Cybersecurity, Privacy and Social Media Group

Privacy Titans: Enter the CCPA

September 17, 2019

Cybersecurity, Privacy and Social Media Group

Privacy Titans: Enter the CCPA

September 17, 2019

Materials

*Visit **Dorsey.com** to check out Dorsey's **Online Screening Tool** to determine your compliance status with California's Consumer Privacy Act (CCPA). To launch Dorsey's **Online Screening Tool** go to: https://www.dorsey.com/services/ccpa*

Cybersecurity, Privacy and Social Media Group

Privacy Titans: Enter the CCPA

September 17, 2019

Overview

Beginning January 1, companies around the world will need to comply with the California Consumer Privacy Act (CCPA) if they collect personal information on California residents. Dorsey's Cybersecurity, Privacy and Social Media Group is conducting a half-day conference to help companies understand the practical aspects of this new, sweeping privacy law.

Agenda and Panel Descriptions

11:45 am – 12:15 pm **Registration and Lunch**

12:15 – 12:20 pm **Welcome: Jamie Nafziger, Partner, Dorsey & Whitney LLP**

12:20 – 1:20 pm **Fines of Fury**

The CCPA contains onerous compliance requirements with hefty penalties. In Fines of Fury, attendees will learn more about the risks of non-compliance, and the significant impact CCPA may have on the increasingly complicated calculus for assessing whether an incident should be reported.

***Shawn Fleury**, Director, The Crypsis Group*
***Pete Storm**, Principal Consultant, The Crypsis Group*
***Robert Cattanach**, Partner, Dorsey & Whitney LLP*

1:20 – 1:30 pm **Break**

1:30 – 2:30 pm **Game of Compliance**

Without significant guidance from the California Attorney General, companies will have to look to each other for help on what constitutes reasonable measures. In Game of Compliance, attendees will learn what other major industry players are thinking about as they work toward CCPA compliance.

***Alfredo Della Monica**, Vice President and Senior Counsel U.S. Privacy & Data Use, American Express*
***Michelle Finneran Dennedy**, Chief Executive Officer, Drumwave, Inc.*
***Cody Wamsley**, CISSP, Associate, Dorsey & Whitney LLP*

2:30 – 2:40 pm **Break**

2:40 – 3:40 pm **Way of the Resilient**

A structured, methodical approach is crucial to achieving CCPA readiness. In Way of the Resilient, attendees will learn what actionable next steps they should take on their path toward January 1.

***Michael Schell**, Director of Strategic Accounts & Channels – U.S., EdgeScan*
***Robert Cattanach**, Partner, Dorsey & Whitney LLP*
***Jamie Nafziger**, Partner & Chair, Cybersecurity, Privacy & Social Media Group, Dorsey & Whitney LLP*
***Cody Wamsley**, CISSP, Associate, Dorsey & Whitney LLP*

3:40 – 3:45 pm **Closing: Jamie Nafziger, Partner, Dorsey & Whitney LLP**

3:45 pm **Reception**

Cybersecurity, Privacy and Social Media Group

Privacy Titans: Enter the CCPA

Speaker Biographies

Robert Cattanach
Partner
Dorsey & Whitney LLP
Minneapolis, Minnesota
(612) 340-2873
cattanach.robert@dorsey.com

Bob Cattanach is a Partner in Dorsey's Regulatory Affairs Group. His technical background and business savvy enable him to understand the challenges of today's cyber world and evolving privacy regulations. Bob works collaboratively with clients to determine their regulatory obligations, evaluate risk tolerances, and find optimal solutions in the ever-evolving world of data collection, use, sharing and ultimately safe destruction. Recognized by his peers as a thought leader in the areas of data security and privacy litigation, Bob serves as a member of the Sedona Conference Steering Committee for Working Group 11. Under his leadership, the Sedona Conference has published for public comment an Incident Response Guide, and he has led Sedona presentations to Working Group 11, as well as Sedona's International Programme, on subjects including incident response, the European Union General Data Protection Regulation (GDPR) and California's new Consumer Privacy Act (CCPA). He represents clients in breach responses, development of privacy policies and procedures, and counsels corporate Boards of Directors and Audit Committees on matters of cybersecurity, privacy and information governance. Bob's unique skill set comes from decades of experience as a trial lawyer, and he maintains an active trial docket in courts around the country. Even the best compliance practices can occasionally fall victim to skilled hackers. When (unfortunately not if) this occurs, Bob's trial-honed ability to craft a compelling narrative that explains the client's compliance efforts and commitment can mean the difference between constructive regulatory dialogue versus potentially crippling sanctions. Bob is also a much-sought-after commentator and contributor to professional and journalistic coverage of cybersecurity issues, ranging from the New York Times and USA Today and numerous electronic media to various professional publications and blogs.

Alfredo Della Monica
Vice President and Senior Counsel U.S. Privacy & Data Use
American Express
New York, New York

Alfredo Della Monica is a VP/Senior Counsel in the Global Privacy Team at American Express. He is responsible for advising on US privacy issues and continues to have an oversight role on EMEA data protection matters, after leading the team in London for 5 years. As a subject matter expert within the General Counsels' Organization, Alfredo has a horizontal view of issues across the different AXP businesses and he regularly provides advice on complex - and cross country - privacy issues. Alfredo joined American Express in 2011 after spending almost 7 years with Cleary Gottlieb Steen & Hamilton LLP in Rome advising various clients on a broad range of regulatory matters, including data protection and privacy issues. Before that, he also worked as intern at the Italian Antitrust Authority and the Federal Trade Commission in NYC.

Michelle Finneran Dennedy
Chief Executive Officer
Drumwave, Inc.
Los Altos, California

Michelle Finneran Dennedy currently serves as CEO of Drumwave, Inc. She is the former Chief Privacy Officer at Cisco where she was responsible for the development and implementation of the organization's data privacy policies and practices, working across business groups to drive data privacy excellence across the security continuum. Throughout her career, Michelle has led security and privacy initiatives, ranging from regulatory compliance, privacy engineering, advocacy and education efforts, and litigation at companies including McAfee/Intel Security, Oracle, and Sun Microsystems. She founded The iDennedy Project, which seeks to change how people think about information and data, and co-authored The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value. Michelle is a highly sought-after public speaker who sits on the boards of the International Association of Privacy Professionals (IAPP) and the National Multiple Sclerosis Society of Northern California. She has been honored with many industry awards

including California's Most Powerful and Influential Women, by the National Diversity Council; the IAPP Vanguard Award; Woman of Influence for Security and Privacy, from the Executive Women's Forum (EWF) and CSO Magazine; Woman of the Year in Technology and Transformation, by the Stevie American Business Awards, and most recently, World Women Awards Silver Winner for Female Executive of the Year for her leadership in optimizing Cisco's privacy maturity.

Shawn Fleury
Director, Risk Management
The Crypsis Group
(234) 244.7236
shawn.fleury@crypsisgroup.com

Shawn Fleury is a digital investigations and computer forensics expert who is a director of The Crypsis Group's risk management practice. Over a 15-year career that began as a computer crimes investigator with the U.S. military, Shawn has handled incident response and digital forensics for companies across a wide range of industries. Shawn joined Crypsis in 2019 from the professional services firm Alvarez & Marsal, where he spent eight years in its global forensics disputes practice, rising from senior security analyst to director. There, he handled network intrusion response, digital media acquisition and analysis, and eDiscovery investigations for the firm's clients. During this time, Shawn also served as an instructor for the U.S. State Department's Anti-Terrorism Assistance Program. In that position he provided advice and training to foreign law enforcement officers on areas including cyber terrorism, computer investigations, and cyber-crime. Previous to that, he was a security analyst at Dell, where he performed digital investigations and was assigned to investigate internal employee cases regarding loss of proprietary information and misuse of company resources. He also worked in the same capacity for the financial services company USAA, where he built and ran its digital forensics lab. Shawn began his career with the U.S. Air Force Office of Special Investigations, where he worked on computer investigations of crimes alleged to have been committed by Air Force personnel.

