The Intersection of Biometric Technology, Privacy and Enforcement Action

Presenters:

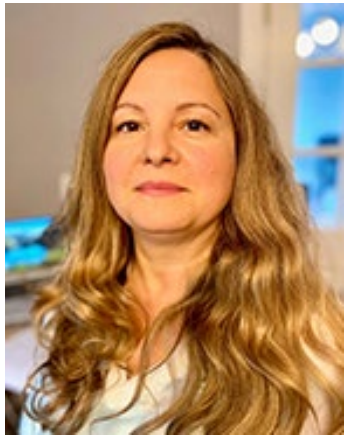
- Agustin Orozco, Partner, Crowell & Moring
- Jason Stiehl, Partner, Crowell & Moring
- Christiana State CIPP/E CIPP/US, Senior Counsel, Crowell & Moring
- Gage Javier, CIPP/US, Associate, Crowell & Moring

Crowell

Our Speakers

Agustin Orozco
Partner, Los Angeles
AOrozco@crowell.com

Jason Stiehl
Partner, Chicago
JStiehl@crowell.com



Christiana State
Senior Counsel, San Francisco
CState@crowell.com

Gage Javier
Associate, Washington, D.C.
GJavier@crowell.com

Disclaimer

The information provided during this webinar does not, and is not intended to, constitute and/or substitute for professional legal advice. All materials have been prepared for general information purposes only and is intended to help a person understand the area of law to help ask the right questions with the attorney of their choice. These information does not create an attorney-client relationship.

Agenda

- Biometrics Risk and Regulation
  - General Biometrics Overview
  - Current Biometrics Legislation
  - Enforcement and Litigation
    - Clearview AI
  - Best Practices for Biometric Compliance
- Crossroads of Privacy and Cybercrime

