The Quiet Revolution, Part III: What You Need to Know About U.S. State Privacy Laws

Scott M. Giordano, Esq., FIP, CISSP
V.P. and Sr. Counsel, Privacy and Compliance
Scott.Giordano@Spirion.com

April 23, 2020

A few housekeeping matters…

- If at any time you cannot hear the audio or see the slides, please check your computer's sound and display settings—if that doesn't work, please use the chat function to alert us. If we have multiple people alerting about the same problem then we know it's on our end.
- The slides and recording will be emailed out to you after we're finished
- We expect this webinar to take an hour with time for questions throughout. Use the chat function and we'll find natural places to pause and take questions. We'll leave time at the end for any questions during the webinars and ones you submitted in advance.

Presenter

Scott Giordano, Esq., FIP, CISSP, VP and Sr. Counsel, Privacy and Compliance

- Specializing in multinational/cross-border aspects of data protection
- Former ISO 17024 Certifications Advisory Board Member, International Association of Privacy Professionals
- Created and taught the first law school course on electronic evidence and -discovery
- Member of the California, the District of Columbia, and Washington state bar associations

If you leave with nothing else…

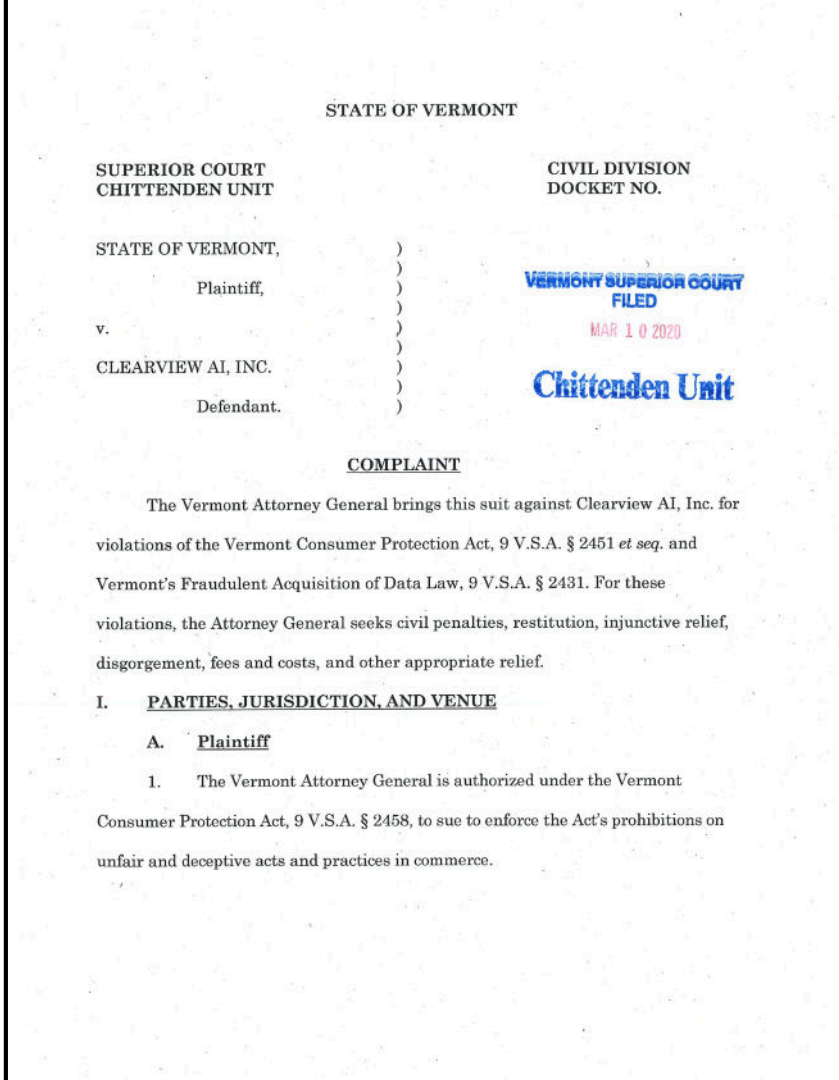
- A fair number of data protection laws are already in effect or will be soon
- CCPA enforcement date is still July 1, 2020; CCPA lawsuits continue to roll in
- CCPA Regulations are on their 2nd revision
- CCPA 2.0 status seems to be on track in spite of the lockdown
- Updates to "breach laws" usually include more, sometimes much more
- Beware of non-financial penalties
- Don't expect any help from the federal government
- Look for bonus material in this deck