Jamie Nafziger
Partner
Dorsey & Whitney LLP
Minneapolis, Minnesota
(612) 343-7922
nafziger.jamie@dorsey.com

Jamie Nafziger is a Partner and Chair of Dorsey's Cybersecurity, Privacy and Social Media Group. For over twenty years, Jamie has helped clients grow their businesses by developing stellar brands, advertising their products and services, and launching cutting-edge online services and mobile apps. A technology lover, Jamie guides clients through complex and ever-changing privacy laws and internet regulations. She has been helping clients comply with the European Union's General Data Protection Regulation (GDPR) in terms of external policies/agreements, internal processes, and responding to data subject requests. She has extensive experience advising on website and mobile app terms of use and privacy policies and licensing agreements having drafted over 100 sets of website and mobile app policies. She also helps clients comply with email and text messaging laws and regulations and deal with internet fraud. She has an interest in facial recognition, other biometrics, and new forms of identification and authentication and the privacy issues arising from them. As part of the firm's top-ranked trademark team, Jamie helps clients develop branding strategies and acquire and enforce U.S. and international rights in trademarks and copyrights. Jamie has prosecuted over 100 trademark oppositions with the U.S. Trademark Trial and Appeal Board. She has deep experience with domain names, successfully assisted several clients with applications to run .brand generic top level domain names, and is assisting several domain name registry operators with contracts, policy development, and compliance with ICANN rules. Jamie also develops defensive domain name strategies and handles domain name disputes. Jamie is a frequent author and national lecturer on privacy, mobile apps, trademark law, internet law, social networking, and domain names. She has served several terms on the Internet Committee of the International Trademark Association and is past Chair of the Computer and Technology Law Section of the Minnesota State Bar Association. Jamie is a contributor to Dorsey's critically-acclaimed IP Blog, TheTMCA.com, which focuses on legal developments in the world of TradeMarks, Copyrights, and Advertising. TheTMCA.com was named one of the "Top 50" law blogs by the ABA Journal in 2018.

Michael Schell
Director of Strategic Accounts & Channels – U.S.
EdgeScan
Los Angeles, California

Michael Schell has almost two decades of experience as a cyber practitioner, business development executive and conference host. He is a high-energy executive who is not afraid to roll up his sleeves. Michael is very easy to approach, and doesn't take himself too seriously.

Pete Storm
Principal Consultant
The Crypsis Group
(320) 828-6980
pete.storm@crypsisgroup.com

Pete Storm, a principal consultant at The Crypsis Group, is a recognized leader in the field of digital investigations, computer forensics, and online fraud. A Certified Public Accountant and a Certified Fraud Examiner, he has nearly a decade of experience investigating network intrusions and helping organizations protect themselves from cyber attacks and other digital threats to their operations. Over the course of his career, Pete has provided expert witness testimony in lawsuits across the country, commenting on issues including the validity of digital photographs, comparison of customer lists, analysis of email communications, and forensic examinations of computers, servers, mobile devices, and log data. He has also presented at numerous IT and legal conferences on topics including risk assessment, digital investigations, and payment fraud trends and prevention strategies. Pete joined Crypsis in 2019 after leading digital forensics and incident response investigations at UnitedHealth Group, where worked with the company's cyber defense team on high impact investigations. Previously, he was a consultant at Stroz Friedberg, where he managed digital forensic and incident response investigations for the firm's clients. His work included leading forensic examinations of a restaurant chain's malware-infected point of sale systems, theft of credit card data from a large retailer, and mass exfiltration of customer records from a global financial institution. Earlier in his career, Pete was a senior information security consultant for the large Accountancy firm CliftonLarsonAllen, where he led and executed Red Team assessments involving network and physical security components. He also advised financial, government, nonprofit, manufacturing, and health care clients in matters involving network security, fraud prevention, incident response planning, and data theft.

Cody Wamsley, CISSP
Associate
Dorsey & Whitney LLP
Minneapolis, Minnesota
(612) 492-6858
wamsley.cody@dorsey.com

Cody Wamsley is an Associate in Dorsey's Trademark Group. His background as a patent attorney and information security subject matter expert enables him to interface seamlessly with technical security professionals while simultaneously drawing on his management experience to integrate with executives and provide strategic guidance to achieve success. Cody's experience includes data breach response, information security policy and program development, third party risk, negotiating and drafting complex technology contracts, providing counsel on technology transactions, and advising on global data security and privacy issues for both startups and large enterprises. Cody is the GDPR lead for Dorsey's internal compliance and has assisted numerous clients in developing comprehensive GDPR-ready privacy programs. He has spoken widely on information security issues at industry conferences and on television.

DORSEY
always ahead

Fines of Fury

Shawn Fleury, *Director, The Crypsis Group*
Pete Storm, *Principal Consultant, The Crypsis Group*
Robert Cattanach, *Partner, Dorsey & Whitney LLP*

Does CCPA Apply to Your Company?

- **$25 Million sales (undefined but assume global)**
- **For-profit (large enterprise non-profits?)**
- **50,000 individuals (sounds like a lot, but it's only 137 visitors a day from California)**

DORSEY
always ahead

CCPA In a Nutshell

- Disclosures to Consumers
- Consumer Rights
- Anti-discrimination
- Adequate Security Measures
- Primary Focus of Our Panel: Security Incidents

DORSEY™ always ahead

Notifications Required Under CCPA

- Categories of personal information a company uses, and how
- What it sells or discloses and to whom
- Consumer's ability to access/delete their information;
- A "Do Not Sell My Personal Information" dedicated link on your website

DORSEY™ always ahead

FINES OF FURY

Data Requests by Consumers

- What do you collect?
- How do you use it?
- To whom do you disclose it?
- DO NOT SELL
- Delete my information

DORSEY always ahead

FINES OF FURY

Exceptions to CCPA

- Employees (some disclosures still required)
- Business-to-business personal information
  - Does not apply to "Do Not Sell"
  - Does not apply to Non-Discrimination
  - Does not apply to information from third parties
- One year moratorium only

DORSEY always ahead

FINES OF FURY

Practical Pitfalls: Consumer Requests

- Businesses may require entirely new processes for responding to consumer requests
- Greater employee training obligations
- Verify consumer's identity before producing responsive info
- Increased vulnerability in communicating with consumers – mistakes will happen
- Increased vulnerability with open websites for consumers
  - Equifax learned the hard way
- How can you demonstrate everything has been deleted?

DORSEY™ always ahead

Cannot Discriminate Against Consumers Exercising Rights Under CCPA

- Denying goods or services
- Charging different prices
- Offering different qualities of goods or services
- ***Unless:*** different treatment is "reasonably related to the value provided to the consumer by the consumer's data"

DORSEY™ always ahead

FINES OF FURY

Special Treatment for Service Providers

- Written contract required
- Contract prohibits service provider from:
  - retaining, using, or disclosing personal information for ***any purpose other than*** performing services specified in the contract
- Service provider must delete the consumer's personal information if requested
- ***If*** the service provider ***also holds personal information***
  - must assist with consumer CCPA requests
  - must provide the consumer with a copy of personal information in a portable and "readily usable" format

DORSEY always ahead

Adequacy of Security Measures

Failure to protect: "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* …" Section 1798.150(a)(1).

- What does this mean for your company?
- Does ISO 27000 or SOC-2 get you anything?
- Can encryption be a safe harbor?
  - As a practical matter, how do you implement?

DORSEY always ahead

CCPA Penalties – Attorney General

- **Violation of consumer rights:**
  - **Notifications**
  - **Consumer requests**
  - **Non-Discrimination**
- **Up to $2,500/violation/day - $7,500 for intentional violations**
- **What constitutes a violation for purposes of the AG-enforcement**
  - ***Each action* by the violator?**
  - ***Each individual* whose rights have been violated?**
  - ***Each section* of the CCPA that has been violated?**

DORSEY™ always ahead

Private Enforcement: Data Breaches

- **Per violation penalties for a breach are more clear**
- **$100 ($750 if intentional) *per consumer; per incident*, or actual damages, whichever is greater**
- ***Private right of action* for *exfiltration* of certain personal information (*unauthorized access* may suffice, too)**
  - **Social Security number, driver's license number, medical information, and other information subject to California's breach notification statute**
  - **More limited definition than CCPA's much broader definition of any information "relating to an individual"**

DORSEY™ always ahead

Penalty Criteria

- Nature and seriousness of the misconduct
- Number of violations
- Persistence of the misconduct
- Length of time over which the misconduct occurred
- Willfulness of the defendant's misconduct
- Defendant's assets, liabilities and net worth

DORSEY™ always ahead

Opportunity to Cure

- 30 days after notice of intention to enforce
- Can you even "cure" a data breach?
  - Presumably could cure the system vulnerability that caused the breach (e.g. patch management)
  - What about inadequate employee training that resulted in a compromise from phishing?