Biometrics Risk and Regulation

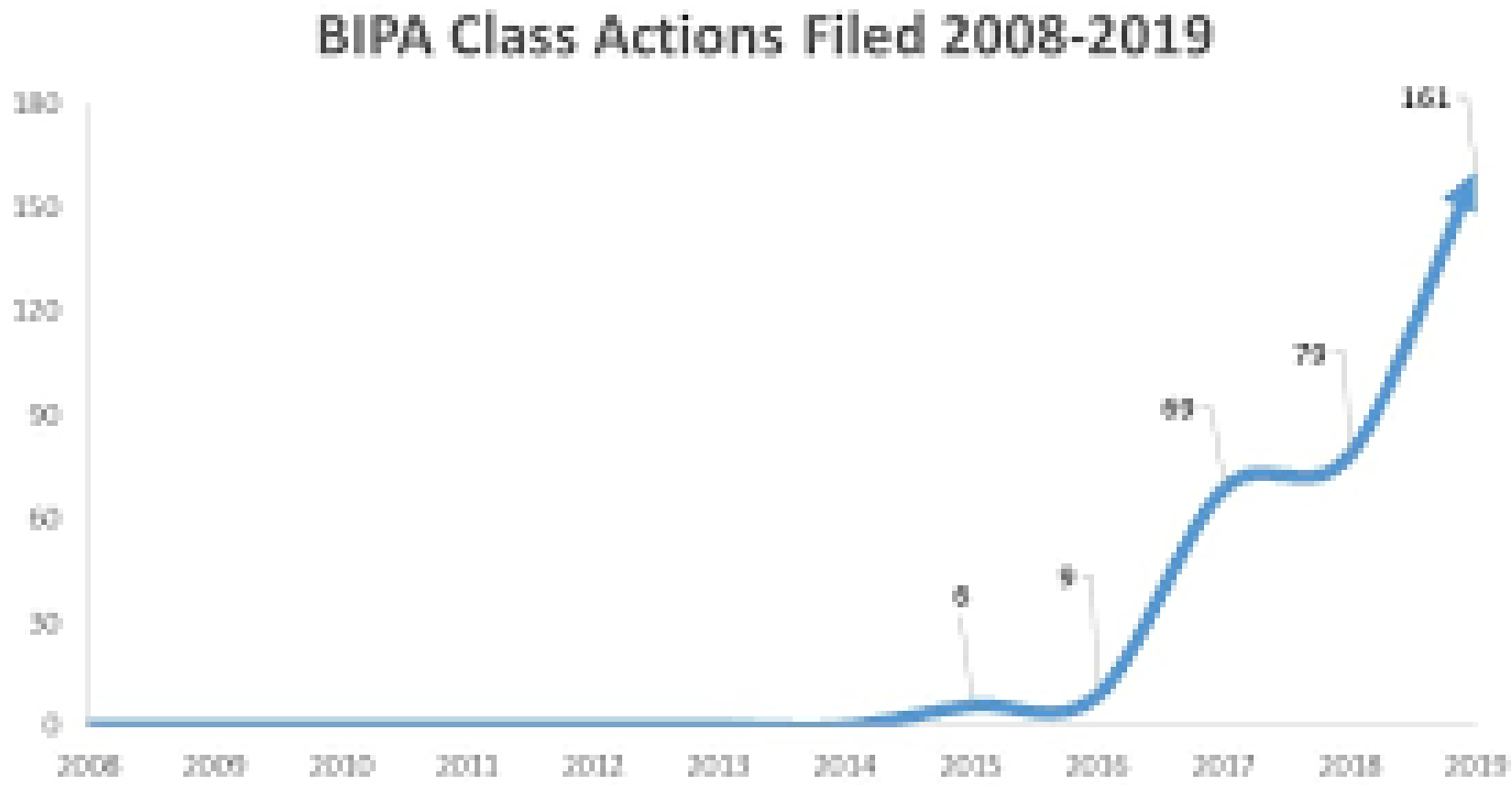
General Biometrics Overview

Biometrics Overview*

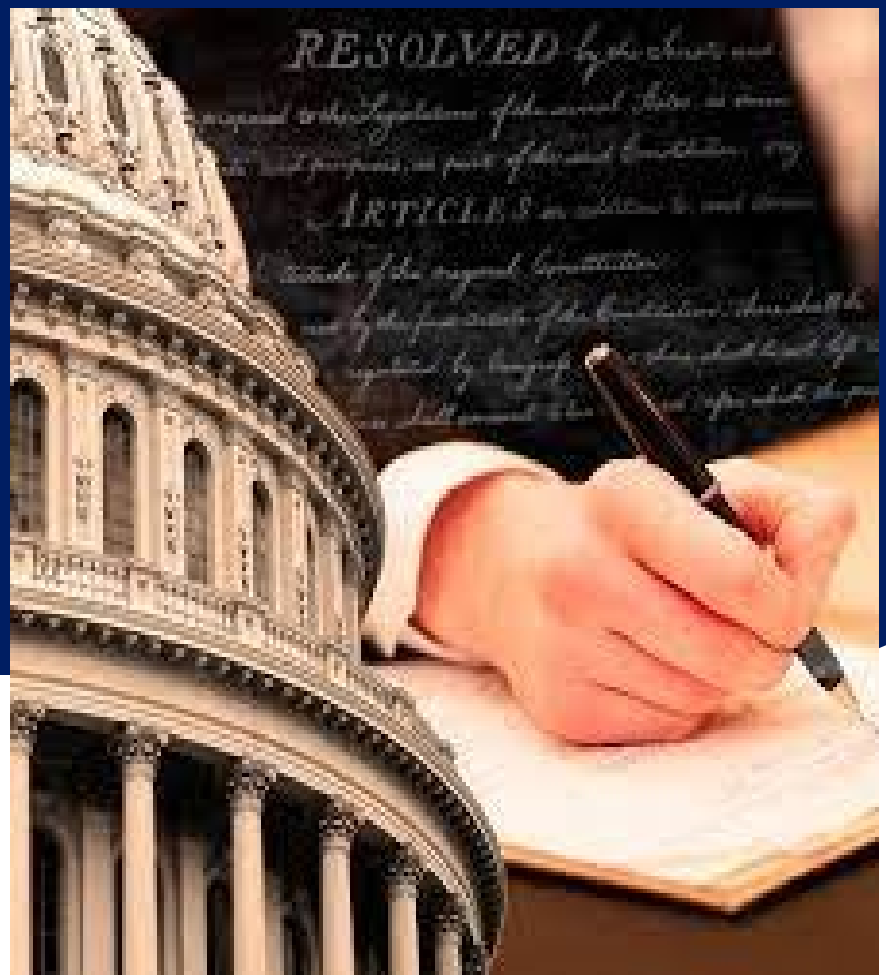
- "Biometrics":
  - Automated recognition of individuals based on their behavioral, biological and physical characteristics
  - Examples: fingerprints, facial pattern, voice pattern, retinal images

*Report by National Academy of Sciences

Prolific Rise Over a 2 Year Period – Over 500 Cases Filed Since 2015



Current Biometrics Legislation



Current Biometric-Specific Legislation – US

- No Federal law regulating the collection or use of biometric data
- Biometric legislation - Illinois, Texas, Washington
- Comprehensive privacy legislation
  - California Privacy Rights Act
  - Colorado Privacy Act
  - Utah Privacy Act
  - Connecticut Data Privacy Act
  - Virginia Consumer Data Protection Act

Current Biometric-Specific Legislation – US

- The Illinois Biometric Information Privacy Act is “the gold standard for biometric privacy protection nationwide”
- 2022 BIPA-like bills introduced in
  - California
  - Kentucky
  - Maine
  - Maryland
  - Massachusetts
  - Missouri
  - New York
    - Private right of action in all bills except Kentucky’s

US State Privacy Laws

- California Privacy Rights Act
  - Biometrics = sensitive data
  - Additional processing obligations imposed
  - No consent required prior to processing
- Colorado Privacy Act, Utah Privacy Act, Connecticut Data Privacy Act, Virginia Consumer Data Protection Act
  - Generally, biometric data = sensitive data if biometric data is processed for the purpose of uniquely identifying an individual
  - States impose slightly different obligations
  - Consent required prior to processing in CO, VA, and CT

Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14

- Illinois was the first state in the United States to pass a law that regulated the collection of biometric information
- Regulates how private organization can collect, use and store biometric data
- Private right of action
- Plaintiff does not have to demonstrate damages or harm from the collection of biometric data – the improper collection of biometric data is enough to enable individual to sue organization under BIPA – *Rosenbach v. Six Flags*

Illinois Biometric Information Privacy Act (BIPA), 740 ILCS 14

- Biometric identifier - retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry
  - specifically excludes photographs
- Biometric information - information "based on an individual's biometric identifier used to identify an individual."