SPIRION

Data Protection Laws Already in Effect

California A.B. 1202, Data Broker Registration Statute, Jan. 1, 2020

- California's law is not the first…Vermont's was
- Many companies that were relatively unknown came to the surface
- Vermont AG filed a lawsuit against Clearview AI in March of this year, citing violations of that law and unfair trade practices
- More to come



STATE OF VERMONT

SUPERIOR COURT
CHITTENDEN UNIT

CIVIL DIVISION
DOCKET NO.

STATE OF VERMONT,
Plaintiff,
v.
CLEARVIEW AI, INC.
Defendant.

VERMONT SUPERIOR COURT
FILED
MAR 10 2020
Chittenden Unit

COMPLAINT

The Vermont Attorney General brings this suit against Clearview AI, Inc. for violations of the Vermont Consumer Protection Act, 9 V.S.A. § 2451 *et seq.* and Vermont's Fraudulent Acquisition of Data Law, 9 V.S.A. § 2431. For these violations, the Attorney General seeks civil penalties, restitution, injunctive relief, disgorgement, fees and costs, and other appropriate relief.

I. **PARTIES, JURISDICTION, AND VENUE**

A. **Plaintiff**

1. The Vermont Attorney General is authorized under the Vermont Consumer Protection Act, 9 V.S.A. § 2458, to sue to enforce the Act's prohibitions on unfair and deceptive acts and practices in commerce.

California A.B. 1202 Data Broker Registration Statute, Jan. 1, 2020

"Data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom **the business does not have a direct relationship**. "Data broker" does not include any of the following:

1. A consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act
2. A financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act
3. An entity to the extent that it is covered by the Insurance Information and Privacy Protection Act

California A.B. 1202 Data Broker Registration Statute, Jan. 1, 2020

Must provide the following:

A. The name of the data broker and its primary physical, email, and internet website addresses.
B. Any additional information or explanation the data broker chooses to provide concerning its data collection practices.

$360 fee for registration; $100/day penalty for failing to register

- Here's the problem: "direct relationship" is not defined – could include many businesses.
- Registry is here: https://oag.ca.gov/data-brokers
- Stay tuned for more.

