No Longer “Nice to Have”:

Privacy and Security is the Law

Cyrus Malek, J.D.
Brett Hebert, J.D.

Cyrus Malek J.D.
Associate
Certification in Cybersecurity and Privacy Law

cmalek@briggs.com
https://www.linkedin.com/in/cyrus-malek-86631b4

Brett Hebert, J.D.
Associate

bhebert@briggs.com
https://www.linkedin.com/in/brett-hebert-b1255513/

“As a small business owner, I don’t need to think too much about cyber security because I’m probably too small to even be worth attacking.”

- Believing the myth
  - Despite making up 99% of businesses, SMBs represented only 13 percent of cybersecurity market spending in 2018.
  - On average, SMBs invest only $500/year in cyber security and use consumer-grade products.

-Juniper Research, The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Leading Vendors 2018-2023

“It’ll never happen to us . . . .”

Figure 2. Who are the victims?

- In 2018: 43% of all cyber attacks targeted SMBs (<250 employees)

-2019 Verizon Data Breach Investigations Report

Not under the radar in the crosshairs

- Two-thirds of SMBs have suffered a cyber attack in the past 12 months (that they knew about)
  - If you *didn't* experience a cyber attack in 2018, you're in the 33% minority
  - Majority of SMBs report that the attacks are more targeted, damaging, and sophisticated.
    - E.g., 4 out of 5 SMBs report malware has evaded their antivirus; 3 out of 4 SMBs say they don't have sufficient personnel to address IT security
  - Chances of being lucky two years in a row?
    - 2018 State of Cybersecurity in Small & Medium Size Businesses report (Ponemon/Keeper Security)

The cost can be closing up shop

- The average cost of an attack is nearly $3 million
  - Ransom costs, sustained system outages, disruption
    - 2018 State of Cybersecurity in Small & Medium Size Businesses report (Ponemon/Keeper Security)

- 40% of SMBs experience ≥8 hours of downtime because of a breach (2018 Cisco Cybersecurity Report: Special SMB Edition)
  - Accounts for more than half of the price tag for the average attack--$1.56 million
    - 2018 State of Cybersecurity in Small & Medium Size Businesses report (Ponemon/Keeper Security)

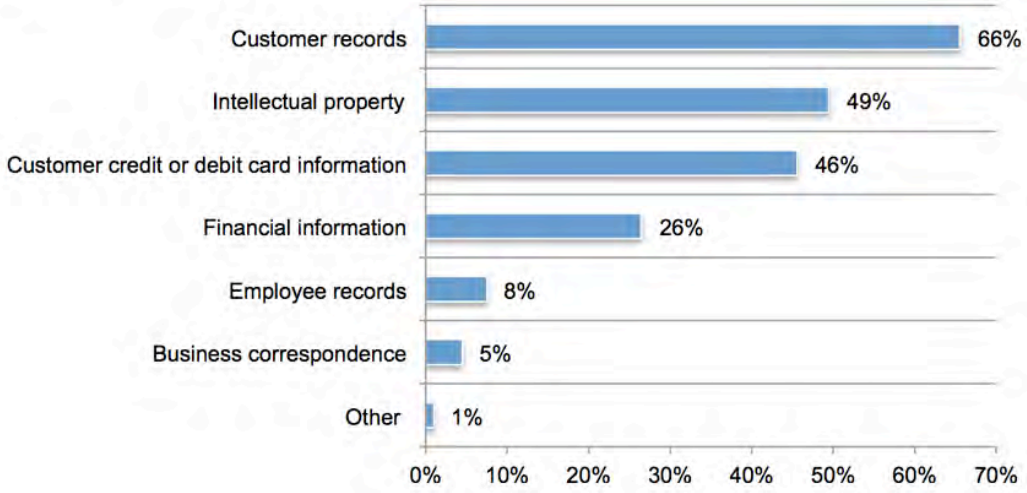
The law has caught up

- No longer is having a security program a good business investment—it's the law!

- Now, even outside the highly regulated industries (e.g., FinServs/Healthcare), privacy and security concerns have caused legislatures to act.