BIPA requirements

- Prohibits companies from collecting, capturing, purchasing, trading, or otherwise obtaining individuals' biometric identifiers, unless they first:
    1. Inform person in writing of what data is being collected or stored;
    2. Inform person in writing of specific purpose and length of time the data will be collected, stored, and used; and
    3. Obtain person's written consent
- Prohibits any company from selling or otherwise profiting from consumers' biometric information
- Requires companies in possession of biometric identifiers to establish and make public a retention schedule and guidelines for permanently destroying biometric identifiers

BIPA's Private Right of Action

- Negligent violations award $1,000 in liquidated damages, or actual damages, whichever is greater
- Intentional or reckless violations award $5,000 in liquidated damages, or actual damages, whichever is greater
- Attorneys' fees and costs as well as injunctions may also be awarded
- Litigation has focused on fingerprint scans, handprint scans and facial scans

Comparison of BIPA v. other States with Biometric Legislation

- BIPA
  - Does not include a state or local government agency or court or private financial institution
  - Requires written notice
- Texas – Texas Business and Commerce Code § 503.001. Capture or Use Of Biometric Identifier Act
  - Does not apply to financial institutions retaining voiceprint data
  - Consent does not have to be written
  - No private right of action - enforced by state attorney general
- Washington – HB 1493
  - Biometric identifier does not expressly include a record of hand or face geometry and excludes photographs, video or audio recording
  - No written consent required
  - No private right of action

Enforcement and Litigation Over Biometrics

The Evolution and Expansion of Biometric Case Law

- In 2019, two cases opened the door to a flood to increased biometric litigation
- Both cases involved the scope of standing to bring a BIPA claim

  – *Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019)

  – *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (Jan. 25, 2019)

Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019)

- The plaintiffs alleged that Facebook subjected them to facial recognition technology without complying to BIPA
- **Biometric at Issue: "**Tag Suggestions" feature. **Scan of Face Geometry** to analyze whether the user's Facebook friends are in photos uploaded by that user.
- The Ninth Circuit held that the violations alleged by plaintiffs caused an injury to the plaintiffs:
  - development of a face template using face recognition technology without consent invades an individual's private affairs and concrete interests

Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Jan. 25, 2019)

- The lawsuit was brought on behalf of a minor whose thumbprint was recorded during a trip to a Six Flags amusement park.
- The **fingerprint scans** were used as a part of the amusement park's season pass program.
- No actual damages were claimed
- The Illinois Supreme Court held that a plaintiff does not need to allege "actual harm," in order to qualify as an "aggrieved" person under the Act.
- "A person is prejudiced or aggrieved, in the legal sense, when a legal right is invaded by the act complained of or his pecuniary interest is directly affected by the decree or judgment."

Clearview AI
The next wave of Biometric Cases

Clearview AI

Clearview AI devised groundbreaking facial recognition app:

- System uses database of 3 billion+ images scraped from Facebook, YouTube, LinkedIn & millions of other websites
  - Allegedly accessible only to law enforcement agencies with a subscription
    - data breach has revealed that this is not true and in reality, it is available to much larger list of clients
- Clearview AI announced its facial recognition software, Clearview 2.0, now features 20 billion publicly available facial images
- The images reportedly include photos of suspects, persons of interest and potential victims

ACLU v. Clearview AI Complaint – May 2020

ACLU sued Clearview AI in 2020 for violating Illinois residents' privacy rights under Illinois' BIPA, alleging Clearview is:

- Capturing billions of faceprints of individuals without notice, consent, or a retention schedule;
- Selling or otherwise profiting from consumers' biometric information; and
- Failing to provide individuals with publicly available policy identifying its retention schedule + guidelines for permanently destroying faceprints in its database

ACLU v. Clearview AI Settlement – March 2022

- Permanently banned from granting paid or free access to its face recognition database to private entities;
- Prohibited from selling access to its database to any entity in Illinois, including state and local police, for five years;
- Required to maintain an opt-out request form on its website;
- Clearview will end its practice of offering free trial accounts to individual police officers, without the knowledge or approval of their employers; and
- Must continue its current measures to attempt to filter out photographs that were taken in or uploaded from Illinois.