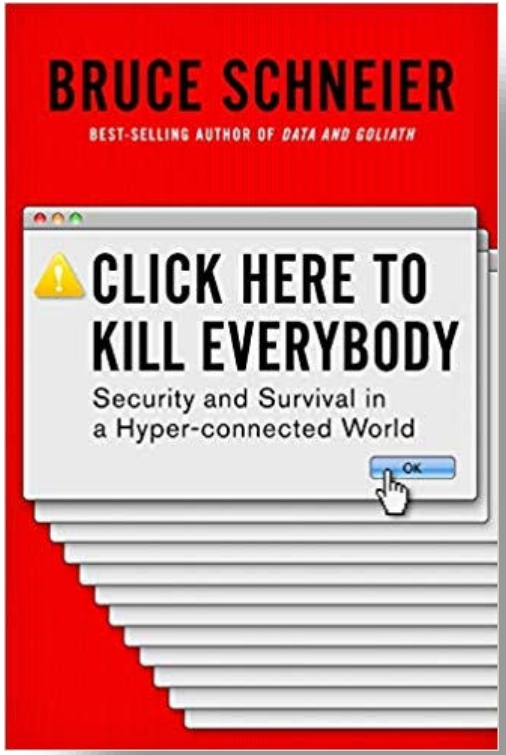
SPIRION

Oregon H.B. 2395, January 1, 2020

- The second “Internet of Things” law in the U.S.; California’s passed before this one
- Summary. Require manufacturers to equip an Internet- **“connected device with reasonable security features”** that protect against “unauthorized access, destruction, use, modification or disclosure that are appropriate for the nature and function of the connected device.” E.g.,
  A. A preprogrammed password that is unique for each connected device; or
  B. A requirement that a user generate a new means of authentication before gaining access to the connected device for the first time
- Applies to: Manufacturers of Internet-connected devices (i.e., uses an I.P. or equivalent address).
- Protects: Oregon residents.

Oregon H.B. 2395, January 1, 2020

- Penalties: The law has no private right of action. Instead, the Attorney General may punish as an unlawful trade practice.
- Second Internet of Things law of any kind; California's version is found at Civ. Code § 1798.91.04 and also effective Jan. 1st
- Applies to any organization selling devices in Oregon.
- IoT bills in the NY and VA legislatures
- Ring LLC lawsuits filed late in 2019
- See Bruce Schneier's book "*Click Here to Kill Everybody*."



SPIRION

Washington state, H.B. 1071, March 1, 2020

H.B. 1071 expands the definition of “personal information” to include:
First name or initial and last name in combination with one or more of the following:

- Social Security number; **[now just the last four digits per S. B. 6187]**
- Driver’s license number or Washington identification card number;
- Account number or credit or debit card number, in combination with any required security code, or password that would permit access to their account
- Full date of birth;
- **Private keys for electronic signature;**
- Student, military, or passport identification numbers;
- Health insurance policy or identification numbers;
- Medical information, including medical history, mental or physical condition, diagnoses, or treatment; and
- Biometric data.

Washington state, H.B. 1071, March 1, 2020

Also:

- Any of the above elements, **not in combination with first name or initial and last name**, if the affected data was not rendered unusable via encryption or redaction and would enable a person to commit identity theft against the consumer.
- **Username and email address in combination with a password** or security questions and answers that would permit access to an online account.
  - Very common; see https://haveibeenpwned.com/

Washington state, H.B. 1071, March 1, 2020

Breach Notification

- Notice of a breach must be provided "in the **most expedient time possible, without unreasonable delay**," and no later than 30 calendar days after the breach was discovered.
- Also must be provided to the Attorney General's Office when the breach affects more than 500 Washingtonians. Send to: SecurityBreach@atg.wa.gov

Washington state, H.B. 1071, March 1, 2020

Expands the information required:

- A list of the types of personal information that were or are reasonably believed to have been breached;
- If known, the time frame of exposure, including the date of the breach and the date of the discovery of the breach;
- A summary of steps taken to contain the breach; and
- A copy of the breach notification sent to affected residents.

- Also requires that breached entities provide updates to the Attorney General's Office for any of the above information that was unknown at the time notice was due.
- AG may enforce this under unfair or deceptive trade acts laws, or private right of action by affected parties

New York S-5575 B, the SHIELD Act, March 21, 2020

An expanded definition of “private information”:

- Social security number;
- Driver's license number or non-driver identification card number;
- Account number, credit or debit card number, in combination with any required security code, access code, password or other information;
- Account number, credit or debit card number;
- Biometric information; or
- **A user name or e-mail address in combination with a password or security question and answer**

New York S-5575 B, the SHIELD Act, March 21, 2020

- Applicability to **any person or entity** that **accesses** the private information of a New York resident – **acquiring the information is not necessary, nor is conducting business in the state**;
- Breach notification "**in the most expedient time possible and without unreasonable delay**" to affected parties and several New York law enforcement agencies; and
- A mandate to develop, implement, and maintain **reasonable safeguards** to protect the security, confidentiality, and integrity of private information including secure disposal of data.