What do they want—what's valuable?

Figure 4. What types of information are you most concerned about protecting from cyber attackers?
Two choices permitted



Security of data is not just important to protect your business's assets, but it also has immense privacy compliance implications.

U.S. Privacy Framework – A Patchwork

- FTC Unfair/Deceptive Trade Practices
- Patchwork of Sector-specific Laws
- State data management/breach-notification laws of varying applicability (CCPA, BIPA, etc)

European Regime

- General Data Protection Regulation (GDPR)
  - Global regulation governing European privacy and security practices with additional obligations imposed by individual Member States.
  - Extraterritorial application

FTC Enforcement Authority

Authority to regulate data security and privacy matters derives from Section 5(a) of FTC Act of 1914, prohibiting “unfair or deceptive” trade practices.

- Unfair Practice
  - Causes or is likely to cause substantial injury to consumers; cannot be reasonably avoided by consumers; not outweighed by countervailing benefits to consumers or competition
- Deceptive Practice
  - Representation, omission, or practice misleads or is likely to mislead consumer; consumer’s interpretation of the foregoing is reasonable; the foregoing is material.

FTC Enforcement Authority

FTC v. Wyndham Worldwide Corp. (2015)

- Wyndham was breached three times between 2008 and 2010
- FTC filed enforcement action against Wyndham for failure to adequately safeguard its network ($1.6 million fraud loss)
- Wyndham argued FTC lacked authority to regulate data security standards—district court decides for FTC; 3d Cir. affirms. Wyndham incurred over $5 million in legal fees just in district court.

LabMD, Inc. v. FTC (2018)

- Despite data security program, LabMD file-sharing program exposed 9,300 patient health records
- FTC issued order obligating LabMD to implement security program that comported with FTC's standard of reasonableness
- 11th Cir. held order unenforceable because FTC's standard of "reasonableness" was too vague. What is reasonable and appropriate must accord with a well-established standard, e.g., statute, common law, or Constitution.

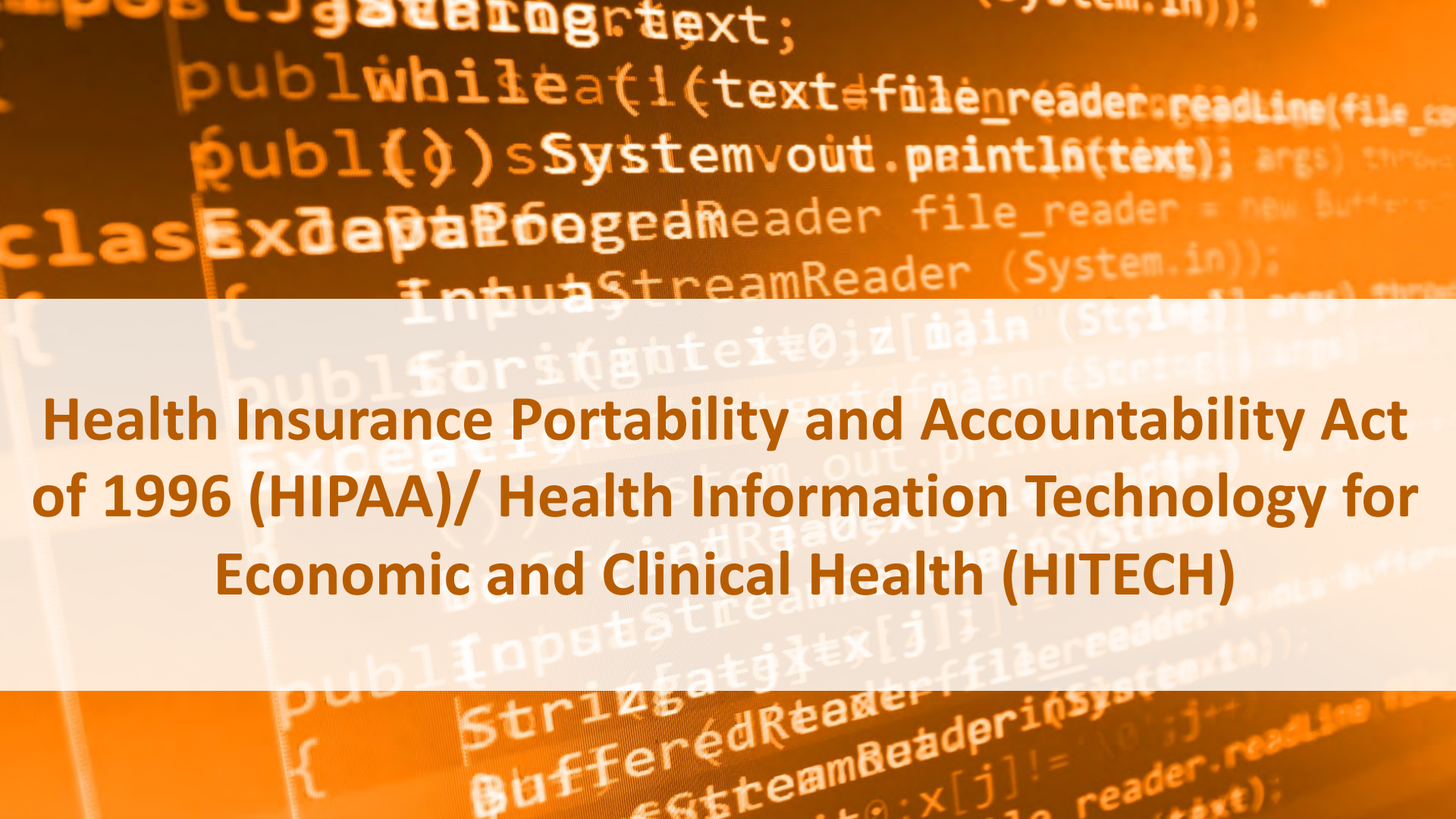
In re Snapchat (2014)

