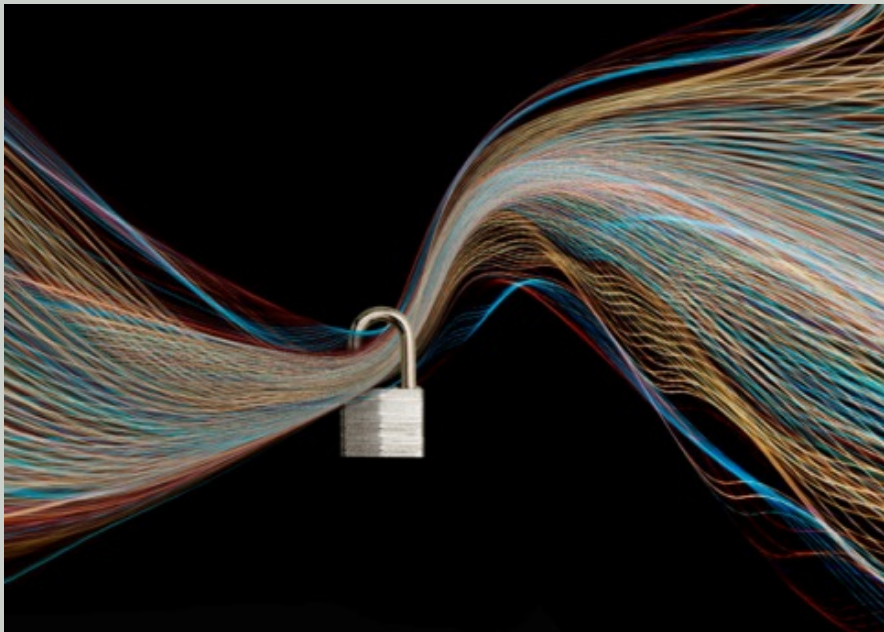


Outside Our Borders: How New Laws Will Affect Businesses



Edward J. McAndrew
mcandrewe@ballardspahr.com

David M. Stauss
staussd@ballardspahr.com

Malia K. Rogers
rogersmk@ballardspahr.com

Speakers



Edward J. McAndrew, Partner

Edward J. McAndrew is a counselor, investigator, and trial lawyer who helps clients navigate life in the digital world. He is the Co-Practice Leader of the firm's Privacy and Data Security Group and the Leader of its national Cyber Incident Response Team. Prior to joining Ballard Spahr, Ed served for nearly a decade as a federal cybercrime prosecutor in the U.S. Attorney's Offices for the Eastern District of Virginia and for the District of Delaware.



David M. Stauss, Partner

David is head of the privacy and cybersecurity practices in Ballard Spahr's Denver and Boulder offices. He advises clients on all aspects of privacy and data security, including data breach responses, data security litigation, and information security compliance. He is accredited by the International Association of Privacy Professionals as a Certified Information Privacy Professional/United States (CIPP/US) and as a Certified Information Privacy Technologist (CIPT).



Malia K. Rogers, Associate

Malia is an associate at Ballard Spahr LLP and a member of its privacy and data security practice group. She has experience in the creation and development of privacy notices and website terms and conditions and regularly writes on privacy-related issues. She is a member of the International Association of Privacy Professionals.

Roadmap

- **California**
- **Update on State Data Breach Notification Laws**
- **Update on State Information Security Laws**
- **GDPR Update**

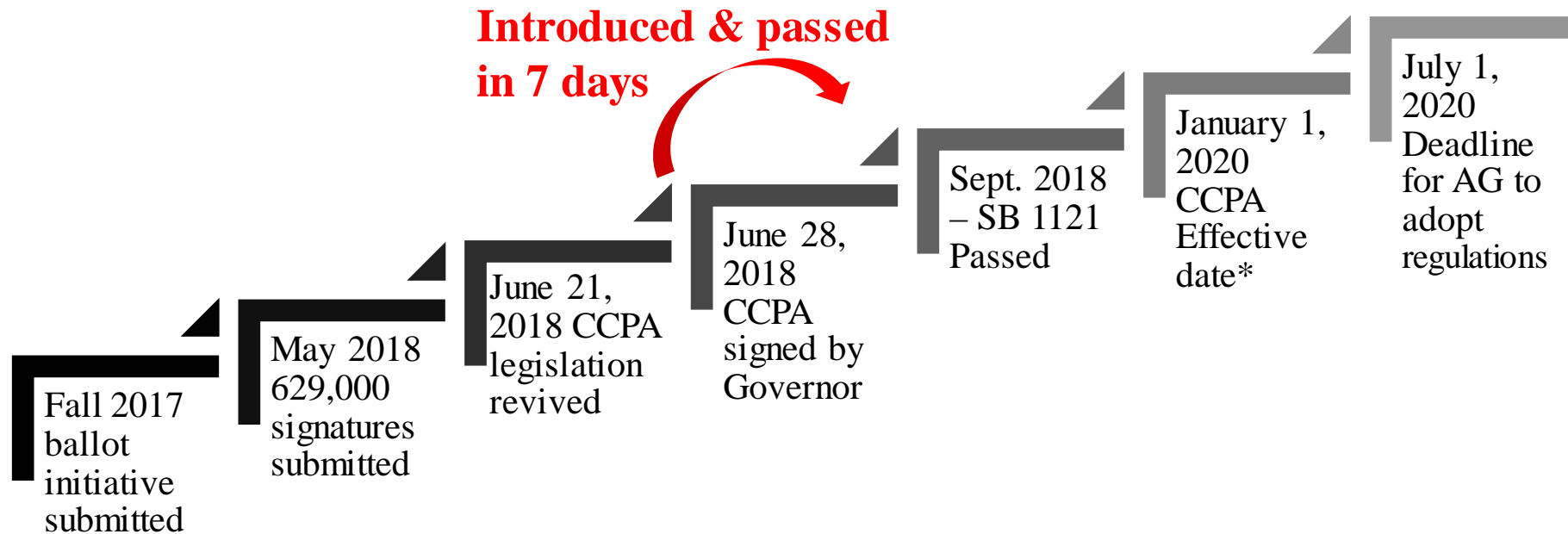
California Consumer Privacy Act of 2018

Biggest Takeaway

It's a Mess

(It's already been amended!)

Background on Enactment



*AG cannot bring enforcement action until six months after publication of final regulations or July 1, 2020, whichever is sooner

Which Entities are Subject to the CCPA?

For-profit businesses doing business in California



[one or more of the following]

Annual gross
revenues
> \$25 million

Personal
information of
 $\geq 50,000$
consumers,
households, or
devices

Sale of Personal
information
accounts for
 $\geq 50\%$ of annual
revenues

Exclusions

- **Financial Institutions (amended in SB1121):**
 - “This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act . . . and implementing regulations, or the California Financial Information Privacy Act, and implementing regulations. **This subdivision shall not apply to Section 1798.150.**”
- **HIPAA PHI Carve Out (amended in SB1121):**
 - Act does not apply to covered entities or PHI collected by covered entity or BA governed by HIPAA Privacy, Security and Breach Rules.
- **Consumer Reporting Agency Carve Out:**
 - Act “shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report . . . and use of that information is limited by the federal Fair Credit Reporting Act”

Who Holds the Rights Afforded Under the CCPA?