New York S-5575 B, the SHIELD Act, March 21, 2020

For violations of the breach notification mandate, the New York Attorney General may bring actions for civil penalties of

(1) up to actual damages incurred by residents for violations that are based on negligence; and

(2) up to $5,000 per violation (with a $250,000 limit) for violations that are “knowing” or “reckless” (either is a higher standard).

For violations of the “reasonable safeguards” requirement, the Attorney General may seek damages of up to $5,000 per violation.

SPIRION

Upcoming Data Protection Laws

Vermont S.B.110, July 1, 2020

- The law is an update to the existing security and breach notification law
- “Personally identifiable information” means a consumer’s first name or first initial and last name in combination with any one or more of the following digital data elements [that are not encrypted/redacted]:
  - A social security number;
  - Government-issued identification **(just about anything)**;
  - A financial account number or credit or debit card number plus an access code or number;
  - Unique biometric data;
  - Genetic information; and
  - Health records or a health insurance policy number.

Vermont S.B.110, July 1, 2020

- Businesses (“data collectors”) must provide notice of a security breach in the **most expedient time possible and without unreasonable delay**, but not later than 45 days after the discovery or notification
- Must also notify the Attorney General or the Department of Financial Regulation
- If the business is a data processor, must notify their customer immediately

Vermont S.B.110, July 1, 2020

Notice shall include a description of each of the following, if known to the data collector:

A. the incident in general terms;
B. the type of personally identifiable information that was subject to the security breach;
C. the general acts of the data collector to protect the personally identifiable information from further security breach;
D. a telephone number, toll-free if available, that the consumer may call for further information and assistance;
E. advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and
F. the approximate date of the security breach.

Vermont S.B.110, July 1, 2020

Creates a new type of regulated business: “Operators” of websites directed at pre-K – 12 students (essentially, educational technology providers). Can not:

- Engage in targeted advertising to the students
- Create student profiles
- Sell, barter, or rent student’s information
- Disclose to a third party (except under certain conditions)

Also must

- Implement and maintain reasonable security procedures and practices;
- Delete student’s data on request
- Provide the school with information about the operator’s collection, use, and disclosure of covered information

SPIRION

The Insurance Data Security Law Implementations

The Insurance Data Security Law (MDL-668)

Before there was an Insurance Data Security Law there was…NYCRR Part 500:

- The principle mandates of the regulation are the (1) establishment of a cybersecurity program and (2) appointment of a Chief Information Security Officer (CISO) to oversee that program. The program must be capable of:
  1. Identifying internal and external cyber risks;
  2. Using “defensive infrastructure” and policies and procedures in concert to protect the entity’s information systems and nonpublic information stored on them;
  3. Detecting cybersecurity events (i.e., attempts to gain access to, disrupt, or misuse information systems or information);
  4. Responding to identified or detected cybersecurity events to mitigate any negative effects;
  5. Recovering from cybersecurity events and restore normal operations and services; and
  6. Fulfilling all regulatory reporting obligations.

The Insurance Data Security Law (MDL-668)

…Then came the IDSL. Summary:

- Each Licensee shall develop, implement, and maintain a **comprehensive written Information Security Program based [WISP]** on the Licensee's Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System.
  - Largely tracks NYCRR Part 500 but doesn't use the word "CISO"
  - Includes Third-Party Service Providers
- Applies to: Insurers domiciled in a given state
- Protects: Residents of a given state.

The Insurance Data Security Law (MDL-668)

Actions required:

- Risk assessment
- Appoint a person or persons to lead the program (they don't use the word CISO, however)
- Board of Directors oversight
- Screening of Third Party Service Providers and imposition of WISP
- Incident response plan
- Investigations of cybersecurity incidents

The Insurance Data Security Law (MDL-668)

"Nonpublic Information" means information that is not Publicly Available Information and is:

a) Intellectual property such as trade secrets;
b) Consumer identifiers:
    a. (a) Social Security number,
    b. (b) Driver's license number or non-driver identification card number,
    c. (c) Account number, credit or debit card number,
    d. (d) Any security code, access code or password that would permit access to a Consumer's financial account, or
    e. (e) Biometric records;
c) Any information or data, except age or gender…from a health care provider or a Consumer and that relates to
    a. (a) The past, present or future physical, mental or behavioral health or condition of any Consumer or a member of the Consumer's family,
    b. (b) The provision of health care to any Consumer, or
    c. (c) Payment for the provision of health care to any Consumer.