DORSEY™ always ahead

FINES OF FURY

Theory Clashes With Reality In a Data Breach: What do You Need to Know, and When do You Need to Know It

- What triggers an obligation to report?
  - Regulators
  - Consumers
  - Law Enforcement
  - Social Media Trumps all

DORSEY always ahead

When Do You Report, and to Whom?

- GDPR Article 33 Notice to Supervisory Authorities
  - 72 hours ***unless*** "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" [different standard than under Article 34]
- New York Department of Financial Supervision (NYDFS)
  - Required if notice to "any other supervisory authority" (e.g. SA's under Article 33)
- Vermont Attorney General
  - 14 days unless Incident Response Plan has been filed with Attorney General
- Insider blackouts for public companies
- South Korea – 24 hours?!?!?
- Securities and Exchange Commission
  - Regulation FD - selective disclosure
- Stakeholders
  - Board
  - Shareholders
  - Employees

DORSEY always ahead

Risk Tolerance, and Risk Assessment

- The Clock Ticks ***Really Quickly*** In the "Fog of Breach"
- Tensions invariably arise
  - Communication specialists will want to control the narrative = speed
  - Legal will press to delay until you know whether any reporting obligations are triggered = delay
- Social Media doesn't follow any rules

DORSEY always ahead

Internal IT and Outside Forensics

- Need to work together
- Preserve the crime scene
- External resources often have more current insight into trends, patterns, attacker signatures
  - E.g. Ransomware and phishing entirely different objectives
- Time and stress saver: retain outside resources in advance through master services agreements
  - Some companies go so far as to retain two forensic consultants in case of a potential conflict

DORSEY always ahead

What Can You Expect and When

- What you can expect:
  - Here's what we're seeing
  - Here's what we're not seeing
  - Here's what we expect to see
- The myth of 'exfiltration' as the benchmark standard
- Don't expect absolute certainty
  - The process is more like an asymptotic function
  - The more time and resources you spend the closer you will get to being certain
- But the clock is ticking…

DORSEY™ always ahead

Business Email Compromise

- Intrusion
  - Threat actor in email system on average two to six weeks
    - Finding targets (employees that manage wires)
    - Searching email – "payment," "wire," etc…
    - Setting up rules to hide or forward mail
  - Aggressive
- Detection
  - Fraudulent wire transfer
- Investigation
  - Triage to determine scope of incident (1 – 3 days)
  - Full analysis to complete investigation (7 – 14 days)

DORSEY™ always ahead

Business Email Compromise

- **Remediation**
  - **Security configurations**
  - **Multifactor**
- **Other Considerations**
  - **Account and email access**
  - **Other services (e.g., SharePoint and OneDrive)**
  - **Email synchronization (data analytics)**
  - **On premise vs. Office 365**
  - **Intent**

DORSEY™ always ahead

Ransomware Attack

- **Intrusion**
  - **Threat actor in network up to a month or two**
  - **Bulk of activity days prior to ransomware deployment**
- **Detection**
  - **Critical systems encrypted**
  - **Business shut down**
- **Investigation**
  - **Two to four weeks for full investigation (average)**
    - **Determine Patient 0**
    - **Determine extent of intrusion**
    - **Determine data access or exfiltration**

DORSEY™ always ahead

FINES OF FURY

Ransomware Attack

- Remediation
  - Often challenging and time consuming
  - Availability of backups
  - Cleaning systems
  - Locking out threat actor
- Other considerations
  - Determining what was accessed
    - Artifacts often limited (encrypted, deleted, etc…)
  - Email access and scraping of metadata
  - Ransom of data (e.g., threat actor copies and deletes database)

DORSEY™ always ahead

Non-Ransomware Network Intrusion Investigations

- Intrusion
  - Months or years with a foothold in the network
- Detection
  - Notification from agency, service provider, vendor, merchant
  - Data posted online
  - Anomalous activity detected on systems
- Investigation
  - Investigation timeline largely depends on the scope of the incident and availability of evidence
  - Investigation weeks to a few months
- Remediation

DORSEY™ always ahead

FINES OF FURY

Takeaways

- **Timing of an investigation depends on**
  - **Availability of response team (retainer?)**
  - **Scope of intrusion (# of systems or accounts impacted)**
  - **Gathering evidence (Forensic imaging, data transfers, restoration, etc…)**
  - **Availability of evidence**
    - **Logging**
    - **Deletion**
- **Data exfiltration**
  - **Often times the entire trail of bread crumbs does not exist**

DORSEY™ always ahead

DORSEY
always ahead

Game of Compliance

Alfredo Della Monica, *Vice President and Senior Counsel U.S. Privacy & Data Use, American Express*

Michelle Finneran Dennedy, *Chief Executive Officer, Drumwave, Inc.*

Cody Wamsley, *CISSP, Associate, Dorsey & Whitney LLP*

Game of Compliance Topics

1) Handling Consumer Requests
2) "Do Not Sell My Personal Information" Button
3) Geofencing California Residents
4) Loyalty / Rewards Programs
5) Privacy Policy Construction
6) Reasonable Security Measures
7) Vendor Agreements

DORSEY
always ahead

Handling Consumer Requests

"A business that receives a verifiable consumer request from a consumer to…"

- **Access personal information**
- **Delete the consumer's personal information**

… shall disclose and deliver the required information to a consumer free of charge within 45 days

- **Extensions possible**
- **"Reasonable fee" or refusal for excessive or burdensome requests possible**

DORSEY always ahead

GAME OF COMPLIANCE

Handling Consumer Requests

Verify
Handle

DORSEY always ahead

GAME OF COMPLIANCE

"Do Not Sell My Personal Information"

"A business [that sells personal information about a consumer to third parties] shall … provide a clear and conspicuous link on the business's Internet homepage, titled 'Do Not Sell My Personal Information,' to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information."

"Sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

DORSEY™ always ahead

"Do Not Sell My Personal Information"

"Sale"
Button placement

DORSEY™ always ahead

Geofencing

"Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally."

DORSEY™ always ahead

Geofencing

Approaches for Geofencing

DORSEY™ always ahead

Loyalty / Rewards Programs

"A business shall not sell the personal information of consumers collected as part of a loyalty, rewards, premium features, discounts, or club card program."

- **Pending amendment AB 846 at time of drafting this slide**
  - **Express consent exception**
  - **Personal information use restrictions**

DORSEY always ahead

Loyalty / Rewards Programs

Industry Perspectives

DORSEY always ahead

Privacy Policy Construction

- List of categories of personal information that have been collected in last 12 months
  - Sources of each category
  - Purpose for collecting each category
- List of categories sold in last 12 months
- List of categories disclosed for a business purpose in last 12 months

DORSEY™ always ahead

Privacy Policy Construction

Placement/Format of Lists Granularity of Categories

DORSEY™ always ahead

Reasonable Security Measures

"Any consumer [whose personal data was breached] 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 for any of the following:

(A) To recover damages in an amount 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…"

DORSEY™ always ahead

Reasonable Security Measures

Assessing Security

DORSEY™ always ahead

Vendor Agreements

If a company intends to share personal information with a vendor, it must include specific contractual provisions, which may include:

- **Prohibition on vendor retaining, using, or disclosing the personal information for any purpose other than that of the contract**
- **Prohibition on selling the personal information**
- **Prohibition on retaining, using, or disclosing the information outside the direct business relationship**
- **"Certification" that vendor understands restrictions and will comply**

Vendor Agreements

Contract Review Process GDPR Article 28 Enough?