- California residents
 - ❑ Every individual in California for other than a temporary or transitory purpose, and
 - ❑ Every individual who is domiciled in California who is outside the State for a temporary or transitory purpose
- Do you know who is a California resident?

Explanation of the Consumer Rights Provided in the CCPA

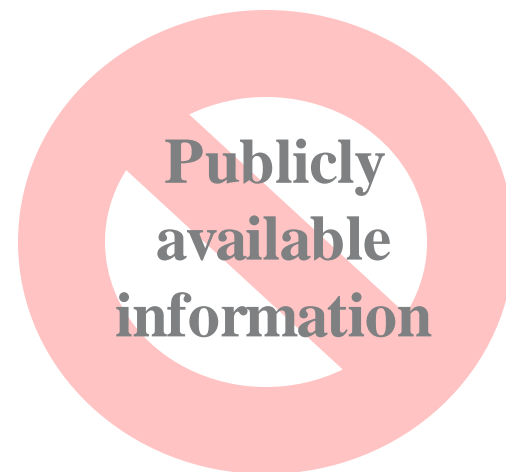
Consumer Rights Provided in the CCPA

- Right to know
 - ❑ Entities must make up-front disclosures of what personal information they are collecting and with whom they are sharing it
 - ❑ Entities must respond to verified requests to provide certain information to consumers
- Right to be forgotten
- Right to opt out of selling of information to third parties
- Right to equal service
- Right to data portability (kind of)

What Information is Protected?

Personal Information means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household

- Biometric data
- Geolocation data
- Browse and search history
- Purchase history or tendencies
- Interactions with ads and apps
- Education information
- Employment-related information
- **Inferences drawn from such information**



Consumer Right to Request Information from . . .

. . . Businesses that “collect” personal information

- Categories of PI collected about that consumer
- Categories of sources from which the PI was collected
- Business purpose for collecting or selling the PI
- Categories of third parties with whom the PI was shared
- **Specific pieces of PI collected about that consumer**

. . . Businesses that “sell” personal information

- Categories of PI collected about that consumer
- Categories of PI sold and the categories of third parties to whom it was sold
- Categories of PI disclosed about that consumer

Consumer Right to Request to Be Forgotten

- Business must delete PI from its records and direct any service providers to do the same

Nine Exceptions:

- Necessary to provide good or service requested by consumer
- Scientific, historical, or statistical research
- Enable solely internal uses “reasonably aligned” with the expectations of the consumer
- Use internally in a lawful manner compatible with the context in which the consumer provided the PI

Consumer Right to Opt Out

- Right, at any time, to direct a business not to sell that consumer's PI to any third parties
- Express authorization required to sell thereafter

Enhanced Rights for Minors

- Under 16 years of age – “right to opt in”
- Willful disregard of a consumer's age deemed actual knowledge of consumer's age

Consumer Right to Equal Service

Businesses are prohibited from:

- Denying goods or services
- Charging or providing a different price, rate, level, or quality of goods or services, or suggesting same

UNLESS the difference is “*reasonably related*” to the value provided to the consumer by the consumer’s data

- Financial Incentive Programs are permitted if that difference is “*directly related*”

Online Privacy Policy Requirements

Online Privacy Policy Requirements

➤ Describe Rights

- Must describe consumer rights in online privacy notice and in any California-specific privacy rights description and identify methods for submitting verified requests

➤ List Categories of Personal Information

- Must list categories of PI that business has (in preceding 12 months) collected and/or sold about consumers and PI disclosed about consumers for a business purpose

➤ Duty to Update

- Must update information at least once every 12 months

➤ Opt Out

- Businesses that sell PI and are required to comply with opt-out provision must have a “**Do Not Sell My Personal Information**” link on homepage and in privacy notice

Enforcement Provisions

Attorney General Enforcement

- California AG's office is vested with exclusive authority to enforce *privacy-related* rights
- 30 day cure period
- Civil penalty of \$2,500 “for each violation” or \$7,500 for “each intentional violation”
 - ❑ What does “each” mean?

But . . .

Attorney General Enforcement

XAVIER BECERRA
Attorney General


State of California
DEPARTMENT OF JUSTICE

1300 I STREET, SUITE 125
P.O. BOX 94255
SACRAMENTO, CA 94244-2550

August 22, 2018

The Honorable Ed Chau
California State Assembly
State Capitol

The Honorable Robert M. Hertzberg
California State Senate



August 22, 2018
Page 2

Const. art. II, § 10). We can and should address this constitutional infirmity by simply replacing the CCPA's current penalty provision with a conventional stand-alone enforcement provision that does not purport to modify the UCL. My team has offered corrective language for this purpose.

Third, the CCPA contains an unnecessary requirement that private plaintiffs give notice to the Attorney General before filing suit (see Civil Code section 1798.150, subdivision (b)(2)). This provision has no purpose as the courts not the Attorney General decide the merits of private lawsuits. Additionally, the filing of a private action does not limit the Attorney General's law enforcement authority. This provision in the CCPA

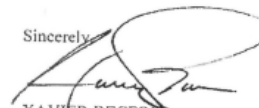
Finally, the CCPA does not include a private right of action that would allow consumers to seek legal remedies for themselves to protect their privacy. Instead, the Act includes a provision that gives consumers a limited right to sue if they become a victim of a data breach. The lack of a private right of action, which would provide a critical adjunct to governmental enforcement, will substantially increase the AGO's need for new enforcement resources. I urge you to provide consumers with a private right of action under the CCPA.

requirements. I urge you to swiftly correct this.

Second, the CCPA's civil penalty provisions are likely unconstitutional. These provisions (see Civil Code section 1798.155 and 1798.160) purport to amend and modify the Unfair Competition Law's (UCL) civil penalty provision (see Business and Professions Code section 17206) as applied to CCPA violations. The UCL's civil penalty provisions were enacted by the voters through Proposition 64 in 2004 and cannot be amended through legislation (see Cal.

unworkable obligations and serious operational challenges. If we fail to address these issues with the CCPA as outlined above, it is the people of California who stand to lose.

Sincerely,



XAVIER BECERRA
Attorney General

Data Breach Private Right of Action

➤ Language

- ❑ “Any consumer whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action”

➤ Damages

- ❑ Can recover “not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) **per consumer per incident** or actual damages, whichever is greater”

Internet of Things Law

Background

- First state to pass law specifically directed at IoT devices
- Law originally titled the “Internet of Things Botnet Prevention Act”
- Waiting for Governor’s signature
- January 1, 2020 effective date
- No private right of action

Requirement

- “Manufacturers” of “connected devices” must equip them with “a reasonable security feature or features” that are:
 - ❑ appropriate to the nature and function of the device;
 - ❑ appropriate to the information the device may collect, contain, or transmit; and
 - ❑ designed to protect the device and any information contained in it from unauthorized access, destruction, use, modification, or disclosure

“Reasonable Security Feature”

- If a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a “reasonable security feature” if the preprogrammed password is either
 - ❑ unique to each device or
 - ❑ the device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time

Definitions

➤ “Authentication”

- ❑ “a method of verifying the authority of a user, process, or device to access resources in an information system”

➤ “Connected device”

- ❑ “any device, or other physical object that is capable of connecting to the internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address”

➤ “Manufacturer”

- ❑ “the person who manufactures, or contracts with another person to manufacture on the person’s behalf, connected devices that are sold or offered for sale in California”

Exceptions

- Does not impose a “duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications that a user chooses to add to a connected device.”
- Does not apply “to any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority.”
- Exempts HIPAA covered entities and business associates to the extent the activity in question is covered by that act

It's just the beginning . . .