The Insurance Data Security Law (MDL-668)

Which states?

- Already the law in SC, OH, MS
- AL.: May 1, 2020
- VA: July 1, 2020
- DE: July 31, 2020
- CT: October 1, 2020
- MI: January 1, 2021
- NH: January 1, 2021

SPIRION

On the Horizon

D.C., B23-0215, Security Breach Protection Amendment Act of 2019

- Signed into law on March 26th; 30-day Congressional review period ends late April

Updated definition of personal information:

1. An individual's first name, first initial and last name, or any other personal identifier, which, on its own or in combination with any of the following data elements, can be used to identify a person or the person's information:
   - Social security number, gov't-issued ID **(just about anything)**;
   - Account number plus a password;
   - Medical information;
   - Genetic/DNA information;
   - Health insurance information;
   - Biometric data; or
   - Any combination of the above.
2. A user name or e-mail address in combination with a password

D.C., B23-0215, Security Breach Protection Amendment Act of 2019

- **Updated breach notification.**
  - Breach report must contain details of the breach
  - Notification must also be made to the Attorney General of D.C.
  - If SSN/TIN are compromised, must provide ID theft protection for 24 months
- **Updated information security**. "A person or entity that owns, licenses, maintains, handles or otherwise possesses personal information of an individual residing in the District shall **implement and maintain reasonable security safeguards…that are appropriate to the nature of the personal information[.]"**
  - Note that the law does not define what's "reasonable"
  - Third parties must function under an agreement requires them to **"implement and maintain reasonable security procedures"** that are **"appropriate to the nature of the personal information[.]"**

New Jersey Disclosure and Accountability Transparency Act (NJ DaTA)

- Effectively, a condensed GDPR clone.
- Requires an opt-in for processing of personal information
- Requires a legal basis for processing
- Copies Art. 5, which relates to principles of using personal data, almost verbatim
- Copies much from Arts. 6 (legal basis), 12 (transparency) and 13 (disclosure of personal data), as well as other Articles
- Prohibit the processing of special personal information without consent
- Establish the Office of Data Protection and Responsible Use – basically, a supervisory authority

Summary and Conclusions

- Get started now with creation or update of your data inventory
- NIST Privacy Framework perhaps the best place to start
- ISO/IEC 27701 Privacy Information Management System (PIMS) has some potential
- Security standards, guidelines, and frameworks such as ISO/IEC 27001/2, NIST 800-171, and CSC Top 20 can address security mandates that cite “reasonable security procedures”
- Business partners (vendors, third parties, licensees, etc.) require vigorous policing
- Don’t expect any help from the gov’t

Sample Data Inventory

Process Descriptions							
Nerve Center' Country (dropdown)	Business teams (dropdown)	Business process activity (e.g. recruiting, payroll calculations, payment processing, etc.)	Description, why activity is done (possible highlight if privacy notice or consent required)	Employees, Customers, Candidates, Suppliers (dropdown)	Types of Personal Data include name, address, date of birth, marital status	personal data type (Standard or Sensitive) - sensitive data type include standard personal data fields	Legal basis for processing
Country	Business Unit	Process flow name	Purpose of the processing	Category of Perso	List of data items	Data Type	Legal Basis
United States	IT	MDM Expert	Mobile Device Management (MDM). Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. MDM is a core component of enterprise mobility management (EMM) which also includes mobile application management, identity and access management and enterprise file sync and share. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise while simultaneously protecting the corporate network.	Employee	IMSI, IMEI, Device ID, ESN	Standard	Legitimate Interest
United States	IT	DLP Master	Data loss prevention; specifically, file centric actions - e.g., copying from a Word document to Yahoo mail or a USB drive. Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.	Employee	Equipment identifier (laptop, desktop ID or processor serial number), UserID, AD credentials	Standard	Legitimate Interest