- Snapchat falsely represented in its privacy policy that “snaps” disappeared once viewed. In reality, the photos remained on the user’s phone and was viewable again with a simple file extension change

- FTC entered into settlement agreement and consent order with Snapchat, under which Snapchat was enjoined from making false claims in its privacy policies and would be subject to 20 years of privacy audits

TAKEAWAY:

Companies should avoid engaging in unfair or deceptive trade practices by having (and complying with) appropriate policies and procedures to ensure privacy and security.



Health Insurance Portability and Accountability Act of 1996 (HIPAA)/ Health Information Technology for Economic and Clinical Health (HITECH)

HIPAA and HITECH Scope

- The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information, and permits the disclosure of personal health information needed for patient care and other purposes.

- HITECH was created to facilitate the implementation of electronic medical records, and also expanded the scope of privacy and security protections available under HIPAA, including implementing breach requirements.

Gramm-Leach-Bliley Act (GLBA) Rule of Privacy of Consumer Financial Information

GLBA Privacy Rule Applicability

- GLBA seeks to protect consumer financial privacy by limiting when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties. Further, the law covers a broad range of financial institutions that engage in "financial activities."

- Financial institutions covered by the act must notify their customers about information-sharing practices and allow consumers the right to "opt-out" if they don't want their information shared with nonaffiliated third parties. The GLBA may cover an entity in two ways: (1) a financial institution must comply with the Privacy Rule; and (2) if an entity receives "nonpublic personal information" from a financial institution not affiliated with the entity, there may be a limit on how the entity uses information collected.

GLBA Requirements

- Generally, under GLBA, financial institutions are required to:
  - Abide by the Financial Privacy Rule: Provide Privacy Notices to their customers and consumers who are not customers under specific circumstances. GLBA provides requirements for what information must be included in the Notice, along with guidance on the appearance of the Notice.
  - Abide by the Safeguards Rule: Develop a written information security plan that describes their program to protect customer information. Financial institutions must also assign an employee or employees to coordinate safeguards; identify internal and external risks to the security, confidentiality, and integrity of customer information, and evaluate the effectiveness of current safeguards; design a safeguards program and detail the plans to monitor its efficacy; select and retain appropriate service providers and require them contractually to implement and maintain the safeguards; assess the security program periodically and adjust it to reflect changes in the business climate.