Takeaways

1) Verify requests - don't create data breaches
2) GDPR efforts are likely not enough
3) Assess your security program
4) Get started now

DORSEY™ always ahead

DORSEY
always ahead

Way of the Resilient – Achieving CCPA Readiness

Jamie Nafziger, *Partner and Chair, Cybersecurity, Privacy & Social Media Group, Dorsey & Whitney LLP*

Cody Wamsley, *CISSP, Associate, Dorsey & Whitney LLP*

Michael Schell, *Director of Strategic Accounts & Channels – U.S., EdgeScan*

Robert Cattanach, *Partner, Dorsey & Whitney LLP*

September 17, 2019

Speakers

Jamie Nafziger

Cody Wamsley

Michael Schell

Robert Cattanach

DORSEY
always ahead

California Consumer Privacy Act of 2018

- **Applies to businesses that collect personal information of California residents and:**
  - **Exceed $25 million in annual gross revenue, or**
  - **Buy, receive, sell, or share (for commercial purposes) personal information of 50,000 or more consumers, households, or devices per year, or**
  - **Derive at least 50% of annual revenue through sharing of personal consumer information**
  - **CCPA also applies to entities that control or are controlled by such businesses, and share common name, service mark, or trademark**
- **Broad definition of "sell" that includes share**
- **Broad definition of personal information**
- **Effective January 1, 2020**

DORSEY™ always ahead

Risk-Based Approach – To Do List

Security operations improvements in anticipation of class actions	Security policies and execution	Opt-out/opt-in planning (buttons, separate websites/apps)
Children under 16	Data mapping	Update privacy policy for website/apps; include Nevada

DORSEY™ always ahead

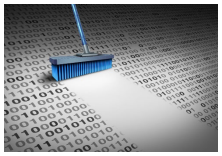
Risk-Based Approach – To Do List (Part 2)

Employee privacy policy	Vendor agreements	Plan/develop technology and procedures re access requests
Plan/develop technology and procedures re deletion requests	Employee/contractor training	Cyber insurance review

DORSEY™ always ahead

Challenges - But Methodical Approach can Overcome

- **Security challenges**
- **Different rights of users from different states**
- **Data is everywhere**
- **Average website/app has many more trackers than in past (more diligence; more contracts)**
  - **Mobile trackers**
  - **App software development kits (SDKs); aggregators of SDKs**
- **CCPA and implementing regulations still evolving**



DORSEY™ always ahead

Tip: Business Purpose Exception

- "Selling" means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration"
- Business purpose exception
  - Not selling - business uses or shares with service provider personal information of consumer necessary to perform business purpose
- Advantage
  - Avoid opt-out (Do Not Sell My Personal Information)
- Requirements
  - One of seven activities listed in CCPA 1798.140(d)
  - Notice (privacy policy)
  - Service provider does not further collect, sell, or use personal information except as necessary to perform business purpose (data processing agreement)

DORSEY always ahead

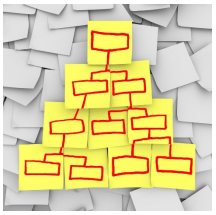
Tip: Do you Really Need that Birthdate?

- Age 13-16: right to opt-in to "selling" rather than opt-out
  - Technologically complex
- Under age 13: need parents/guardians to opt-in and to comply with COPPA
- Actual knowledge that consumer less than 16
- Willfully disregards = actual knowledge
- Avoid collecting birthdate (year) unless absolutely necessary

DORSEY always ahead

Tip: Affiliates

- "Business" includes entities that
  - control or are controlled by business; and
  - share common name, service mark or trademark
- Risk that affiliate sharing beyond above may be "selling"
  - Subject to opt-out
  - Parent/sub vs. sister
- Review org chart, branding, and data sharing between affiliates to identify issues



DORSEY always ahead

Tip: GDPR Data Subject Requests – Coming to America

- Many companies in EU overwhelmed with requests
- Disgruntled former employees
- Scams/Spam
- Litigation "discovery"
- Testers
- Third party requesters
- Responding time-consuming and costly
- Technology, planning, team readiness

DORSEY always ahead

Reasonable Security

Failure to implement "reasonable security procedures and practices" results in statutory damages of:

$100-750 PER CONSUMER PER INCIDENT

DORSEY always ahead

Reasonable Security

"The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

- Kamala Harris, as California Attorney General in 2016

DORSEY always ahead

CSC 20

1) Inventory and Control of Hardware Assets
2) Inventory and Control of Software Assets
3) Continuous Vulnerability Management
4) Controlled Use of Administrative Privileges
5) Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6) Maintenance, Monitoring and Analysis of Audit Logs
7) Email and Web Browser Protections
8) Malware Defenses
9) Limitation and Control of Network Ports, Protocols and Services
10) Data Recovery Capabilities
11) Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12) Boundary Defense
13) Data Protection
14) Controlled Access Based on the Need to Know
15) Wireless Access Control
16) Account Monitoring and Control
17) Implement a Security Awareness and Training Program
18) Application Software Security
19) Incident Response and Management
20) Penetration Tests and Red Team Exercises

DORSEY™ always ahead

Reasonable Security, generally

- Written Information Security Policy
  - Segregation of duties & least privilege
  - Retention policies for logs, audits, etc.
  - Consequences for violating WISP
  - Patch management
  - Data disposal/deletion policies
- Follow industry standards (ISO 27001, NIST 800-53, etc.)
- Incident Response Plan
- Change Management Controls
- Encryption Standards
- Vulnerability Management
- Audit/Certification Processes (SOC2)
- Security Awareness Training
- Vendor Management

DORSEY™ always ahead

Reasonable Security, generally

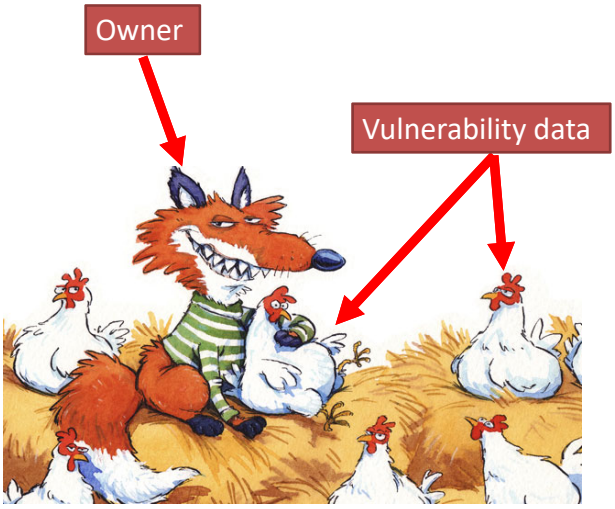
CCPA Basic Assessment	CCPA Basic+	CCPA Readiness
Limited scope assessment: • Provide client with self-assessment questionnaire for infosec & privacy processes • Meet with client to understand data flows and business justification for keeping data • External vulnerability assessment • Gap analysis memo	All items in CCPA Basic Assessment plus: • Limited evaluation of current infosec policies • Evaluation and creation of needed opt-in/opt-out processes • Website or app privacy policy • Authenticated vulnerability assessment • Data processing addendum language	All items in CCPA Basic+ plus: • Assessment of all written infosec policies • Validation of questionnaire • Evaluation of information security controls • Third party management • Incident response planning • Data subject processes • Employee policies • Vendor agreements • Insurance advice • etc.

DORSEY™ always ahead

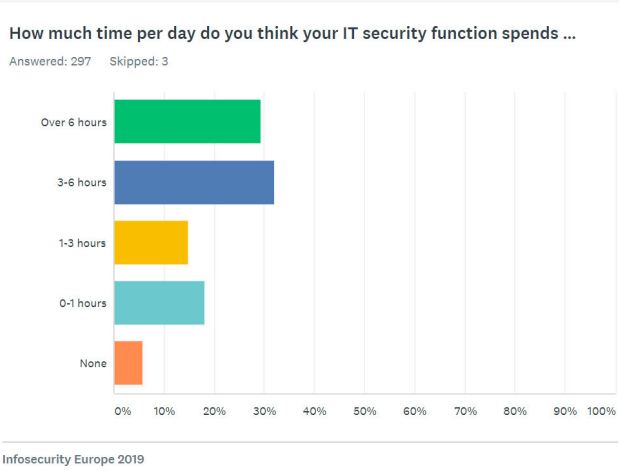
Hidden Costs

- false positives?
- staff burnout/fatigue?
- #fullstack?
- pentest costs?
- product training?
- Loss of trust?

1) Relationship between cyber and legal/compliance teams?
2) Cyber team's time/resources?
3) Trust your cyber teams?