➤ Many other areas for potential legislation:

❑ IoT Cybersecurity Improvement Act of 2017

- Would have required vendors of IoT devices used by federal government to ensure that their devices are patchable, rely on industry standard protocols, do not use hard-coded passwords, and do not contain vulnerabilities

❑ H.R. 6032, State of Modern Application, Research, and Trends of IoT (or SMART IoT) Act

- Would direct Commerce Secretary to study the state of IoT device industry

➤ Consumer Product Safety Commission

❑ Held hearing in May 2018 on safety concerns with IoT devices

➤ FDA

❑ “Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software”

Data Breach Notification Laws

Understanding Data Breach Notification Laws

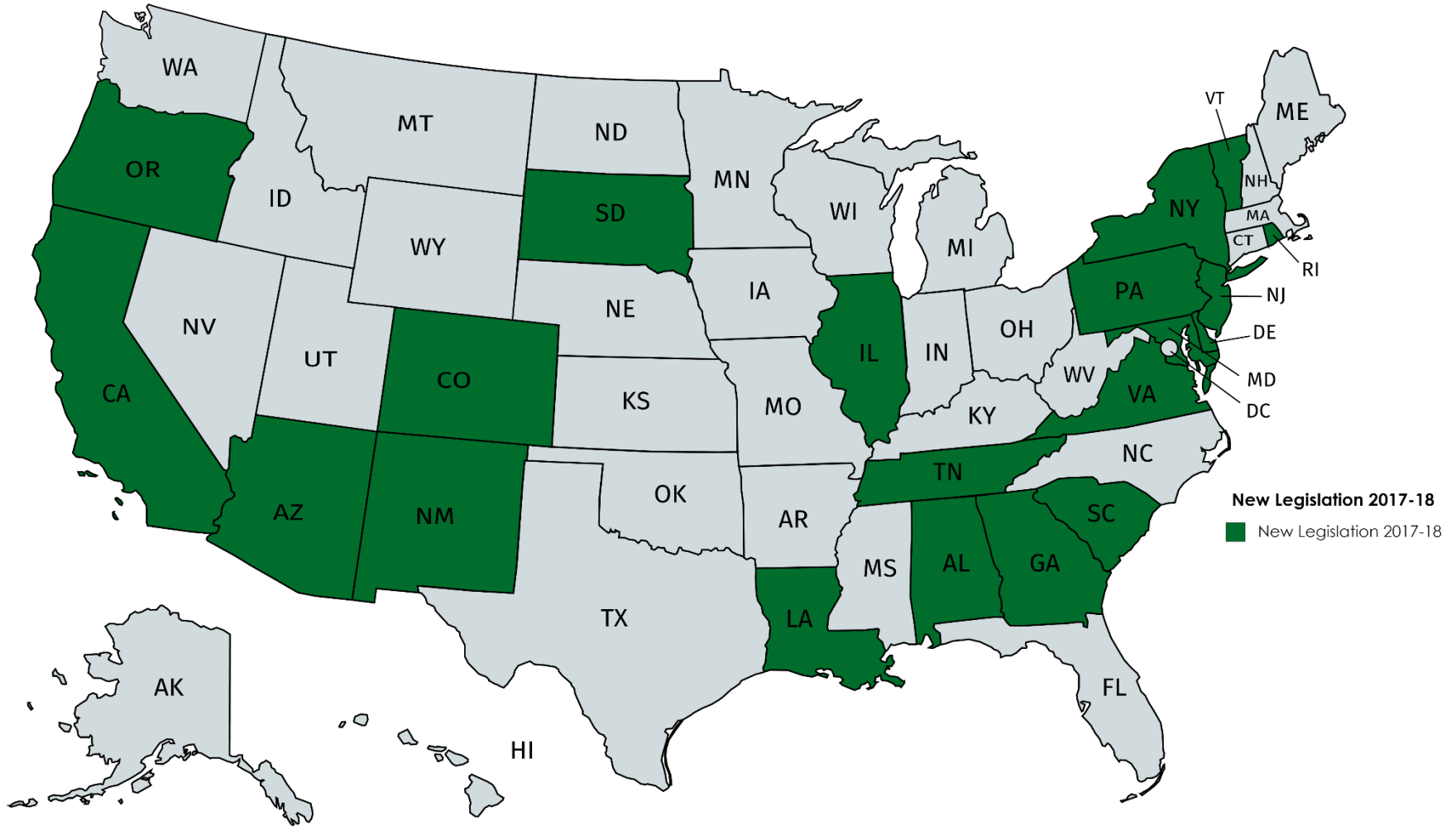
- 50 State laws
 - What constitutes personal information?
 - When is a notice required?
 - Who must be notified?
 - Timing of notice
 - What information must be included in notice?
 - Method of delivering notice
 - Other state-specific requirements, *i.e.*, data security
- Applicable industry-specific laws
- Applicable international laws



Data Breach Legal Developments

- “Personal Information” definitions are expanding
- Regulator notification expanding – 37 states
- Notification timeframes are tightening
 - NY DFS Cybersecurity Regulation – 72 hours
 - GDPR – 72 hours
 - State laws – as expeditiously as possible
 - Contracts/Outside Counsel Guidelines – immediately/24 hrs
- Litigation is growing as cases survive early dismissal
 - Consumer Privacy Class Actions
 - Regulatory Enforcement Actions
 - Shareholder/D&O
 - Commercial Litigation
 - Insurance Coverage

Recent State Statutory Enactments and Amendments



Trends: Companies are no Longer “Victims”

The number of data breaches affecting North Carolina residents “is staggering and unacceptable. North Carolina’s laws on this issue are strong – but they need to be even stronger.”