Children's Online Privacy Protection Act (COPPA)

COPPA Scope

- Protect personal information collected from children, defined as individuals under the age of 13.

- Applies to operators of commercial websites directed to children, online services (like mobile applications), and services that integrates outside services like plug-ins or advertising networks that collect, use, or disclose personal information of children—or those with actual knowledge that they are collecting PI derived rom children.

Personal Information Under COPPA

- Under COPPA, personal information includes:
  - First and last name;
  - A home or other physical address including street name and name of a city or town;
  - Online contact information;
  - A screen or user name that functions as online contact information;
  - A telephone number;
  - A social security number;
  - Persistent identifier that can be used to recognize a user over time and across different websites or online services;
  - A photograph, video, or audio file where the file contains the voice or image of a child;
  - Geolocation data sufficient to identify street name and name of a city or town; or
  - Information of a child or parent that the operator collects and combines with an identifier described above.

Compliance Requirements – COPPA

- To comply with COPPA, operators of a website or online service must:
  - Provide a clearly and understandably written privacy notice that does not contain unrelated, confusing, or contradictory materials;
  - With limited exceptions, obtain verifiable parental consent prior to collecting personal information of children;
  - Provide parents the ability to review information collected from their child, and to prevent further use or maintenance of their child's information;
  - Limit the personal information a child must provide to participate in a game, prize offering, or other activity to the information reasonably necessary to participate in the activity; and
  - Use reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

COPPA Enforcement

- COPPA violations are subject to civil, equitable relief, and remedies available under the FTC Act.
  - Operators who violate the rule may be liable for civil penalties of up to $41,484 per violation.

- Where the FTC lacks jurisdiction over an operator, applicable federal agencies with jurisdiction have COPPA enforcement authority.

- State attorneys general also have COPPA enforcement authority.

European General Data Protection Regulation (GDPR)

European General Data Protection Regulation (GDPR)

Came into Effect: May 25, 2018

Scope:

- Comprehensive legislation granting unprecedented data privacy rights to European Economic Area residents.
- Applies to organizations operating within the EU along with Non-EU organizations offering goods/services to European Union residents. Special rules apply for cross-border data transfers.

GDPR

Application:

Applies to any data *controller* (organization that processes personal data) or data *processor* (organization that processes personal data on behalf of controller) that *processes* the *personal data* of an EU resident (the *data subject*).

- *Processing* – any operation performed on personal data (*e.g.*, collection, storage, organization, transmission, destruction, etc.)
- *Personal data* – broadly defined—any information relating to an identified or identifiable natural person (*i.e.*, information that (directly or indirectly) identifies, describes, or can be used to reasonably link to a particular person)

GDPR

Personal Data: Any information relating to an identified or identifiable natural person

- *E.g.*, name, address, email, IP address, account name, SSN, cc and other financial information, driver's license, passport, protected classifications (race, nat'l origin), political beliefs, union membership, commercial information (purchasing habits), biometric information (fingerprints, facial recognition, sleep data), Internet activity, geolocation data, signature, education, thermal info, inferences that organizations can draw from other personal information to create consumer profiles.

GDPR

Underlying Principles

- Lawfulness, fairness, and transparency
- Accountability
- Minimization of data; Limited purpose
- Accuracy of data
- Limitations on data storage/retention
- Security, integrity, and confidentiality of data

GDPR

Default rule: **No processing of personal data** unless one of of 6 lawful bases applies.