InfoSec Europe 2019 – Survey Results



False Positives

More than 60% of security professionals estimate their security function spend over 3 hours per day validating false-positives. Nearly 30% are spending over 6 hours on this task. Most agree that it is too much and the time could be better utilised. For most, it is the part of their job they like least.

www.edgescan.com

@edgescan

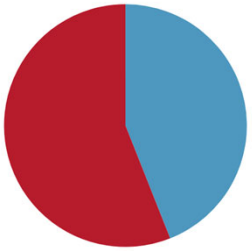
InfoSec Europe 2019 – Survey Results

edgescan

Personal Impact

Impact of false-positive on personal life.

Have you ever been pulled out of an important life event because of a security incident that turned out to be a false positive?



Shockingly, 129 of our respondents recall leaving an important life event to deal with a security alert, which, when verified, was determined to be a false-positive.

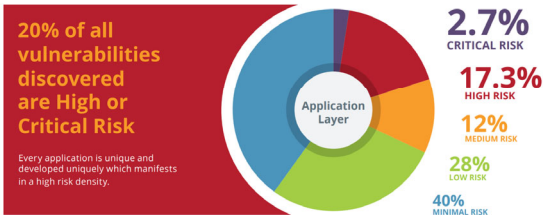
The Threat Is Real

edgescan

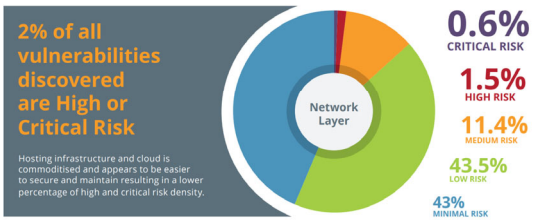
- **20%** of all web application vulnerabilities are a high or critical risk.
- **22%** of all discovered vulnerabilities (fullstack) are high or critical risk.
- **18%** of all vulnerabilities discovered (fullstack) in 2017 had a CVSS v2.0 score of 4.0 or more – a PCI compliance fail.
- **32%** of all vulnerabilities discovered in the web application layer has a CVSS v2.0 score of 4.0 or more. – a PCI compliance fail.

See: 2018 edgescan Stats Report

APPLICATION LAYER RISK DENSITY



NETWORK LAYER RISK DENSITY



Assessment Reporting and Mitigation.

Weaver
- High volume scanner orchestration platform.
- Scan configuration and monitoring
- Scoping and exclusion management
- Automation & scheduling interface
- Integration into the edgescan platform

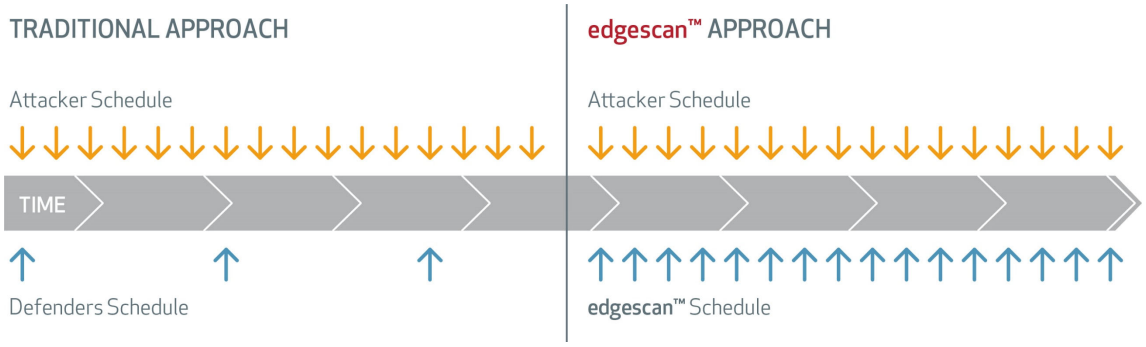
Weasel
- Web application scanner.
- One-Page site capability - Single Page applications.
- JavaScript parsing capability via headless browser.
- Integration into edgescan platform.
- Distributed architecture –scalability.
- Highly configurable and granular.
- Intelligent scope definition

Mapper
- Continuous Asset profiling
- Distributed scalable architecture
- Multi-region deployment
- DNS resolution
- Service Fingerprinting / OS identification
- AWS API for asset identification*

PCI Reporting Engine
- Dynamic Attestation reporting.
- Intelligent conditional logic compliant with ASV.

WAF Integration
- Netscalar
- Mod_security
- F5

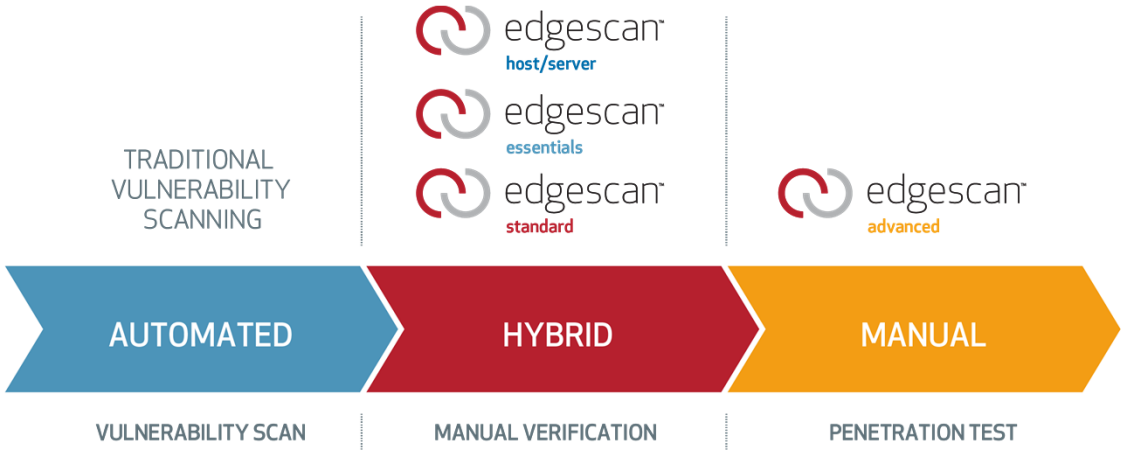
edgescan™ Approach



Detecting Vulnerabilities with Expertise

edgescan

edgescan's approach to cyber security can be compared in the following way:



Leading #FullStack Vulnerability Management

edgescan

Continuous Asset Profiling:

edgescan™ H.I.D.E (Host Index Discovery & Enumeration) is a feature for all edgescan licenses. With fast network host discovery and asynchronous port scanning to help you identify and monitor assets and network changes.

H.I.D.E supports service and OS detection and can generate alerts based on what you need to know.

Web Application Security Assessment:

Validated web application security assessments on demand when you want them and scheduled as often as you need them.

Recording of risk, trending and metrics on a continuous basis, all available via our rich dashboard for superior security intelligence.

Host/Server Security Assessment:

Server Vulnerability Assessment covering over 90,000 CVE's. Designed to help ensure your deployment be it in the cloud or on premise is secure and configured securely.

All vulnerabilities are validated and risk rated by experts and available via the dashboard to track and report on when required.

PCI ASV Compliance:

edgescan™ is an PCI Approved Scanning Vendor (ASV) and exceeds requirements of the PCI DSS by providing continuous, verified vulnerability assessments for both internal , public Internet facing websites and hosting environments.

edgescan™ Advanced includes business logic and penetration testing required by the PCI DSS standard.

Web Application Firewall (WAF) Integration

edgescan™ integration with Web application firewalls (WAFs) supports the creation of virtual patches to fix vulnerabilities while providing the reports needed to pass auditor inspections.

Open API:

edgescan™ is built to provide up to date vulnerability intelligence to the enterprise. The Open API allows easy integration to existing and new business systems for a complete view of cyber risk and web security posture.

The edgescan™ API enables increased automation and interoperability within the key security metrics of established enterprise information security programmes.

Thank You!