- North Carolina Attorney General Josh Stein

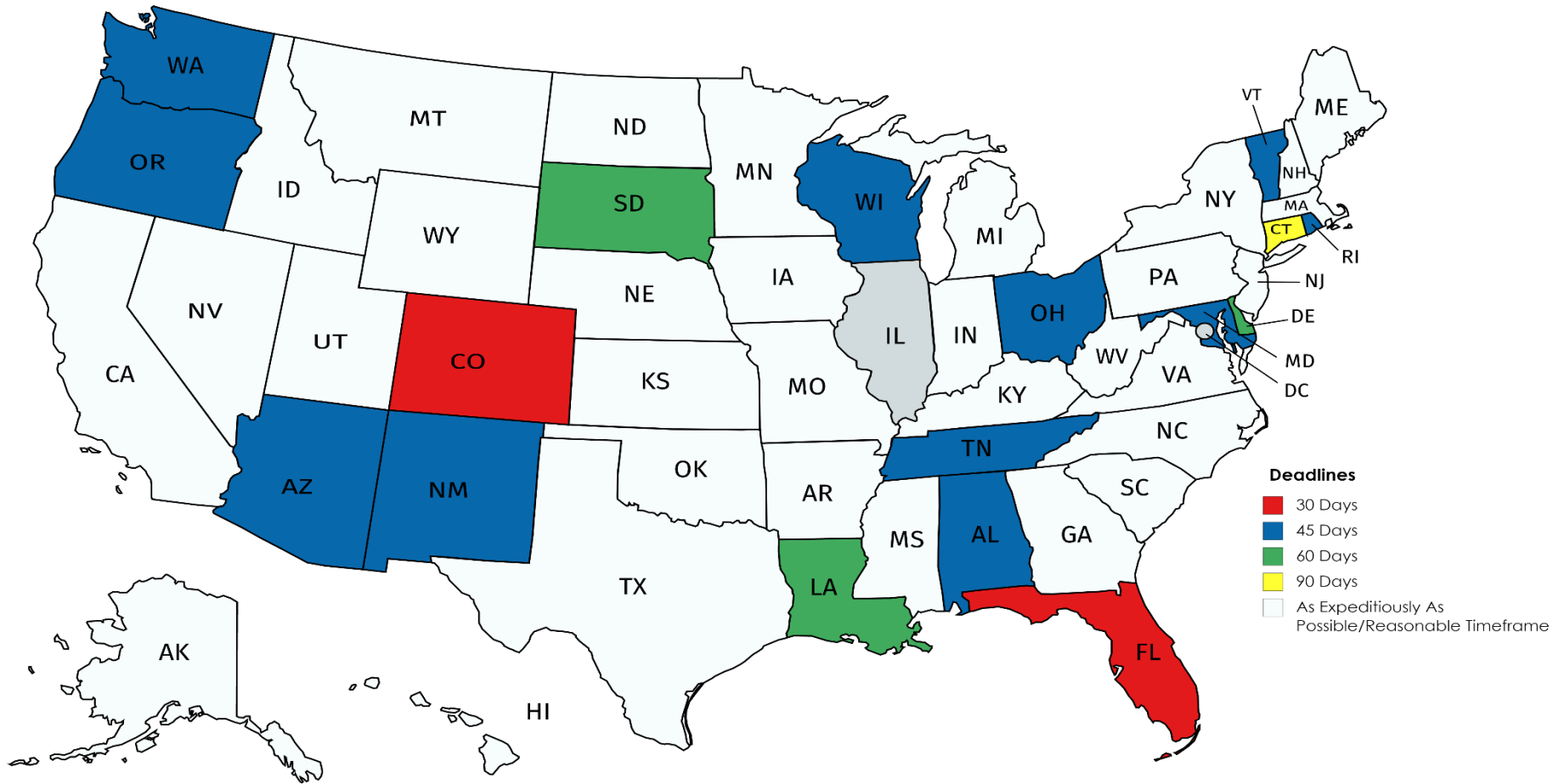
“It’s clear that New York’s data security laws are weak and outdated. The SHIELD Act would help ensure these hacks never happen in the first place. It’s time for Albany to act, so that no more New Yorkers are needlessly victimized by weak data security measures and criminal hackers who are constantly on the prowl.”

- New York Attorney General Eric Schneiderman

Trends: Expanded Definitions of “Personal Information”

	AL	AZ	CO	DE	LA	MD	NM	OR	SD	TN	VA
Passport #	☺	☺	☺	☺	☺			☺			
User Name/Email + Log-In Information	☺	☺	☺	☺					☺		
Medical History/Information	☺	☺	☺	☺				☺	☺		
Health Ins. Policy #	☺	☺	☺	☺				☺			
Biometric		☺	☺	☺	☺		☺	☺	☺		
Tax ID #		☺		☺		☺					
Government Issued ID	☺		☺	☺			☺	☺			
Private Key		☺									

Trends: Enhanced Notice Requirements



Trends: Ransomware Triggers Notification

➤ Currently Four States Require Notice

- Florida, Connecticut, New Jersey, Rhode Island, & Puerto Rico
- Proposed: North Carolina



➤ “Access” v. “Acquisition”

- Florida defines “breach of security” or “breach” as “unauthorized *access* of data”
- Colorado defines “breach of the security system” as “unauthorized *acquisition*”

➤ HIPAA -- 2016 guidance issued by the U.S. Department of Health & Human Services stated that OCR presumes that a ransomware attack triggers “breach” notification obligations under HIPAA.

➤ NYDFS – Ransomware is reportable if it has a material adverse impact.

Trends: Increasing Civil Penalties

- **Arizona**

- Attorney General's office may impose a civil penalty for knowing and willful violations of the statute in an amount "not to exceed the lesser of [\$10,000] per affected individual or the total amount of economic loss sustained by affected individuals" but not to exceed \$500,000.

- **Washington**

- State AG filed civil action against Uber for not timely disclosing its 2016 hack and is contending that statute authorizes AG to seek civil penalty of up to \$2,000 per day per affected individual, totaling several millions of dollars.