6 lawful bases for processing of personal data

1. Consent
2. Necessary for performance of contract
3. Necessary to comply with legal obligation
4. Vital interests (matter of life and death)
5. Public interest (public authorities)
6. Legitimate interests (weighing of interests where rights of individual is outweighed by need for processing)

GDPR

6 lawful bases for processing of personal data

1. ***Consent***

   "freely given, specific, informed and unambiguous indication of data subject's wishes" manifested via "statement or clear affirmative action"

   - Only appropriate if other lawful bases do not apply
   - Cannot use consent as condition of using service
   - Pre-ticked boxes not permitted
   - Must be granular—cannot be a blanket consent
   - Cannot rely on another lawful basis if consent revoked

GDPR

6 lawful bases for processing of personal data

2. Necessary for performance of contract

- Narrowly tailored; personal data must actually be *necessary* to perform the contract
- *E.g.*, employment contract, sale of goods or services

GDPR

6 lawful bases for processing of personal data

3. Necessary to comply with legal obligation

"where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, **the processing should have a basis in Union or Member State law**"

- Narrow exception—only permitted if necessary to comply with EU or Member State's law.

GDPR

6 lawful bases for processing of personal data

4. Vital interests

- Processing must be necessary to protect “vital interests” of data subject
- Applies in life-or-death scenarios (*e.g.*, monitoring spread of infectious disease; protection of public in natural disaster)

GDPR

6 lawful bases for processing of personal data

5. Public interest

- Processing must be for performance of tasks carried out by a public authority or private organization acting in the public interest

- *E.g.*, privately operated public transit; energy; taxation; reporting crimes

GDPR

6 lawful bases for processing of personal data

6. Legitimate interests

- Most flexible/broad basis
- Balancing test—processing may be permissible if controller has legitimate interest in processing data if such interest is not overridden by the data subject's rights or freedoms.
- *E.g.*, detecting or preventing fraud, maintaining network or information security, *maybe* direct marketing (depends on circumstances)

GDPR

Data Subject Rights

- Right to be informed
- Right of access
- Right to rectification
- Right to be forgotten
- Right to data portability (if lawful basis is consent)
- Right to object (profiling, direct marketing)
- Right to not be subjected to automated decision-making that produces legal effects
- Others (breach communication, withdrawal of consent, etc.)

GDPR

Obligations

Governance, Risk, and Compliance (GRC)

- *Develop formal data security program to ensure that both policies, procedures, and practices comply with GDPR obligations; Records of Processing Activities (ROPA)*

Data protection must be both by design and default

- *Data mapping*
- *Both Technical and organizational safeguards*
- *Data Protection Officer (DPO), Data Protection Impact Assessment (DPIA)*

GDPR

Penalties

Punishment for non-compliance can be substantial

- Penalties for non-compliance can be as much as €20 million or 4% of global revenue, whichever *greater*.
- For some infractions, €10 million or 2% of previous year's global revenue, whichever is greater (e.g. failure to carry out DPIA if required)
- Penalty can (with or without fine) also be reprimand, ban on data processing (either temporary or permanent), or suspension of data flows to recipient in non-EU country.

California Consumer Privacy Act of 2018 (CCPA)

California Consumer Privacy Act of 2018

Enacted: June 28, 2018 Effective: January 1, 2020

- CA is the first state to enact such a comprehensive consumer privacy law

Scope:

- CCPA provides new rights and protections for consumers regarding most data that businesses may collect about them.

- Establishes significant new set of privacy and data security requirements for entities conducting businesses in California.

California Consumer Privacy Act of 2018

Application:

- Any company doing business in California that:

  1. has at least $25 million in total revenue;

  2. holds the personal information (broadly defined—information that is "reasonably capable of being associated with" a particular consumer or household) of at least 50,000 consumers (California domicile);
  or

  3. derives ≥50% of annual revenue from selling consumers' personal information

- Also covers entity that controls/is controlled by a covered business or shares common branding with covered business

California Consumer Privacy Act of 2018

Application Exceptions:

1. Collecting/selling consumer's personal information if every aspect of commercial conduct takes place wholly outside CA;

2. Completing one-time, single transactions that does not retain collected personal information;

3. Selling personal information as part of merger or acquisition transaction;

4. Complying with other laws, defending legal claim, or cooperating with law enforcement

California Consumer Privacy Act of 2018

Enforcement:

California Attorney General empowered with regulatory and enforcement authority

- May promulgate rules (e.g. further defining personal information, providing content for consumer notices, procedures for consumers to opt out of data collection or make requests for information about them)
- Businesses can seek advice from CAG re compliance. 30-day cure period to address identified violations.