- **Stay tuned**
  - **Governor has until October 13 to sign amendments**
  - **California AG draft regulatory guidance expected this fall**
- **Monthly eUpdates for clients**
- **Many thanks to our guest speakers**
- **Please join us for reception!**

- Nafziger.Jamie@Dorsey.com
- Wamsley.Cody@Dorsey.com
- Cattanach.Robert@Dorsey.com

September 16, 2019

Breathing Room? California Legislature Passes Two Major Amendments to California Consumer Privacy Act (CCPA)

Jamie Nafziger and Divya Gupta

Businesses may receive a bit of breathing room as a result of two amendments to the California Consumer Privacy Act (CCPA) passed on Friday, September 13, 2019, by the California Legislature. The Legislature gave businesses a one-year moratorium on two significant aspects of the law: its application to employees, job applicants, owners, officers, directors, medical staff members, and contractors; and its application to business-to-business transactions. The Governor has until October 13, 2019, to sign or reject the amendments. Although the amendments provide some of the needed clarifications and error corrections and a significant break from needing to respond to certain data subject requests from employees and B2B contacts, businesses will still need to complete their data mapping (even for these categories of consumers) and will still need to be prepared to offer the rights not exempted on January 1, 2020, even if these amendments are signed by the Governor.

For those following the process, five bills passed the Legislature: AB 25, AB 874, AB 1146, AB 1355, and AB 1564. Proposed amendment AB 846 on loyalty programs was shelved. In addition to the two widely applicable amendments about employees and business-to-business transactions discussed in detail below, the Legislature also passed a number of minor or narrowly applicable amendments. The amendments amount to 98 pages of printed material. We will cover only the more significant of them in this article.

The employment-related amendments in AB 25 exempt businesses from many of the CCPA's requirements for one year when applied to employees, job applicants, owners, officers, directors, medical staff members, and contractors "to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business" (emphasis added). The amendment also covers certain use of personal information in the context of emergency contact information and benefits administration.

If AB 25 is signed by the Governor, two CCPA requirements will still apply to these types of individuals when collected and used in this context: (1) the requirements to inform them about the categories of personal information collected and the purposes for which the personal information will be used in 1798.100(b) and (2) the right to sue in a private right of action after a data breach in 1798.150. This would mean the other consumer rights to deletion, access, opt-out of selling, and no price discrimination would not apply in this context for one year (until January 1, 2021). This will be a welcome change to most businesses, to the extent it gives them a break from the experience EU businesses have had responding to data subject requests from employees, ex-employees and job applicants in Europe since the General Data Protection Regulation (GDPR) became effective. Unfortunately, even if this amendment becomes law, businesses will still need to complete their data mapping and draft disclosures in connection with the information of employees, job applicants, owners, officers, directors, medical staff members, and contractors.

The business-to-business (B2B) moratorium in AB 1355 would exempt businesses from many of the CCPA's requirements for one year when applied to "personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or

government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency" (emphasis added).

The B2B moratorium would not apply to collection or use of personal information outside of the context described in this amendment, to the right to opt-out of "selling" in 1798.120, to the price discrimination provisions of 1798.125, or to the right to sue in a private right of action after a data breach in 1798.150. If this amendment is signed into law, businesses will have a break until January 1, 2021, in the requirements of notice, deletion, access, information about onward disclosures, the opt-out link and the means for exercising consumer rights when it comes to B2B diligence or product/service provision or receipt. This means businesses would still need to complete their data inventories of information received in a B2B context, be prepared to respond to opt-out requests, and apply all other sections of the CCPA to uses of B2B personal information outside of the diligence or transaction itself (such as marketing uses).

Other important amendments include:

- Clarifications regarding authentication of data subject requests in AB 25;
- Changes to language regarding methods for submitting data subject requests in AB 1564;
- Changes to exempt certain vehicle-related information from the right to opt-out from selling in AB 1146;
- Changes to exempt certain warranty and product recall information from the right to deletion in AB 1146;
- Changes to the definition of "personal information" in connection with the reasonability of associating information with a particular consumer or household, with the definition of "publicly available," and with the applicability to deidentified or aggregate consumer information in AB 874;
- Correction of errors in the price discrimination section 1798.120 about "value provided to the consumer" versus "value provided to the business" in AB 1355;
- Clarification regarding impact of encrypting and redacting personal information on civil right of action in AB 1355;
- Changes to the exemption regarding consumer credit and related information in AB 1355; and
- Error corrections in 1798.110(c) regarding privacy notice requirements and in 1798.115(a)(2) regarding right to know in AB 1355.

If these amendments are signed by Governor Newsom by October 13, 2019, they will provide a one-year extension in connection with some provisions of the CCPA. However, the majority of the provisions related to consumer privacy will still be in effect. No fundamental rights have been removed from the CCPA. Businesses will need to continue their compliance efforts with focused intensity over the next several months. We will provide updates regarding the Governor's actions and the California Attorney General's regulatory guidance as they become available.

The completed legislative session gives businesses a clearer understanding of the CCPA's obligations (subject of course to signature by Governor Newsom). For those companies not previously required to comply with the European Union's GDPR, this may pose significant operational and technical challenges. Dorsey has developed fixed fee packages to help clients on their CCPA compliance journey, a simple screening tool (**https://www.dorsey.com/services/ccpa**) which is publicly available to help companies understand whether the CCPA affects them, and a more comprehensive online self-assessment tool for our clients, which can be requested by emailing Dorsey at **CCPA.Assessment@dorsey.com**.

September 12, 2019

CCPA Requires "Reasonable Security": But You Can't have Reasonable Security Without Proper Vulnerability Management

Divya Gupta and Cody Wamsley, CISSP

With the California Consumer Privacy Act ("CCPA") set to take effect on January 1, 2020, and the resulting looming specter of statutory damages and data breach class action litigation for failure to implement "reasonable security" on the near horizon, reducing or mitigating the harms that result from such cyber-attacks is more important than ever. Since 2015, more than three in five Californians have been a victim of a data breach, making implementation of reasonable security controls now a critical and necessary component of CCPA compliance.[1] While the retail industry has had record breaking breaches from malware and hacking, especially with card data, no industry is risk free when it comes to adequate data security.

Managing or mitigating risk, however, requires implementing "reasonable security," which derives from the Center for Internet Security's Top 20 Critical Security Controls (CSC 20) per then California Attorney General in 2016, Kamala Harris. In California's 2016 Data Breach Report, Harris stated that "[The CSC 20] are the priority actions that should be taken as the starting point of a comprehensive program to provide reasonable security."[2] Recommendation 1 of the same report is more explicit:

> The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. **The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.** (emphasis added).

Based on these statements, the CSC 20 likely comprise a defensive list to detect, prevent, respond to, and mitigate security incidents, and are designed to address various domains of information security to provide organizations with a roadmap to achieve resiliency. Whether the CSC 20 will become the explicit standard for "reasonable security" is still an open question, but given the California AG's previous statements, these controls should be top-of-mind for any organization that seeks to avoid significant liability under the CCPA.

---

1 See California's 2016 Data Breach Report, available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

2 https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

The CSC 20 is broken down into three main categories of controls: Basic, Foundational, and Organizational. The total scope of the CSC 20 is beyond the scope of this article, but suffice it to say that an organization may be hard-pressed to assert that it has "reasonable security" in place if it does not at least adhere to the Basic controls. The Basic controls consist of the following six items:

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Of these six Basic controls, #3, Continuous Vulnerability Management, stands out as one of the most important for an organization to focus on to prevent data breaches. According to a recent study, nearly 60% of recent data breaches were the result of unpatched vulnerabilities.[3] Indeed, the California AG stated that "patching newly discovered security vulnerabilities is critical" while citing the related CSC 20 control. In the last few years, the importance of vulnerability management has become more apparent and this control has risen to become the #3 control in the CSC 20.

Vulnerability management's main purpose is to identify and remedy software vulnerabilities as quickly as possible. It often doesn't take any significant skill on an attacker's part to exploit published vulnerabilities and so once a software vendor releases a patch, knowledge of its associated vulnerability quickly becomes widespread and the race is on between organizations deploying patches and attackers attempting to exploit the vulnerability. Organizations that do not scan for and proactively address vulnerabilities are at great risk for a breach.

Patching software security is a no-brainer, or so you'd think. Well, the challenge lies in the scale of the organization, the effect a patch could have on other organization systems, and the attacker's ability to quickly weaponize ahead of scheduled patch rollouts, among other things. To properly implement vulnerability management may not be as easy as we'd like, but it is critical and low-hanging fruit on the CSC 20 tree.