Consumer Action Pursued *In re: Clearview AI, Inc.*

- In early 2021, several cases were brought by consumers against Clearview AI, Inc. along lines similar to those brought by the ACLU and the cases were MDL'ed into the Northern District of Illinois
- However, in 2022, the plaintiffs filed a Second Amended Complaint, adding one of Clearview's alleged customers, Macy's, Inc., and bringing claims under several non-BIPA statutes, such as Commercial Misappropriation, Right of Publicity and Invasion of Privacy and New York Civil Rights Law

In re Clearview AI, Inc.

- The class also pursued the unique concept of alleging Macy's Inc. as the class representative for a Defendant class of any similarly situated entities
- Macy's sought dismissal of the claims, but the majority of the claims were allowed to proceed
- Most recently, the Plaintiffs attempted to amend the complaint to add several additional retailers that would purportedly be in the Defendant class– that motion was denied.

Takeaways from *Clearview*–An Expansive Judicial View

- The Court has allowed these claims to stand against Clearview and Macy's under the theory that even though BIPA does not protect photographs as biometric information, the information that an entity can derive from that photograph (like facial geometry) could qualify as biometric information
- The Court also let stand the common law claims under the theory that even using Clearview data to prevent loss or fraud could constitute "profiting" from the use of the data, as it avoids a loss

International Enforcement Actions Against Clearview AI

2021 – Canada – Clearview AI found to violate national laws and also ordering it to cease processing citizens' data

2021 – Sweden –local police authority fined €250,000 ($300,000+) for unlawful use of Clearview AI's technology, in breach of the country's Criminal Data Act.

2021 – UK – issued Clearview AI a provisional notice to stop further processing of UK citizens' data and to delete any data it already holds; $22M provisional fine

2021 – France – issued a formal notice to Clearview AI to stop "unlawful processing" and delete user data within 2 months

2021 – Australia – Clearview AI ordered to stop collecting facial images and biometric templates from individuals in Australia, and to destroy existing images and templates collected from Australia

2022 – Italy – Clearview AI issued €20 million penalty for breaches of EU law

Best Practices in an Evolving Biometric World

Understand Potential Risk Areas of Biometric Gathering/Use

- Most litigation, to date, has involved either fingerprints or facial geometry
- The fingerprint technology is often connected with either security or employment tracking
- For retailers, any use of cameras to create database of consumers or consumer reactions
- Also, online shopping has become a recent target, for example virtual “try on”

Try On Cases

- Over the past few months, several online retailers have been sued
  - L'Oreal (cosmetics)
  - Louis Vuitton (clothing)
  - Target (clothing)
  - Zenni Optical (glasses)
  - LVMH (eyewear)

Create a Compliant Policy and Consent Practice

- As noted, Illinois has one of the most rigorous standards, which requires:
  - (i) implement and publish a written biometric retention policy;
  - (ii) inform data subjects in writing of the specific purpose for collection, as well as the actual use and storage practices; and
  - (iii) obtain a written release from data subjects consenting to the disclosed collection, use, and storage practices

Create a Compliant Data Privacy Policy

- At a minimum, privacy policies should encompass the following issues:
  - (1) notice that biometric data is being collected and/or stored;
  - (2) the current and reasonably foreseeable purposes for which it utilizes biometric data;
  - (3) how biometric data will be used;
  - (4) a description of the protective measures used to safeguard biometric data; and
  - (5) the company's biometric data retention and destruction policies and practices.

Provide Written Notice of Collection and Use

- At a minimum, all written biometric data notices must contain language informing individuals that:
  - (1) biometric data is being collected and stored;
  - (2) the specific purpose for collecting and using biometric data;
  - (3) the length of time for which the data is being collected, stored and used;
  - (4) the company's schedule and procedure for permanently disposing of biometric data;
  - (5) any protective measures utilized to safeguard biometric data; and
  - (6) that biometric data may be shared with service providers or third parties.

