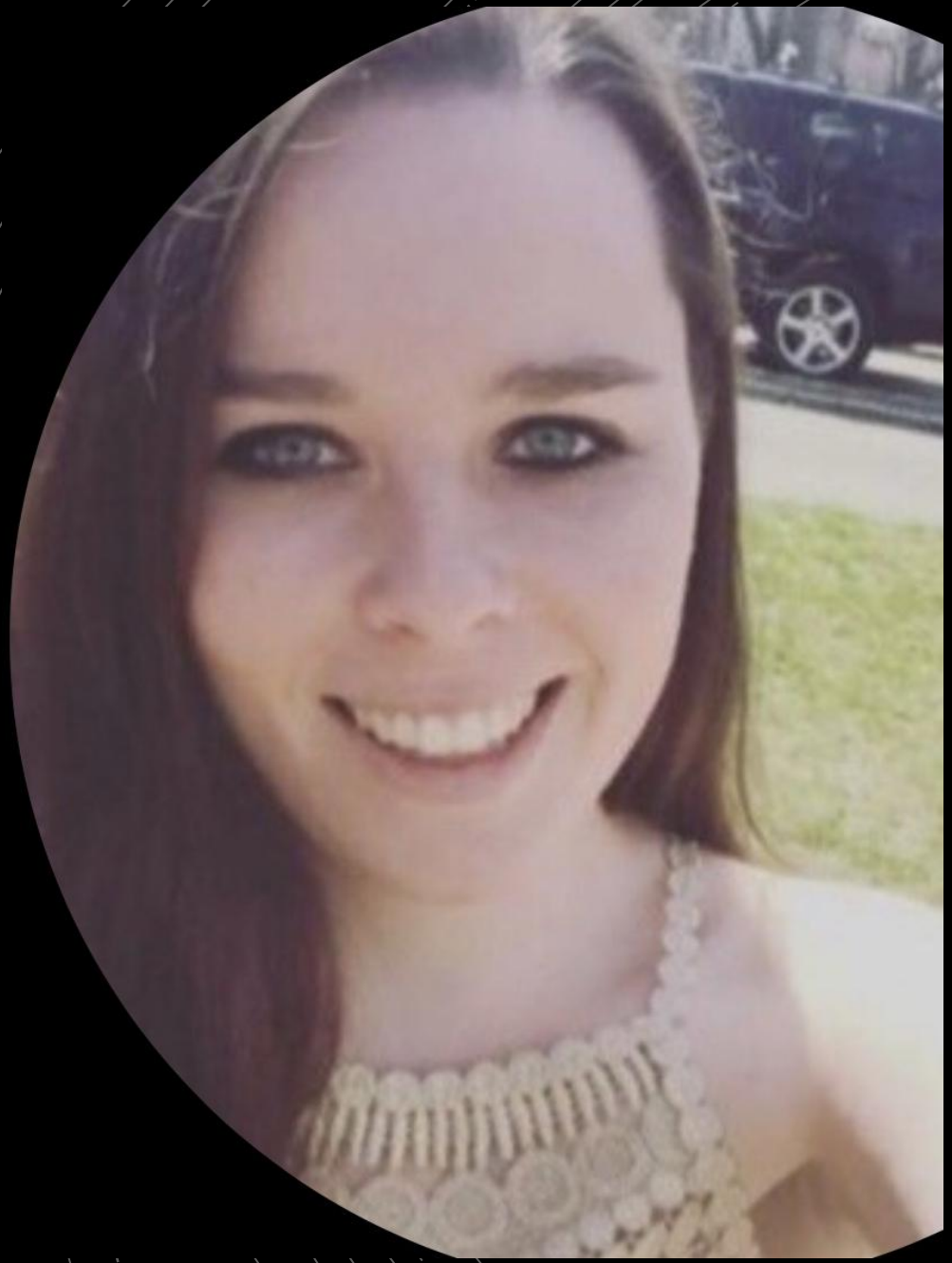
Facial Recognition Technology





FaceApp

The Jonas Brothers' Aging FaceApp



"The unfortunate reality is that most messaging apps have vulnerabilities that can be exploited by sophisticated cyber spies. No messaging service is bulletproof."
-Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black.