The European Union deems privacy a fundamental human right, and is taking enforcement seriously -- think Marriott and British Airways GDPR fines. We expect to see similar, if not greater, liability for organizations that violate the upcoming CCPA. Organizations that haven't yet automated the process to monitor for and remediate vulnerabilities on networks and systems should do so now and should institute vulnerability and patch management policies. While all of the CSC 20 controls are important, perhaps the most effective solution to prevent a major data breach for any organization lies in assessing and managing known vulnerabilities. Modernizing

---

3 https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465.

vulnerability management programs should be a focus in the short term run up to January 1, 2020 effective date.

Dorsey's Cybersecurity and Privacy Team has developed a catalog of security practices and procedures to help achieve operational resilience and defend companies from the forthcoming wave of data breach litigation. Notably, Dorsey has partnered with leading technical security industry organizations to offer full service advice.[4]

Additional references:

https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180

---

4 https://www.dorsey.com/services/cybersecurity-privacy-social-media.

June 28, 2019

National Financial Institutions—Developing A Project Plan To Comply With The California Consumer Privacy Act

Joseph Lynyak, Tom Scanlon and Erin Bryan

Since its adoption last year, U.S. financial institutions have been confronted with the challenge of planning their compliance with the California Consumer Privacy Act (the "CCPA")[1]. The CCPA becomes effective in two stages—January 1, 2020 and July 1, 2020 (or possibly sooner depending upon the date the California Attorney General adopts implementing regulations).[2]

Regrettably, considerable confusion exists within the financial industry about the scope of the CCPA and the obligations it imposes on financial institutions.

In an effort to provide our financial intermediary clients and friends with a workable summary of a financial institution's obligations—and in particular for financial institutions that do not have a physical presence in California—this Alert is intended to assist in identifying coverage considerations, and provide a practical approach to the development of a project plan that will demonstrate reasonable compliance with the CCPA's admittedly ambiguous set of requirements and obligations.

What obligations does the CCPA impose on a covered business?

The CCPA requires that a covered business respond to newly enacted privacy rights for a California resident, which includes the rights to:

- Know what categories of "personal information" or "PI" is being collected;
- Know whether personal information is sold or disclosed and to whom;
- Say "no" to the sale or disclosure of personal information, and to require a covered business to delete PI; and
- Receive equal service and price, whether or not privacy rights under the CCPA are exercised.

1 Cal. Civ. Code § 1798.100 et. seq.

2 Cal. Civ. Code § 1798.185.

The CCPA creates a complicated set of procedural and substantive requirements on the part of a covered company. For example, a covered business must be capable of responding to a "verified consumer request" for personal information, provide a summary of categories of PI that are collected about a California resident, state whether PI is sold or transferred to third parties, and delete information at the direction of the California resident (similar to the right to be forgotten under the EU's General Data Protection Regulation).[3]

Is a financial institution a covered business under the CCPA?

Two distinct questions should be asked to determine whether a financial institution could be subject to the requirements of the CCPA: (1) does the financial institution qualify as a "business" covered by the CCPA; and (2) to what extent may a covered financial institution take advantage of one or more of the exemptions, including the exemption for its treatment of PI pursuant to Title V of the federal Gramm-Leach-Bliley Act ("GLBA") or the California Financial Information Privacy Act ("CFIPA") (which we refer to collectively as the "GLBA Exemption").[4]

The CCPA broadly defines the term "business" to include various entities, including a corporation, partnership, limited liability company or similar entity, "that is organized or operated for the profit or financial benefit of its shareholders or other owners." However, a covered business also must "[do] business in the State of California" and meet one or more of the following thresholds: (A) have an annual revenue (currently interpreted to be global revenue) of $25,000,000; (B) engage in commercial activities involving the collection, sale, or disclosure of "the personal information of 50,000 or more consumers, households, or devices;" or (C) "[d]erive 50 percent or more of its annual revenues from selling consumers' personal information." Even though the conditions and thresholds appear to target larger or data-rich companies, the definition of a "business" will subject most national financial institutions to the facially broad coverage of the CCPA.[5]

Second, the GLBA Exemption may afford a financial institution partial relief from certain requirements of the CCPA. Commercial banks, savings banks, mortgage companies, loan servicers, data aggregators, and others generally qualify as a type of "financial institution" that is engaged in collecting, processing, selling, or disclosing PI "pursuant to" the GLBA (and the CFPB's implementing Regulation P[6]) or the CFIPA. The scope of the partial GLBA Exemption is important for purposes of developing an effective compliance plan, and will be discussed in greater detail below.

---

3 Cal. Civ. Code § 1798.105 to 1798.125.

4 15 U.S.C. § 6801 et seq.; Cal. Fin. Code § 4050 et seq.

5 Cal. Civ. Code § 1798.140(c). It should be noted that California takes an expansive view of what constitutes "doing business" for purposes of the CCPA and other statutes intended to protect its citizens. Specifically, dealing with a California resident using the internet and commercial webpages will likely constitute doing business for purposes of the CCPA.

6 12 C.F.R. § 1016.1 et seq.

To what extent might the GLBA Exemption reduce a financial institution's compliance obligations under the CCPA?

Unfortunately for the financial industry, the GLBA Exemption leaves financial institutions exposed to a number of compliance risks under the CCPA. After the CCPA was enacted, the GLBA Exemption was hurriedly added at the very end of the 2018 California legislative session. The GLBA Exemption states:

> This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.[7]

By its terms, the CCPA's GLBA Exemption only exempted PI—meaning the data itself—from coverage under the CCPA, but not the financial institution holding the data. Further, notwithstanding the exemption, liability for data breaches of a limited range of a California resident's data remains subject to the CCPA's private right to recover statutory damages.[8]

How do the CCPA, the GLBA and the CFIPA fit together?

This interplay among and between the CCPA, the CFIPA and the GLBA has created an interpretative quagmire for covered financial institutions attempting to determine the scope of their compliance responsibilities. On one hand, some industry stakeholders have argued that the GLBA Exemption excludes PI from virtually all requirements under the CCPA, while others have advocated that the exemption is very limited in scope, and specifically does not exclude financial institutions from obligations established by the CCPA that are not similar to those in the GLBA and the CFIPA.

The compliance risk for financial institutions

As a starting point in the analysis, we look at the interplay between the CFIPA and the GLBA. When initially adopted by the California Legislature in 2003 (and effective in 2004), it was clear that the CFIPA was an attempt to create substantially equal privacy rights under California law as were created by the GLBA. However, the CFIPA was more extensive than the GLBA in that, rather than providing a California consumer with the right to "opt-out" from covered data being sold or transferred to a non-affiliated party (which was the approach adopted by the GLBA), the CFIPA required that covered financial institutions obtain an affirmative opt-in consent from a California consumer prior to sharing or transferring data to third parties. Importantly, because Section 524 of the GLBA contains a "reverse preemption" provision that provides that state law privacy rights trump privacy rights as contained in the GLBA, for years covered financial institutions have provided the more extensive California-based privacy rights contained in the CFIPA rather than the more limited privacy rights as contained in the GLBA.[9]

---

7 Cal. Civ. Code § 1798.145(e).

8 Id.

9 15 U.S.C. § 6807.

It is important to understand that both the GLBA and the CFIPA are primarily disclosure statutes, and impose no substantive obligations on a covered financial institution beyond the opt-out and opt-in rights exercised by a California consumer, discussed above. Neither statute limits the amount or content of information that may be collected by a covered financial institution, including responding to consumer requests for information following the delivery of required disclosures.[10]

Given the limited nature of the GLBA Exemption—and its interplay with the CFIPA—the disclosure scheme as contemplated by those statutes (including Regulation P) arguably may control initial disclosures required to be delivered (as specified by the CFIPA and the GLBA), but may not exempt a financial institution from responding to a "verified consumer request" for PI whether or not the data was originally disclosed in accordance with the GLBA (as modified by the opt-in requirements of the CFIPA).

Planning for compliance

A careful reading of the CCPA's GLBA Exemption indicates that, subsequent to the delivery of initial account disclosures, the GLBA Exemption may be of limited value in real-world communications between a covered financial institution and California residents exercising their privacy rights pursuant to Sections 1798.100 through 1798.125 of the CCPA. Importantly, both the GLBA and the CFIPA contain data definitions that are narrower than the expansive definitions of PI contained in the CCPA. Also, the GLBA and the CFIPA are generally limited to consumers opening accounts with a covered financial institution, whereas the exercise of a consumer's privacy rights under the CCPA is not limited by the establishment of an account relationship. Further, the CCPA's definition of a "consumer" extends to a California resident, whereas the GLBA's and the CFIPA's disclosure requirements are limited to the traditional concept of data obtained as part of a "consumer purpose" relationship (*i.e.*, for personal, household or family purposes).