California Consumer Privacy Act of 2018

Enforcement:

Private right of action for unauthorized access, theft, or disclosure of personal information

- Statutory damages of $100-$750 per consumer per incident
- Consumers must provide businesses 30 days to cure any notified violations before initiating the action
- Consumers that file action must notify CAG within 30 days so that CAG may decide to
  - 1. Take over the case;
  - 2. Allow action to proceed; or
  - 3. Stop the action from proceeding.

California Consumer Privacy Act of 2018

Consumers' Rights:

- Right to knowledge
  - What info about them is collected, sold, and/or disclosed to third parties (including to whom the data are disclosed)
- Right to notice (before or at time data are collected)
  - What personal information is collected and intended use/purpose
- Right to access
  - Upon submitting verifiable request, entitled to receive portable electronic version of their personal information

California Consumer Privacy Act of 2018

Consumers' Rights:

- Right to be forgotten
  - Right to request that business and its service providers delete personal information (subject to certain exceptions)
- Right to opt out
  - Must be given right to opt out of having their personal information sold

California Consumer Privacy Act of 2018

Consumers' Rights:

- Right to opt-in (children)
  - For children (< 16 yrs), must have affirmative opt-in right for sale of personal information (parental consent if < 13 years)
- Not be discriminated against for asserting data rights
  - Businesses can impose payments or price/service differences if those differences are directly related to the value provided by consumer's data (but cannot result in unjust, unreasonable, coercive, or usurious incentive practices)

California Consumer Privacy Act of 2018

Business Obligations:

- Privacy Notice on website
  - Updated annually
  - Describes consumers' rights, and at least 2 methods for submitting data requests (including toll-free number)
  - Lists personal information categories collected in past 12 months
  - Separate list of personal information categories sold or disclosed for business purposes in past 12 months (or statement that no consumer information has been sold or disclosed)

California Consumer Privacy Act of 2018

Business Obligations:

- Opt-Out
  - "Do Not Sell My Personal Information" link on webpage (must be clear/conspicuous and accessible from homepage), allowing consumers to exercise opt-out rights
- Implement procedures to respond to consumer requests
  - Must be able to follow procedures so that consumers' verifiable requests for their data can be responded to within 45 days

California Consumer Privacy Act of 2018

Business Obligations:

- Train employees
  - Must ensure those responsible for handling consumer inquiries about privacy practices and compliance requirements

- No resale of consumer information without notice/opt-out
  - Cannot resell consumer information received from third parties unless consumer has received notice of resale and an opt-out opportunity

California Consumer Privacy Act of 2018

CCPA Last-Minute Amendment Exceptions:

1. De-identified/aggregated consumer info exempted from personal information;

2. Collection of business owner/employee/job applicant/contractor (B2B) data exempted, but only for one year;

3. Business that only operates online and has direct relationship with consumer whose data is collected must only provide an email address for submission of CCPA requests;

California Consumer Privacy Act of 2018

Business Obligations:

Statutory Requirement to *"implement and maintain reasonable security procedures and practices appropriate to the nature of the information*."

California Consumer Privacy Act of 2018

Data Security Program:

- Guidance from requirements imposed by statutes regulating highly sensitive information, e.g., healthcare (HIPAA/HITECH) & financial-services (GLBA)