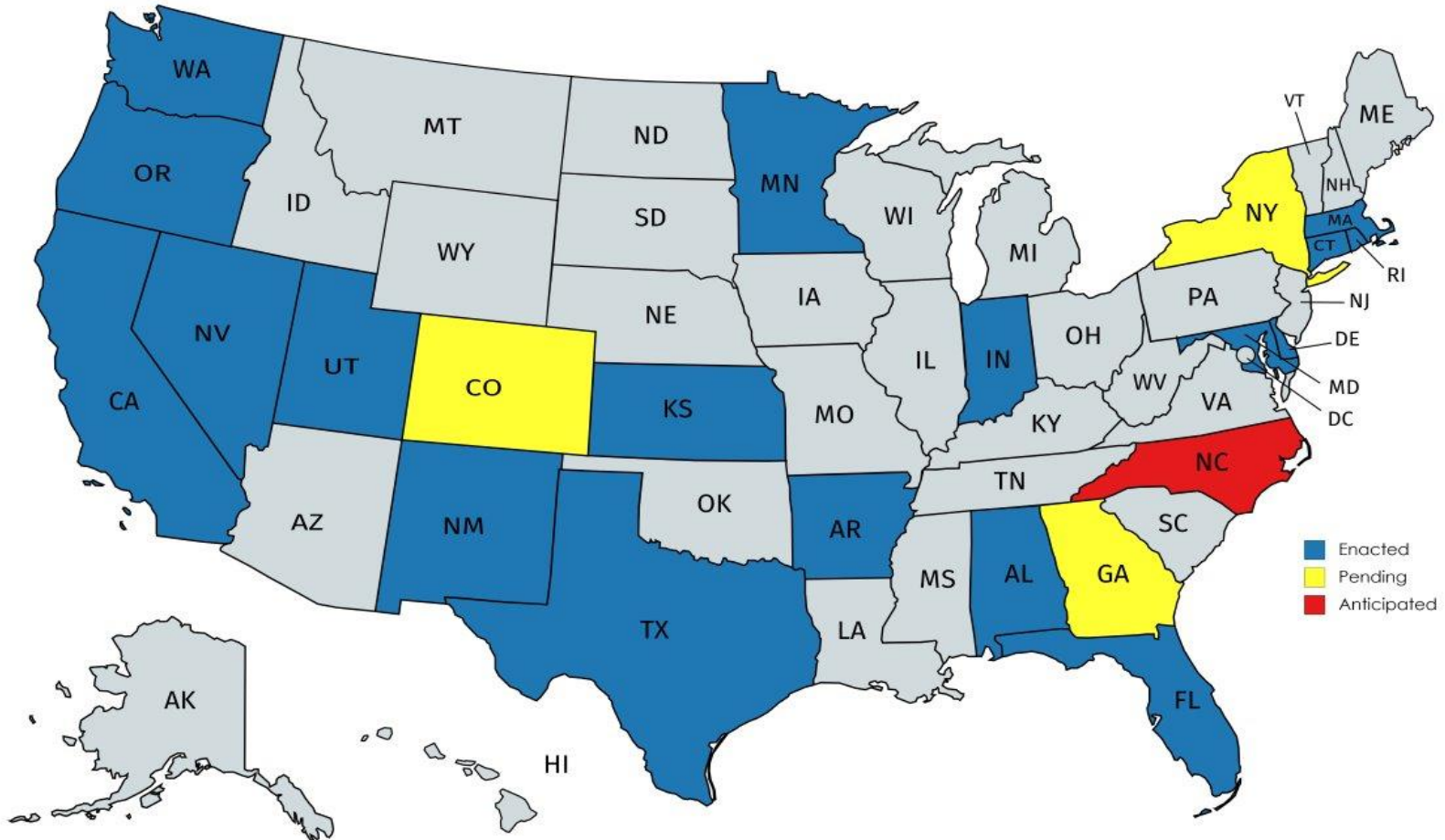


Information Security Laws

State Data Security Laws

- 20 state and numerous federal laws with data security requirements
- Data security laws generally require businesses to:
 - Maintain appropriate security policies, procedures and safeguards (encryption, least privilege, multi-factor authentication)
 - Create an Incident Response Plan
 - Train employees
 - Oversee service providers
 - Periodically assess risks
 - Monitor their programs
 - Fund their programs
 - Massachusetts requires a **written information security program** (WISP)
- California sets a **baseline** for reasonable security practices: “CIS 20 Critical Security Controls.”
- Massachusetts delineates requirements by regulation.
- NYDFS Cybersecurity Regulations are prescriptive.

State Information Security Laws



FTC – Data Security Enforcement

- LabMD v. FTC (11th Cir. 6/6/18)
- Challenge to FTC Consent Order & C&D Order as to “reasonable data security practices”
- Assumes “negligent failure to design and implement reasonable data security practices” can violate §5(a) unfair practices prong
- FTC uses breach “as an entry point to broadly allege that LabMD’s data-security operations are deficient as a whole.”
- Injunction’s command “does not enjoin a specific act or practice” and is therefore unenforceable.

[T]he respondent shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers Such program . . . shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers^[41]

FTC – Data Security Enforcement

In re Uber Technologies, Inc. – FTC Consent Order (April 2018)

- Failure to disclose multiple data breaches (2014 & 2016) affecting over 57 million customers and drivers
- Failure to disclose 2016 breach while negotiating FTC settlement over 2014 breach.
- First FTC data breach notification requirement in a Consent Order

IV. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, within a reasonable time after the date of Respondent's discovery of a Covered Incident, but in any event no later than 10 days after the date Respondent first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission:

Two Types of Information Security Laws

- **Implement and Maintain Reasonable Security Procedures and Practices:**
 - Arkansas, California, Connecticut, Delaware, Florida, Indiana, Kansas, Maryland, Minnesota, Nevada, New Mexico, Rhode Island, Texas, Utah, Washington
- **Prescriptive:**
 - Alabama, Massachusetts, Oregon, NYDFS

Business Takeaways

- **Laws are being used in two significant ways:**
 - By state attorneys' general as part of enforcement actions after data breaches
 - By plaintiffs' attorneys as a basis for claiming that company's negligence caused a data breach

Commonwealth of Mass. v. Equifax

- Massachusetts Attorney General filed civil complaint in September 2017
- Complaint alleged:
 1. Failure to provide notice “as soon as practicable and without reasonable delay” in violation of state’s data breach notification statute
 - Equifax took **41** days to notify



Commonwealth of Mass. v. Equifax

2. Failure to safeguard personal information in violation of state's information security statute

102. Equifax also failed to satisfy its obligations to develop, implement, and maintain a WISP that contained “administrative, technical, and physical safeguards that are appropriate” to: (a) “the size, scope and type of business of” Equifax; (b) “the amount of resources available to” Equifax; (c) the amount of data Equifax stores; and (d) “the need for security and confidentiality of both consumer and employee information.” 201 CMR 17.03(1).

103. These failures include, without limitation: not adequately patching or implementing other safeguards sufficient to avoid the March Security Vulnerability; keeping the Exposed Information unencrypted or otherwise not protected through other methods from unauthorized disclosure in an area of its network accessible to the Internet; and not maintaining multiple layers of security sufficient to protect personal information from compromise.

Commonwealth of Mass. v. Equifax

3. Equifax’s online Privacy Policies were “deceptive” due to Equifax’s “failure to implement, develop, and/or maintain a WISP complaint with” the state information security statute or “industry standards”

118. At all relevant times, Equifax represented to the public on its online Privacy Policy that it has:

[B]uilt our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

119. In its “Consumer Privacy Policy for Personal Credit Reports,” accessible at <http://www.equifax.com/privacy/personal-credit-reports>, Equifax further publicly represented that it has “reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers’] personal information.”

Motion to Dismiss Ruling

- Court denied Equifax’s motion to dismiss in its entirety
- Issue of whether 41 days to provide notice was timely was question of fact for jury to resolve
- Commonwealth’s allegations that “Equifax knew for months it needed to patch its open source code in order to keep its databases secure – or at least that it should have been aware that the software provider had provided public notice of the software vulnerability and how to fix it – and that it failed to do so . . . plausibly suggest that Equifax breached its legal duties” under the state’s information security statute

Class Action Lawsuits

54. Plaintiffs and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's failure to secure and protect their personal identifying information as a result of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft herein, insurance incurred in mitigation, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they suffered loss and are entitled to compensation.
55. Furthermore, Defendant failed to maintain security measures mandated by NRS 603A and was therefore negligent *per se*.
56. Defendant's wrongful actions and/or inaction (as described above) constituted (and continue to constitute) negligence at common law.