- Don't use private messages on Facebook, Twitter, Snapchat, LinkedIn, Instagram, etc. for communicating any secure or private information.
- Anything, even private messages, can be hacked, even if the website does have security settings to attempt to restrict people and hackers from accessing messages.
- 2019 Example: vulnerability of "WhatsApp," which is owned by Facebook, and is the world's most popular messaging platform. This app was targeted by spyware, which allegedly permitted an Israel-based company to install malware onto phones that had downloaded the app. Supposedly, this malware could have been used to tap calls or access photos made and sent on WhatsApp.
- Popular apps are the ones that are and will be targeted because "that is where the users are." –Tom Uren, senior analyst at the Australian Strategic Policy Institute's International Cyber Security Centre.

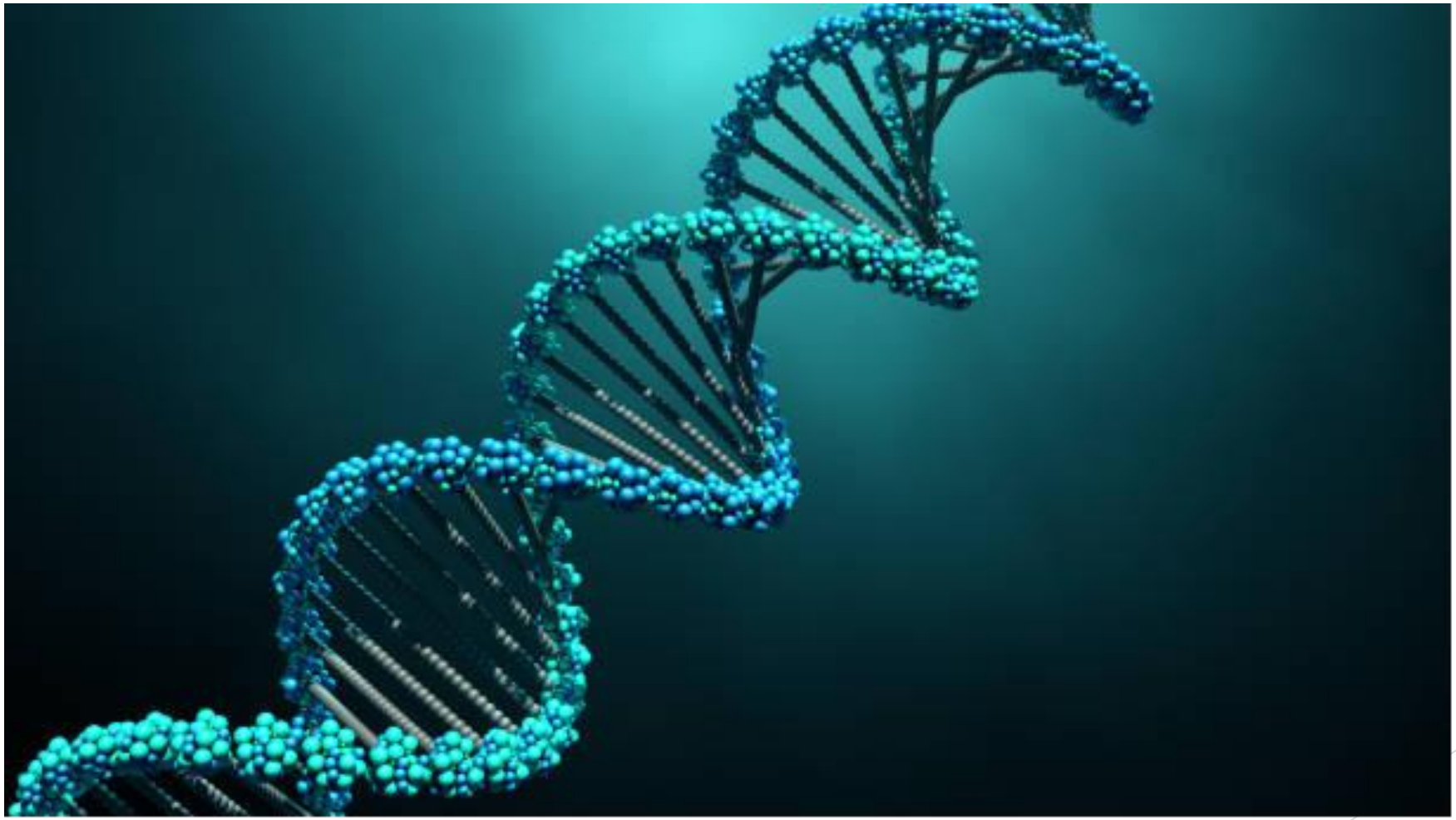
DNA

Raise your hand if you know anyone who has had their DNA tested.

DNA


YOUR DNA TEST RESULTS CAME IN.
OH? WHAT DO THEY SAY?
WELL...THERE SEEMS TO BE A LITTLE BIT OF BEFUDDLEMENT.
YOU'RE EITHER 1/3 SCANDINAVIAN, 1/3 IRISH, AND 1/3 ENGLISH SPANIEL, OR ELSE THE SAMPLE WAS CONTAMINATED SOMEHOW.
10/7
WHAT?
© 2016 Brian Crane. dist. by Washington Post Writers Group
© Brian Crane.

DNA



GED PRIVACY TERMS

- *Your DNA; DNA of a person for whom you are a legal guardian; DNA obtained and authorized by law enforcement to identify a perpetrator of a violent crime against another individual, where 'violent crime' is defined as murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault*

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

- "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."
- "With access to [cell site location information] the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers…"
- "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."
- "Our decision today is a narrow one. We do not express a view on matters not before us…. We do not…call into question conventional surveillance techniques and tools, such as security cameras."

CCPA