Obtain Written Consent

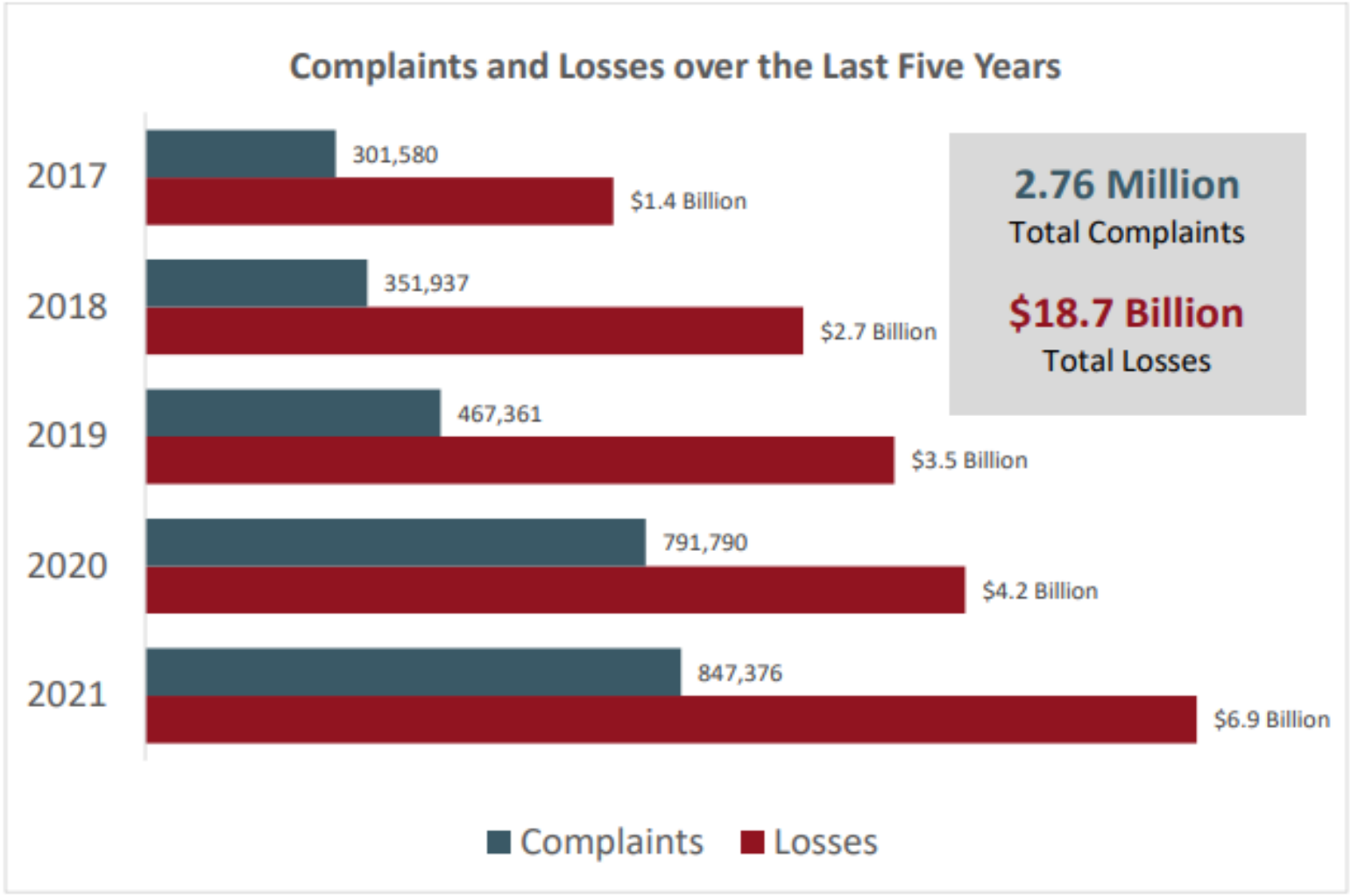
- In signing the written consent, the individual should:
  - acknowledge he/she has read the company's general biometric data policy as well as the more specific written notice that has been provided regarding its collection and use of biometric data.
  - Acknowledge consent to those policies and guidelines, as well as to the collection and use of his or her biometrics, including the company's ability to share their biometrics with any service providers or third-party vendors.

Review Agreements, including with Third-Parties and Vendors

- To the extent any vendor may be involved in collecting or providing biometric data, ensure language exists in contracts that requires compliance with all laws
- Consider adding indemnification language on these issues
- Consider updating contracts with arbitration/class waiver clauses as to these particular issues
- Review Terms of Use on Websites were data may be collected, shared or used

The Crossroads of Data Storage and Data Protection: Privacy and Cybercrime

Cybercrime Trends



Cybercrime Trends - 2021

- Ransomware
  - Ransomware incidents against 14 of the 16 U.S. critical infrastructure sectors
  - Victims: 3,729
  - Losses: $49.2 million
- Phishing/Vishing/Smishing/Pharming
  - Victims: 323,972
  - Losses: $44 million
- Business Email Compromise
  - Victims: 19,954
  - Losses: $2.3 billion
- California
  - Most victims: 67,095
  - Highest losses: $1.2 billion