Third-Party Contract Requirements

- **8 states require entities to address information security in contracts that govern transfer of personal information**
 - California, Florida, Maryland, Massachusetts, Nevada, New Mexico, Oregon, and Rhode Island
- **California:**
 - "A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure."

GDPR Update

Enforcement

- Effective May 25, 2018
- EU Commission received complaints on Facebook, Google, Amazon, Instagram and WhatsApp within hours of GDPR taking effect but no large scale enforcement actions announced
- DPAs from various countries have stated that it will take months for process to unfold and any potential fines to be assessed

Enforcement

➤ Increase in Complaints

❑ UK Information Commissioner's Office

- 160% increase (6,281 complaints between May 25, 2018 and July 3, 2018 v. 2,417 complaints over same time period in 2017)

❑ CNIL (French Data Protection Authority)

- 56% increase in first 100 days (2,770 complaints v. 1,780 complaints)

❑ Danish Data Protection Agency

- Expects to handle 20,000 cases this year v. 5,000 last year

➤ Over-reporting

- ❑ ICO reports receiving around 500 calls per week to report data breaches since effective date with 1/3 not reportable events

Enforcement

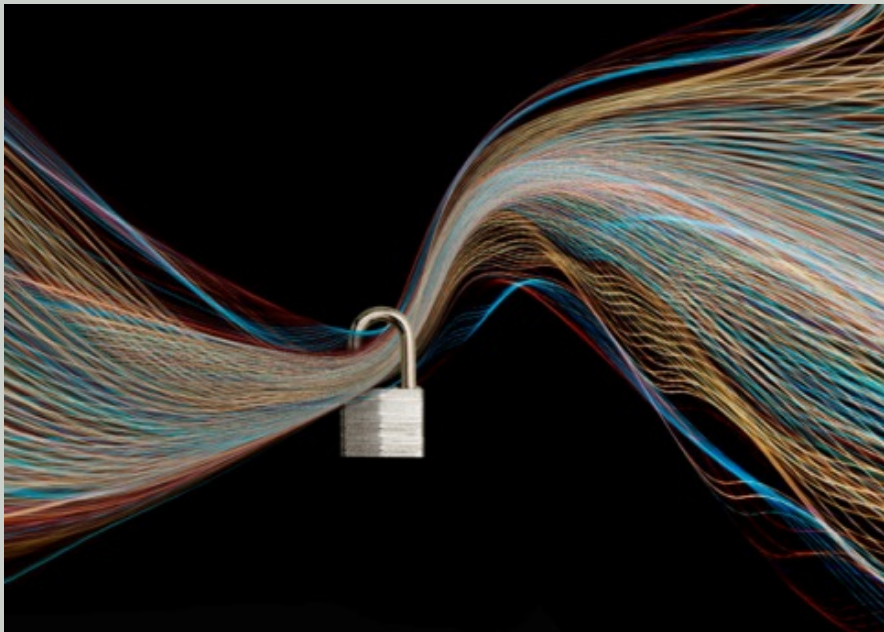
If you take your responsibilities under the GDPR seriously, and have taken reasonable steps to protect that data in line with our security guidance, then we will recognise that. If you adopt privacy by design, treat cyber security as a boardroom issue, and demonstrate a robust culture with appropriate transparency, control and accountability for your and your customers' data, then we will not usually have an issue with you should the worst happen.

-- ICO Deputy Commissioner (Operations) James Dipple-Johnstone – speech to the CBI Cyber Security: Business Insight Conference, September 12, 2018

British Airways as Test Case?

- Hack compromised over 380,000 online transactions from August 21 to September 5
- Credit card and other information for making reservations affected
- BA notified regulators and started notifying affected consumers within 72 hours

Outside Our Borders: How New Laws Will Affect Businesses

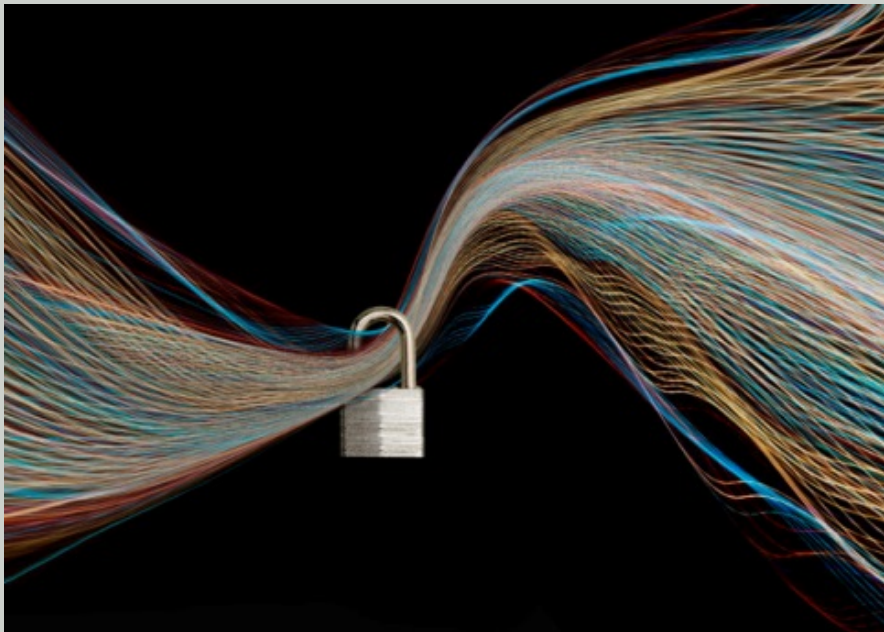


Edward J. McAndrew
mcandrewe@ballardspahr.com

David M. Stauss
staussd@ballardspahr.com

Malia K. Rogers
rogersmk@ballardspahr.com

The End of the “See No Evil” Approach to Vendor Management



Gregory P. Szewczyk

Ballard Spahr LLP

303.299.7382

szewczykkg@ballardspahr.com

Panelist Introductions

Timothy Burke

Director of Cyber Risk
IMA, Inc.



Panelist Introductions

Douglas Brush

Director, Cyber Investigations
Kivu Consulting, Inc.



Agenda

- Outsourcing Upside / Downside
- Privacy Related Issues
- Operational Disruption
- Emerging Areas

Outsourcing Upside

- Reducing and controlling operating costs
- Improving company focus
- Gaining access to world-class capabilities
- Freeing internal resources for other purposes
- Streamlining or increasing efficiency for time-consuming functions
- Maximizing use of external resources
- Sharing risks with a partner company

What About the Downside?

- False sense of security
- Supply chain risk
- Lack of contractual recourse
- Privacy breaches
- Operational disruption

Mixed Levels of Confidence in Vendors



Only 6 percent of in-house counsel report high confidence in their vendors' protecting the company from cybersecurity risks, while a majority (56 percent) say they are somewhat confident. Twenty-one percent are not at all confident. These results are very similar to two years ago (7 percent highly confident, 60 percent somewhat confident, and 17 percent not at all confident).