Reproduced with permission from Robert Half Legal Consulting

SPIRION

SPIRION

Your Questions, Answered

Your Questions, Answered

- Is a customer count by each state based on the period from the end of the quarter with a lookback count of the previous 12 months an appropriate reference? I keep a reference book of each state's reporting requirements including the number of records potentially involved in a breach, and this number varies from state to state for reporting purposes... For example, I might have only 42 records for North Dakota consumers and this does not reach the threshold for reporting to the AG; and 100sK records of California consumers that have completed at least one order in the past year...
- What advice do you have for companies trying to train employees to navigate this complicated terrain?
- what is the recommended level of data encryption?
- How does CCPA define and treat DataControllers vs DataProcessors
- If CCPA was modeled after GDPR, and if one is already GDPR-compliant, what are the other areas that are needed to ensure compliance in CCPA?

Your Questions, Answered

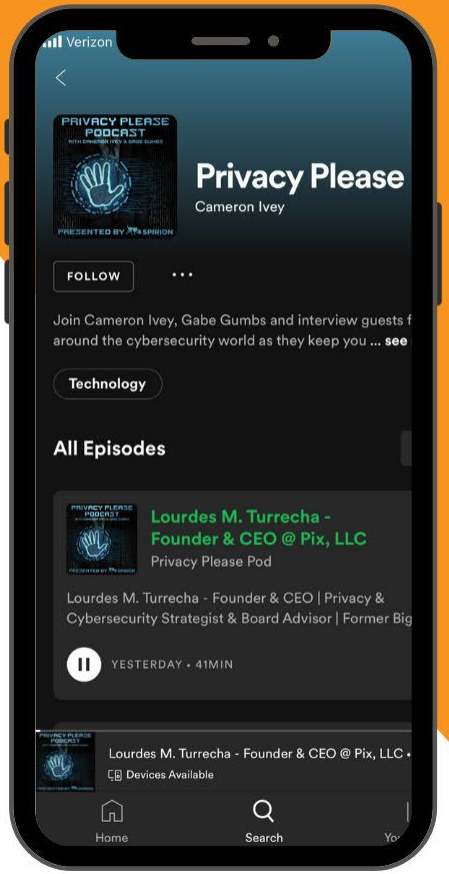
- Are there any conflict requirements between state privacy laws and federal privacy law? How to determine the appropriate protection level for privacy related information? An example, if a list of names and addresses (PII) was made public (e.g. real estate record, license registration record, etc.) by state or local government. Should federal agencies treat such info also as public data or provide the same protection as they treated other PII collected by federal agencies (even though such info was not originally collected by federal agencies)?
- What about New Jersey?
- Please include how students and families are impacted. Are social media posts picturing adults illegal without consent?
- Please discuss interstate responsibilities.
- Are the states all confirming to the requirement to demonstrate ‘reasonable security’? And is there any trend towards a more prescriptive approach for this?
- How do these state privacy laws impact healthcare organizations operating under HIPAA privacy rules?
- Who designed the model that states are implementing?
- “How to define if the legislation is applicable for out-of-USA IT service providers with USA-based customers (organizations only, not person)”

SPIRION

Visit Our Privacy Please Podcast

Available on Spotify, Google Podcasts, iTunes or anywhere you get your podcasts.