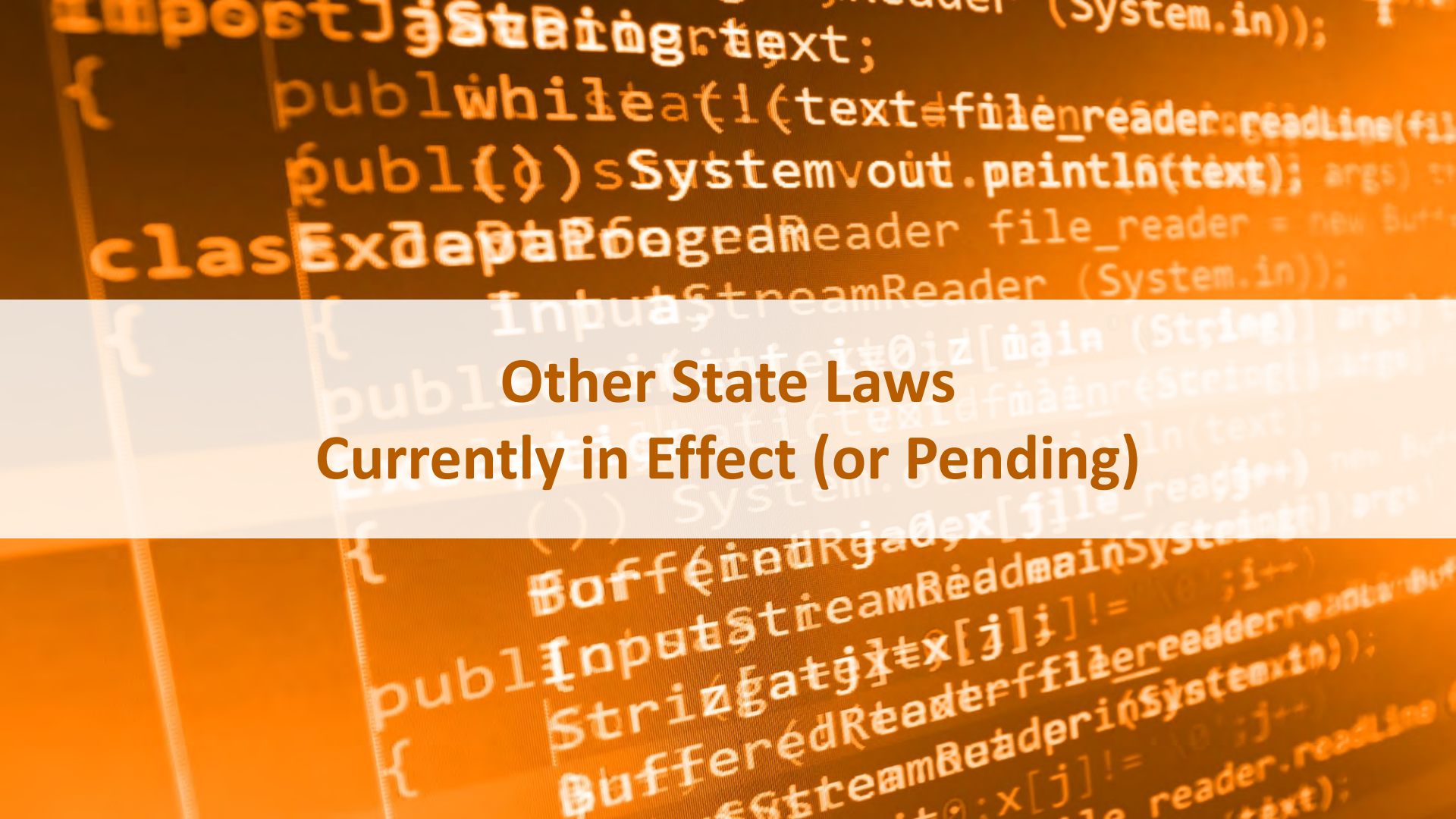
- Assess types of data collected, assess risk, and develop formal data security program that is audited and updated annually.

TAKEAWAY:

Legislation like the GDPR and CCPA created the need for companies to look at privacy and security differently.

Instead of organizations looking at these issues as a one-time compliance project approach, we see a shift to an enterprise-wide privacy program approach.

E.g., Automated tools (data-subject request tool), Privacy by Design, Data Protection Impact Assessments/Risk Assessments, Data Mapping, Privacy Notices and Terms of Use, Incident Response Plans, Red/Blue team testing, Data Classification, Retention, and Destruction policies, Acceptable Use policies, Employee Training, Technical and Physical Security Solutions.