PRIVACY RELATED ISSUES

Obvious Risk – Vendor Breaches

Data Breaches Often Come From Where You Expect It Least | Inc.com

A Very Large Percentage Of Data Breaches Are Traced Back To Third Parties

By one estimate, as many as 63% of data breaches are traced back to a third party vendor. Many of the major data breaches that have made the news in recent years - Target, CiCi's Pizza, Wendy's, DoTERRA - have been traced back to third party vendors.

PUBLISHED ON: JUL 1, 2017

Always in the News

Vendor Blamed for Health Data Breach Exposing 1,500 BCBSRI Members

September 17, 2018 - Blue Cross and Blue Shield of Rhode Island (BCBSRI) said that a health data breach of PHI affecting 1,567 people was caused by a vendor responsible for sending benefits explanations to members, the *Providence Journal* **reported**.

Other Recent Examples

April 5, 2018

Sears and Delta Airlines customers' payment data exposed by third-party vendor breach

[Bradley Barth](#)



Technical Threats

- Code and application developers
- IT Managed Service Providers
- DDoS
- IoT – all the things (privacy, not just sec)
- Not just technical providers

Technical Threats

National Institute of Standards and Technology
Best Practices in Cyber Supply Chain Risk Management
Conference Materials

Cyber Supply Chain Best Practices

In a Nutshell: Cybersecurity in the supply chain cannot be viewed as an IT problem only. Cyber supply chain risks touch sourcing, vendor management, supply chain continuity and quality, transportation security and many other functions across the enterprise and require a coordinated effort to address.

Cyber Supply Chain Security Principles:

1. **Develop your defenses based on the principle that your systems will be breached.** When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.
2. **Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem.** Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.
3. **Security is Security.** There should be no gap between physical and cybersecurity. Sometimes the bad guys exploit lapses in physical security in order to launch a cyber attack. By the same token, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to get access.

Key Cyber Supply Chain Risks: Cyber supply chain risks covers a lot of territory. Some of the concerns include risks from:

- Third party service providers or vendors – from janitorial services to software engineering -- with physical or virtual access to information systems, software code, or IP.
- Poor information security practices by lower-tier suppliers.
- Compromised software or hardware purchased from suppliers.
- Software security vulnerabilities in supply chain management or supplier systems.
- Counterfeit hardware or hardware with embedded malware.
- Third party data storage or data aggregators.

Examples of Cybersecurity Questions: Companies are using the following questions to determine how risky their suppliers' cybersecurity practices are:

- Is the vendor's software / hardware design process documented? Repeatable? Measurable?
- Is the mitigation of known vulnerabilities factored into product design (through product architecture, run-time protection techniques, code review)?
- How does the vendor stay current on emerging vulnerabilities? What are vendor capabilities to address new "zero day" vulnerabilities?
- What controls are in place to manage and monitor production processes?

NIST National Institute of Standards and Technology • U.S. Department of Commerce Page 1

But Also Exposure Under Laws and Regulations

NEW COLORADO CYBERSECURITY LAW

(2) UNLESS A COVERED ENTITY AGREES TO PROVIDE ITS OWN SECURITY PROTECTION FOR THE INFORMATION IT DISCLOSES TO A THIRD-PARTY SERVICE PROVIDER, THE COVERED ENTITY SHALL REQUIRE THAT THE THIRD-PARTY SERVICE PROVIDER IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE:

(a) APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION DISCLOSED TO THE THIRD-PARTY SERVICE PROVIDER; AND

(b) REASONABLY DESIGNED TO HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION.

How These Requirements Can Play Out

152 3134

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

Commissioners: **Maureen K. Ohlhausen, Acting Chairman**
Terrell McSweeney

_____)
In the Matter of)
)
LENOVO (UNITED STATES) INC.)
a corporation.)

Docket No. C-4636

COMPLAINT

The Federal Trade Commission, having reason to believe that Lenovo (United States) Inc. has violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Lenovo (United States) Inc. ("Lenovo") is a Delaware corporation with its principal office or place of business located at 1009 Think Place, Morrisville, North Carolina 27560-9002.
2. The acts and practices of Respondent alleged in the Complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Respondent is one of the world's largest manufacturers of personal computers, including desktop computers, laptops, notebooks, and tablets. Respondent employs approximately 7,500 people in the United States.
4. In August 2014, Respondent began selling certain laptop models to U.S. consumers with a preinstalled ad-injecting software (commonly referred to as "adware"), known as VisualDiscovery. VisualDiscovery was developed by Superfish, Inc., a Delaware corporation with its principal office or place of business located in Palo Alto, California.
5. VisualDiscovery delivered pop-up ads to consumers of similar-looking products sold by Superfish's retail partners whenever a consumer's cursor hovered over the image of a product on a shopping website. For example, if a consumer's cursor hovered over a product image while the consumer viewed owl pendants on a shopping website like Amazon.com, VisualDiscovery would overlay pop-up ads onto that website of other similar-looking owl pendants sold by Superfish's retail partners.

FTC Action Against Lenovo

- Lenovo laptops with preinstalled Superfish software program called VisualDiscovery
- VisualDiscovery acted as a "man in the middle" between browsers and websites
- To facilitate pop-up ads, VisualDiscovery replaced digital certificates for encrypted websites with its own certificates
 - Did not verify websites' certificates before replacing them
 - Used same easy-to-crack password on every laptop

Allegations of Vulnerabilities – Not Breaches

RESPONDENT FAILED TO IMPLEMENT REASONABLE SECURITY REVIEWS OF ITS CUSTOMIZED VISUALDISCOVERY SOFTWARE

24. Respondent failed to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptops. For example,
- a. Respondent failed to adopt and implement written data security standards, policies, procedures or practices that applied to third-party software preinstalled on its laptops;
 - b. Respondent failed to adequately assess the data security risks of third-party software prior to preinstallation;
 - c. Respondent did not request or review any information about Superfish's data security policies, procedures and practices, including any security testing conducted by or on behalf of Superfish during its software development process, nor did Respondent request or review any information about the Komodia tool after Superfish informed Respondent that it could cause VisualDiscovery to be flagged by antivirus companies;
 - d. Respondent failed to require Superfish by contract to adopt and implement reasonable data security measures to protect Lenovo users' personal information;
 - e. Respondent failed to assess VisualDiscovery's compliance with reasonable data security standards, including failing to reasonably test, audit, assess or review the security of VisualDiscovery prior to preinstallation; and
 - f. Respondent did not provide adequate data security training for those employees responsible for testing third-party software.

Contracting Considerations

- Confidentiality
- Information Security Requirements
 - General v. Specific
- Audit Rights
- Disclosure and Use Controls
- Breach and Investigation Obligations
- Indemnification

Risk Assessment

Inventory

- What providers have access to our data?
- Type of data?

Controls

- Technical risk evaluation?
- Contractual controls?

Risk Transfer

- Do we have insurance coverage for acts of vendors on our behalf?
- Does vendor have appropriate coverage?