LISTEN NOW

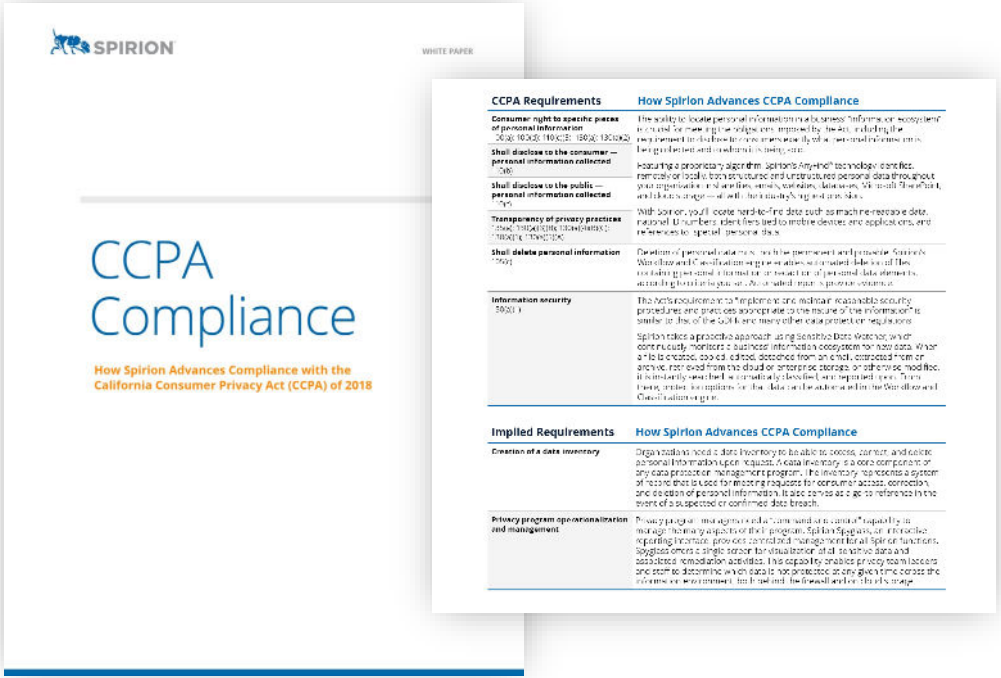


Thank you!

Scott M. Giordano, Esq.
Scott.Giordano@Spirion.com

Learn more about how Spirion can help accelerate CCPA compliance through automated accurate data discovery, classification and monitoring.

Visit www.spirion.com



Compliance Deadlines

State	Bill Number and/or Name	Compliance Mandate Area(s)	Enforcement Begins
California	S.B. 327, A.B. 1906	Internet of Things (IoT) security	January 1, 2020
California	A.B. 375, S.B. 1125	Comprehensive personal data privacy; security	January 1, 2020
Oregon	H.B. 2395	Internet of Things (IoT) security	January 1, 2020
Illinois	S.B. 1624	Breach notification	January 1, 2020
Oregon	S.B. 684	Personal information; breach notification for vendors	January 1, 2020
Texas	H.B. 4390	Breach notification	January 1, 2020

Compliance Deadlines

State	Bill Number and/or Name	Compliance Mandate Area(s)	Enforcement Begins
Washington state	H.B. 1071	Breach notification	March 1, 2020
New York	S. 5575-B, the SHIELD Act	Identify and protect “private information”; breach notification; secure disposal	March 21, 2020
Alabama	S.B. 54, the Insurance Data Security Law	Comprehensive written information security program	May 1, 2020
Washington state	S.B. 6187	Updated definition of personal data	June 11, 2020

Compliance Deadlines

State	Bill Number and/or Name	Compliance Mandate Area(s)	Enforcement Begins
Maine	L.D. 946	Sales of personal information	July 1, 2020
Vermont	S.B.110, An Act Relating to Data Privacy and Consumer Protection	Breach notification; definition of personal data; student data	July 1, 2020
Virginia	H.B. 1334, the Insurance Data Security Act	Comprehensive written information security program	July 1, 2020
Delaware	H.B. 174, the Insurance Data Security Act	Comprehensive written information security program	July 31, 2020
Connecticut	H.B. 7424, the Insurance Data Security Law	Comprehensive written information security program	October 1, 2020
Michigan	H.B. 6491, the Insurance	Comprehensive written	January 1, 2021