Other State Laws
Currently in Effect (or Pending)

Current State Laws

Massachusetts Data Privacy Rule (2010)

- Applies to companies that process, use, maintain or have access to personal information (name plus SSN, DL, or financial account number) of a Massachusetts resident.

- Requires that companies implement a data security program meeting specific standards, and to impose restrictions on vendors by contract, if those vendors will have access to personal information.

Current State Laws

Delaware statute regarding data disposal (Del. Code tit. 6 § § 5001C to 5004C) (2015)

- Applies to corporations incorporated in Delaware. No limiting language suggesting it applies only to businesses located in Delaware.

- Requires destruction of consumers' personally identifying information (name in combination with SSN, DL, insurance policy number, etc.) to be done in a secure manner, i.e., by shredding hard copies or destroying electronic records.

Current State Laws

20 States mandate a form of “reasonable” data security requirement (4 pending in 2019)

4 States Mandate Specific Data Security Standards

- Connecticut (Conn. Gen. Stat. § 4e-70)
- Nevada (Nev. Rev. Stat. § § 603A.210, 603A.215(2))
- Oregon (Or. Rev. Stat § 646A.622)
- South Carolina (S.C. Code § 38-99-10 to -100.)

Current State Laws

Nevada Data Encryption Statute (2015):

- Applies to any corporation doing business in the state. Statute's applicability is not limited to data of Nevada residents.
- Data collectors that do any business in Nevada must use encryption for:

  (1) all electronic transmissions of personal information, except faxes, outside the secure system of the data collector; and

  (2) any movement of a data storage device (broadly defined) containing personal information outside the confines of the workplace of the data collector or its data storage contractor.

Current State Laws

Illinois Biometric Information Privacy Act (2008)

- Applies to all companies “doing business in Illinois”
- Consent/secure storage/destruction requirements
- Provides potential claimants a private right of action, and may do so without pleading damages (“aggrieved” claimants may file suit)
- TX and WA have similar statutes in place – MA is enacting in 2020

Current State Laws

Data Breach Notification Obligations

- Minn. Stat. § 325E.61 (2006)
  - Person or business that conducts business in MN must notify Minnesota resident of breach of security of system when unencrypted personal information is (or is reasonably believed to have been) acquired by an unauthorized party.
  - Personal information = name + SSN, DL, account number/cc info, etc.
  - Disclosure must be made as expediently as possible and without undue delay by way of written, electronic, or substitute notice (if conditions of such notice are met)
  - If personal information of >500 persons disclosed, must notify all consumer reporting agencies.

Current State Laws

Data Breach Notification Obligations

- Report breach to state attorney general (*e.g.*, IL, MT, OR, NE, ND)
- Specific content required in breach notification (*e.g.*, CA, IL, RI, TN, WA)
- Free credit monitoring for one year following breach (CT)
- Notification required even if the information was encrypted (TN)
- Exemption from notification of compromised encrypted data if NIST cybersecurity framework followed (WA)

Pending Legislation

CCPA language found in “copy cat” legislation throughout state legislatures

- HI, MD, MA, MS, NM, NV, NY, ND, RI
  - All in various stages of legislation process

WA draft bill models GDPR (failed initial floor vote in 2019)

Pending Federal Legislation(?)

House of Representatives

- Rep. Jan Schakowsky (D-Ill.) discussed introducing a floor bill providing comprehensive data protection requirements as recently as late September 2019
- We are still waiting…

Senate

- Bills introduced pertaining to consumer *health* data and jailing social media CEOs
- Still no comprehensive consumer data privacy bill

Key Takeaways

1) **Data Privacy & Cyber Security Laws Are Not New; They Are Maturing.**

2) **Data Privacy and Cyber Security Compliance Will Become (if they are not already) a Consumer Expectation.**

3) **Planning Solely for Immediate Compliance = Planning for Obsolescence.**

Thank you for your time.