What Regulators Want to Know

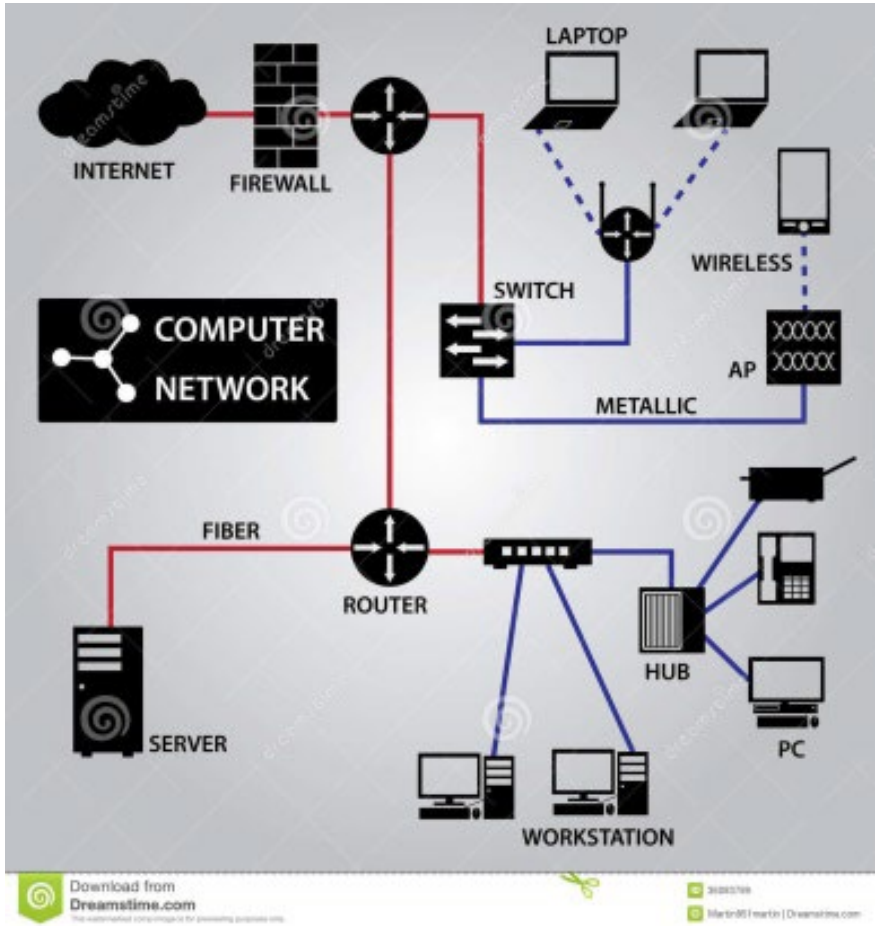
- What happened?
- Where it happened?
- Who was affected?
- Has it been contained?
- What is being done to protect the individuals affected?
- What is being done to stop this from happening in the future?

Cyber Incident – What?

- Common types of incidents:
  - Phishing
  - Denial of service (DDoS)
  - Vulnerability exploits
  - Credentials use
  - Ransomware
  - Data theft/access
  - Third party notification

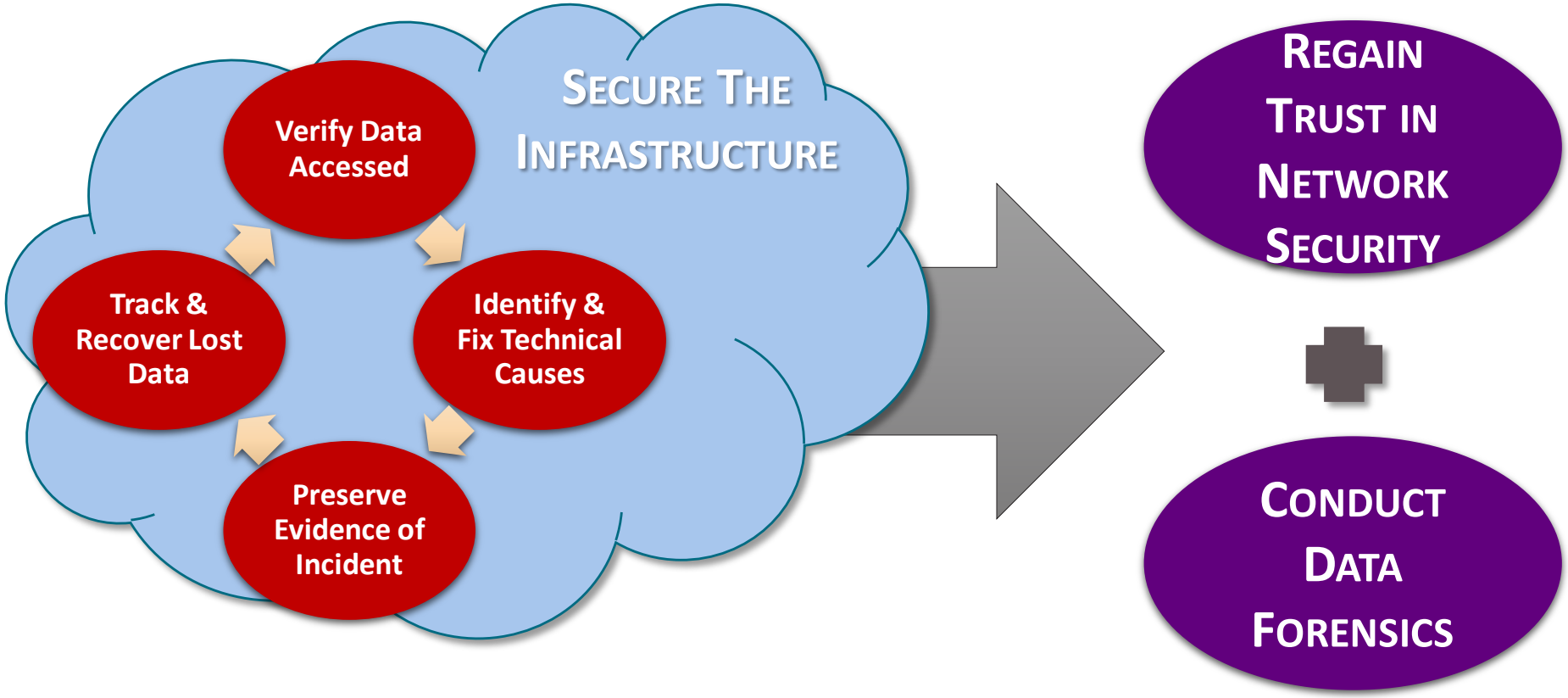
Cyber Incident – Where?