- The California Consumer Privacy Act (CCPA) is the first consumer privacy act in the country. No other US state has provided its citizens with protections similar to the General Data Protection Regulation (“GDPR”), which include a transparency right that requires companies to inform consumers about the data collected and shared, and gives them a right to access, to delete, and to opt-out.

Senate Bill 5642 – New York Privacy Act

- New York Privacy Act if passed, would impose stricter requirements on companies than the California Consumer Privacy Act and provide legal innovations that would change the current framework of U.S. privacy law. Senate Bill 5642.

Jury Lab Video

Comment 8 to the NYRPC 1.1

- To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

What are attorney obligations regarding wayward emails?

- As an attorney, if you realize that you have accidentally sent materials to an adversary or third party, you should notify that party immediately, inform them of the situation and request that they destroy, sequester, or return the documents. If the recipient of the wayward email is a lawyer, Rule 4.4(b) of the NYRPC requires the attorney to notify you that he or she received your confidential materials, but the Rule does not currently require the recipient to take further action.

The American Bar Association Standing Committee on Ethics and Professional Responsibility issued Opinion 477, which provides a list of best cyber security practices for attorneys:

- (1) understand the nature of the cybersecurity threat, including a careful consideration of the sensitivity of a client's information and whether a particular client is a higher risk for attack;
- (2) understand how the firm's electronic communications are created and stored, so that a lawyer may access and manage the risk of inadvertent disclosure;
- (3) understand and use reasonable security measures, such as the use of a secure internet access methods;
- (4) train non-lawyer support staff in the handling of confidential client information;
- (5) clearly and conspicuously label confidential client information as "privileged and confidential; and
- (6) conduct due diligence on third party vendors providing digital storage and communication technology.

Questions?