Insurance Solutions

- Most Cyber policies will respond to acts of vendors on your behalf
 - Data breach management expenses
 - Forensic expenses
 - Legal expenses
- Eliminates need to wait for vendor to respond and allows for a pro-active solution
- Requires some form of contract in place with service provider

OPERATIONAL DISRUPTION


Caveat Emptor

- An extreme cyber incident that takes a top cloud provider offline in the US for 3 to 6 days would result in economic losses of \$15bn and up to \$3bn in insured losses.
- Businesses outside the Fortune 1000 would carry 63% share of economic losses and 57% of insured losses – indicating that they are at the highest risk.

Source: Lloyds of London - Cloud down

- According to a recent survey by Veritas Technologies, 60 percent of respondents have not fully evaluated the cost of a cloud outage to their business and are therefore ill prepared to deal with the impact of an outage.

Recent Example

A photograph of healthcare providers in a clinical setting, wearing scrubs and surgical masks. The image is overlaid with a dark blue semi-transparent layer containing white text.

Healthcare Providers Still Paralyzed Following Allscripts Ransomware Attack

by [Chris Brook](#) on Monday June 25, 2018

Technical Diligence / Threats

- If they are out, you are out
- SaaS based (not just the biggies)
- Contract review – can you get your data back when you need to – ownership?
- Don't put your egg in one basket

Risk Assessment

Inventory

- What providers are mission critical?
- Maximum Tolerable Downtime?

Controls

- Technical risk evaluation?
- Contractual controls?

Risk Transfer

- Do we have insurance for vendor disruption built into Business Continuity Plan (BCP)?
- Does coverage address downtime / degradation at service provider?

Insurance Solutions

- Business Continuity Plan
- Cyber policies can provide coverage for Contingent Business Interruption
 - Downtime of service provider
- Subject to a waiting period (6-12 hours)
- Coverage will indemnify you for the loss of income
 - Forensic expense
 - Arrange for alternative providers
 - Internal expense

New Technologies, New Risks

2018 Study on Global Megatrends in Cybersecurity

Ponemon Institute, February 2018

Disruptive technologies that can increase the possibility of a security incident are the IoT, acceptance of virtual currencies, use of artificial intelligence, big data analytics, use of drones and use of cloud services (SaaS). However, participants predict their ability to minimize the risks

A data breach from an unsecured Internet of Things (IoT) device in the workplace is predicted to be very likely over the next three years. 82% of respondents predict unsecured IoT devices will likely cause a data breach in their organizations. **80% say such a breach could be catastrophic**

Takeaways: How to Mitigate Risk to Maximize Benefits

- Meaningful Diligence
 - Legal and Technical
- Real Contractual Controls
 - Information Security / Breach Response
 - Operational Disruption
- Make Sure Coverage Matches Risk

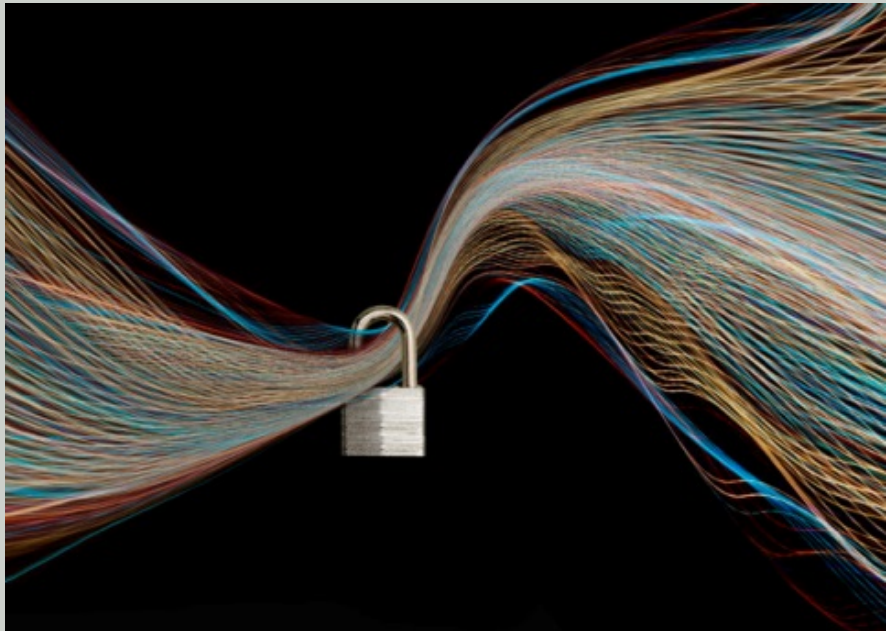
Questions?

Gregory P. Szewczyk
Privacy and Cybersecurity
303.299.7382
szewczyk@ballardspahr.com

Tim Burke
Director, Cyber Risk
303-615-7676
tim.burke@imacorp.com

Douglas Brush
Director, Cyber Investigations
720-990-5390
dbrush@kivuconsulting.com

Perspectives from the Enforcers: The New Colorado Cybersecurity Law



Alissa Gardenswartz

Deputy Attorney General

Colorado Attorney General's Office

Jennifer Anderson

Former Director of Legislative Affairs

Colorado Attorney General's Office

David M. Stauss

Partner

Ballard Spahr LLP

Background

Attorney General Coffman Joins \$18.5M Settlement with Target Corporation Over 2013 Data Breach

Coffman will convene a working group over the summer focused on strengthening Colorado's data breach laws and privacy protections

DENVER – Today Attorney General Cynthia H. Coffman announced that Colorado has joined with 46 other states and the District of Columbia in an \$18.5 million settlement with the Target Corporation to resolve the states' investigation into the retail company's 2013 data breach. The settlement represents the largest multistate data breach settlement achieved to date.

Date

May 24th, 2017

Author

Annie Skinner

Background

“Target’s inadequate security measures became obvious in this case, and nearly one-fifth of our population was impacted by the breach. However, because Colorado’s data breach and privacy laws are so weak compared to other states, we were unable to credibly take a leadership position in the litigation. It’s time Colorado’s data protection law sets a higher standard for companies and governments entrusted with consumers’ private information,” said Attorney General Coffman. “I will be convening a privacy working group this summer to research and recommend more effective legislation in the 2018 session. Colorado needs to move to the forefront in protecting consumers from theft of their personal information and the potentially devastating consequences.”

Background

- Bill introduced in Colorado House of Representatives on Jan. 19, 2018
- Spearheaded by Colorado Attorney General's office with bi-partisan support in House and Senate
- Underwent significant revisions with six published versions
- Ballard Spahr was involved as a neutral party providing assistance to Attorney General's office and bill sponsors
- Passed House and Senate without a single "no" vote
- Signed by Governor on May 29, 2018
- Effective September 1, 2018

Key Takeaways

- **New Information Security Requirements**
 1. Implement and maintain reasonable security measures to protect documents containing personal identifying information
 2. Contractually require third-party service providers to implement and maintain reasonable security measures
 3. Implement a written policy to dispose of documents containing personal identifying information

Key Takeaways

- **Significant Changes to Breach Notification Statute**
 1. 30 days to provide notice (shortest time frame in the country)
 - No carve outs for HIPAA and GLBA regulated entities
 2. Expanded definition of “personal information,” including medical information and log-in credentials
 3. New obligation to notify Attorney General