- Endpoint (laptop/mobile device)
- Server and Networks
- OT and IT
- Cloud vs. On-Premises
- Third party network (vendor/customer)
- DarkWeb



Cyber Incident – Initial Investigation

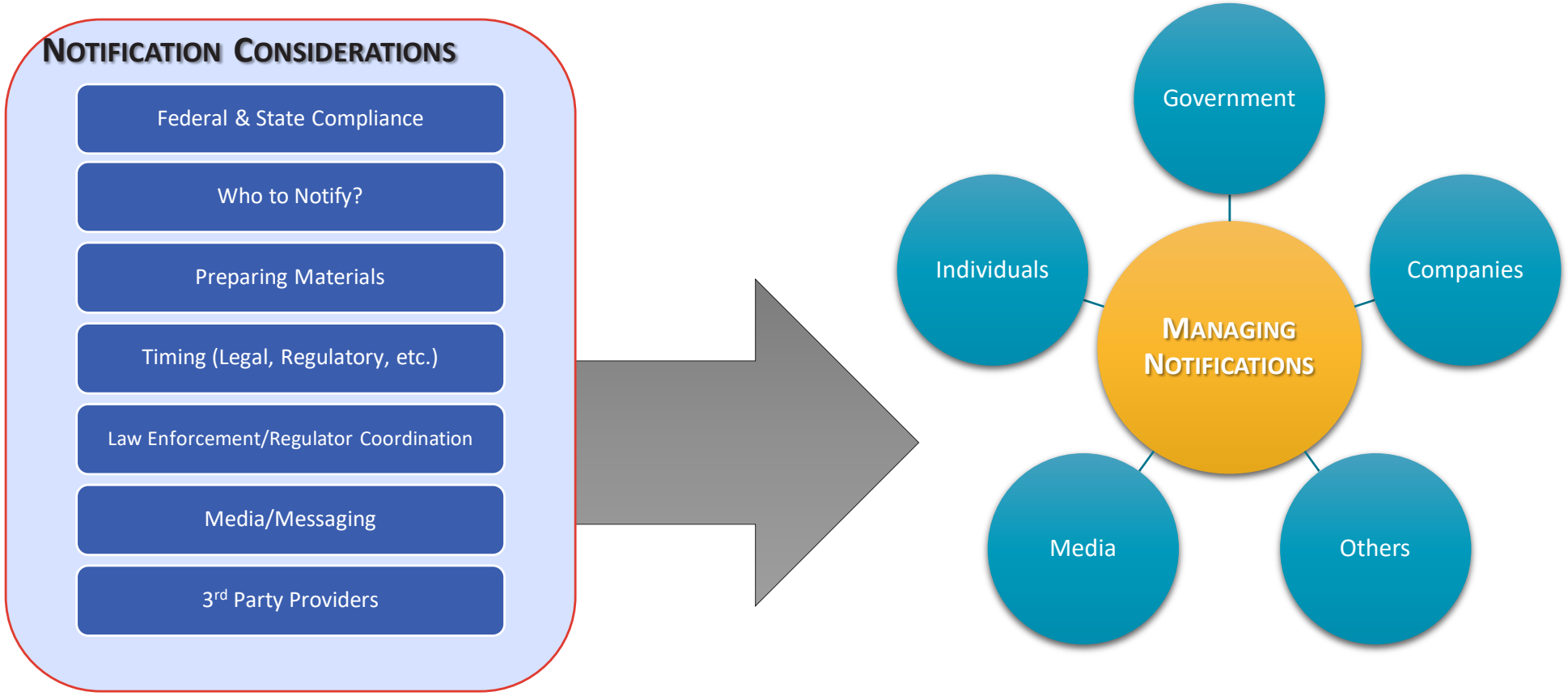
Remediation & Evidence Preservation



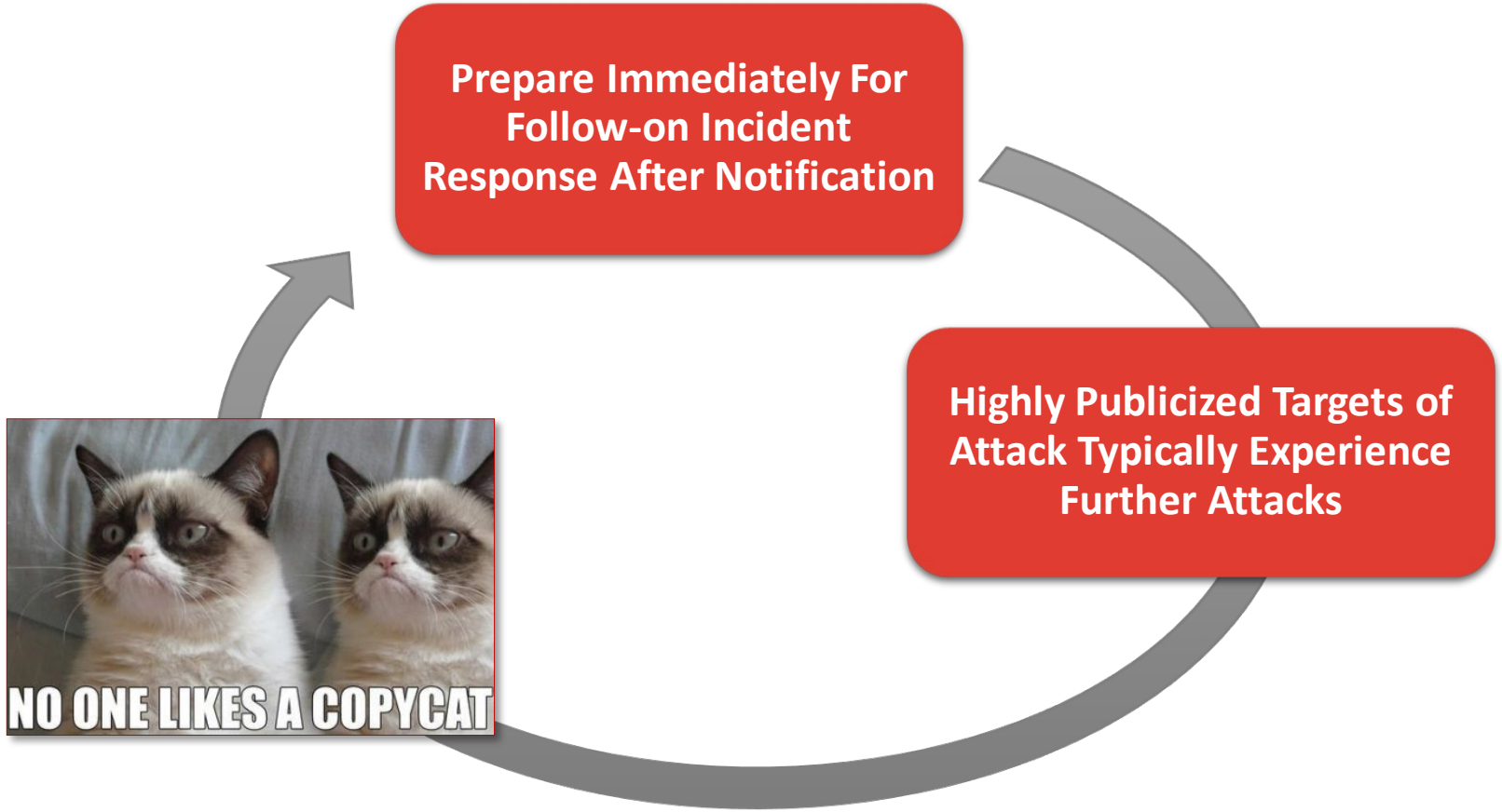
Legal Requirements

- **Legal / Regulatory Obligations**
  - Domestic
    - Federal Regulations: FTC Act, HIPAA, GLBA, FERPA, DFARS, CFAA, SEC, FERC/NERC, ITAR/EAR
    - State Regulations: 50+ data breach laws, CCPA, industry specific rules (CA IoT law, BIPA, VT data broker law)
  - International
    - Comprehensive Data Laws: GDPR (EU), LGPD (BR), PIPA (ROK), PDPA (SG), APPA (JP), PIPEDA (CA)
    - Data Localization Laws: China, Russia, Vietnam
    - Data Transfer Rules: GDPR Adequacy, EU/US Privacy Shield, APEC CBPR, ASEAN Cross-Border Mechanism
- **Contractual / Quasi-contractual / Supply Chain**
  - PCI DSS
  - DFARS
  - Contract-specific

External Notifications



Prepare for Round 2



Lessons Learned

Recap: Engaging Regulators

- Preparation begins well before a data breach
  - Identify and classify sensitive data
  - Implement controls to protect data and systems
  - Establish clear governance
  - Review and update policies & procedures
- If a data breach occurs, companies will want to demonstrate:
  - The company's education and awareness around data security issues
  - Efforts to identify and contain the breach
  - Compliance with legal obligations
  - Mitigation efforts

Recap: Key Takeaways for In-House Counsel

- Final comments from the panelists
- QUESTIONS?

Thank you!