Unless the California Attorney General elects to clarify the coverage question created by the GLBA Exemption discussed above, covered financial companies may have no choice but to comply with all requirements of a covered business under the CCPA (with the possible exception of continuing to employ GLBA- and CFIPA-compliant disclosures). Failing to adopt a narrow view of the scope of the CCPA's GLBA Exemption may jeopardize the structuring of an effective compliance program by the deadlines established by the CCPA in 2020.

What must be included in a project plan to comply with the CCPA?

In order to comply with the extremely short time frames required by the CCPA, we suggest that several components should be considered, as follows:

Essential plan elements

There are two essential elements that should be included in any CCPA project plan. The first is data mapping to identify systems of records that contain PI covered by the CCPA. Anecdotal reports from national financial institutions—particularly those who did not engage in data mapping in order to comply with the GDPR—indicate significant operational difficulties being

---

10 See generally, 289 Cal. Fin. Code §§ 4050, et seq.; 6 CFR § 313.1 et seq. (15 U.S.C. § 6801 et seq.).

experienced to both identify data systems and develop methodologies to capture and to retrieve covered data to respond to a verified consumer request. Stated another way, data mapping should begin as soon as possible.

The second element is perhaps the most important risk mitigation step that a covered financial institution can take to avoid liability. The CCPA allows for the recovery of statutory damages for specified data breaches by private parties (including class action liability for breaches involving multiple California residents). Statutory damages range from $100 per incident to $750 per individual breach.[11] According to the statutory liability provision of the CCPA, the only defense to statutory damages is a showing that a covered company had in place reasonable data security measures for the PI it held in its systems.[12] Liability for statutory damages for specified data breaches commences as of January 1, 2020, regardless of whether the California Attorney General issues implementing regulations after that date.[13]

Accordingly, as an essential element of a project plan, a covered financial institution should be prepared to demonstrate that its data security measures are reasonable, based upon industry standards, and have been regularly confirmed by internal and external audits.

General project plan elements

In addition to the two essential components of a financial institution's project plan, discussed above, the following implementation tasks may likely be required to be included in a CCPA project plan, and include:

- Identifying data constituting PI
- Determining the applicability of full or partial exemptions from data use and retention
- Determining the scope of the GLBA Exemption for data, discussed above
- Determining the methodologies for receiving and responding to a verifiable consumer request
- Designing and building internal call centers/response teams
- Amending disclosures of privacy policies
- Modifying website(s)
- Adopting methodologies to implement "opt-out" and "opt-in" elections and deletion of PI

---

11 Cal. Civ. Code § 1798.150(a)(1)(A). Although the categories of PI that are covered by the CCPA's statutory damages provisions is narrower than the entire definition of PI, it includes personal identifiers that are commonly part of a data breach.

12 Cal. Civ. Code § 1798. 150(a)(1)(C)(2).

13 Cal. Civ. Code § 1798.198(a).

- Reviewing and modifying agreements with third parties and vendors
- Drafting internal policies and procedures
- Establishing training programs

A recommended implementation approach—evolving compliance

We note that several commentators and vendors have advocated engaging in an implementation program that is extraordinarily complex and (in our view) not capable of being completed within the CCPA's time limitations. Importantly, the patent ambiguities in regard to a covered financial institution's compliance obligations require that a financial institution establish its own compliance goals and response measures while interpretative guidance is being developed and eventually becomes available.

As a practical matter, lending and account relationships may form the basis for most data requests made by a California resident to a covered financial institution, which may constitute an initial starting point for responding to CCPA inquiries. Similarly, a financial institution may have to determine the degree of information included in a response, and may have to implement an evolving degree of data inquiries as the Attorney General refines the question of reasonable compliance.[14]

In sum, until the matter is clarified, financial institutions should be wary of overreliance on a broad reading of the partial GLBA Exemption. To do so may result in the development of an implementation plan that is deficient in regard to reasonable scope and content.

Please note that the analysis set forth in this Alert is not intended to be a comprehensive discussion of the obligations that are contained in the CCPA; California-licensed lawyers at Dorsey have been closely following CCPA legislative and regulatory developments, and are available to discuss the same.

---

14 One of the significant compliance challenges presented is the degree of specificity of PI that must be provided to a California resident when responding to a verifiable consumer request. See, Cal. Civ. Code § 1798.110(c)(5).

June 7, 2019

Nevada's New Privacy Law – Beating California in the Backstretch

Jamie Nafziger

Just as companies are reaching the straightway in their efforts to get ready to comply with the California Consumer Privacy Act ("CCPA") by January 1, Nevada has burst ahead with a privacy law that will take effect before the CCPA. On May 29, 2019, Nevada Governor Steve Sisolak signed SB 220 into law, amending Nevada's existing law that requires an operator of an Internet website or online service to provide a privacy notice to consumers detailing certain of the operator's privacy practices; SB 220 goes into effect on October 1, 2019.[1] SB 220 allows consumers to opt-out of operators of Internet websites and online services selling personally identifiable information to other entities for monetary consideration and will require both legal and operational changes for businesses. Operators, as defined by the law, must create a "designated request address" that allows consumers to submit requests prohibiting sale of information collected about the consumer, and operators must respond to the requests within 60 days.

SB 220 is a substantial amendment to Nevada's existing privacy law, and presents a new challenge to industry in general. On its face, the law is narrower in scope than the CCPA, and includes narrower definitions of "consumer" and "sale," along with carving out exceptions for financial institutions covered by the Gramm-Leach-Bliley Act ("GLBA") and covered entities under the Health Insurance Portability and Accountability Act ("HIPPA"). Nonetheless, companies focusing on CCPA compliance must now shift resources to becoming compliant with SB 220.

---

1 See Nev. Rev. Stat. §603A.340. Under the provision, an operator must make available a notice that: (1) Identifies the categories of covered information that the operator collects through its Internet website or online service about consumers who use or visit the Internet website or online service and the categories of third parties with whom the operator may share such covered information; (2) Provides a description of the process, if any such process exists, for an individual consumer who uses or visits the Internet website or online service to review and request changes to any of his or her covered information that is collected through the Internet website or online service; (3) Describes the process by which the operator notifies consumers who use or visit the Internet website or online service of material changes to the notice required to be made available by this subsection; (4) Discloses whether a third party may collect covered information about an individual consumer's online activities over time and across different Internet websites or online services when the consumer uses the Internet website or online service of the operator; and (5) States the effective date of the notice.

SB 220 Requirements

SB 220 has four main requirements, but several key definitions and exclusions govern the law's application:

1. An "operator"[2] must establish a "designated request address"[3] through which a consumer may submit a "verified request"[4] directing the operator not to make any sale[5] of "covered information"[6] collected about the consumer.

2. The consumer can submit a verified request through the designated request address, at any time, directing an operator to not make any sale of covered information the operator has collected about the consumer.

---

2 SB 220 defines an "operator" as a person who: (1) Owns or operates an Internet website or online service for commercial purposes; (2) Collects and maintains covered information from consumers who reside in [Nevada] and use or visit the Internet website or online service; and (3) Purposefully directs its activities toward Nevada, consummates some transaction with Nevada or a resident thereof, purposefully avails itself of the privilege of conducting activities in Nevada, or otherwise engages in any activity that constitutes sufficient nexus with the State to satisfy the requirements of the United States Constitution. However, the following are not considered operators as defined by the law: (1) Some Third Parties: A third party that operates, hosts or manages an Internet website or online service on behalf of its owner or processes information on behalf of the owner of an Internet website or online service; (Financial Institutions as defined under the GLBA: A financial institution or an affiliate of a financial institution that is subject to the provisions of the GLBA, 15 U.S.C. §§ 6801 et seq., and the regulations adopted pursuant thereto; (3) Covered Entities under HIPPA: An entity that is subject to the provisions of the HIPPA, Public Law 104-191, as amended, and the regulations adopted pursuant thereto; or (4) Motor Vehicle Manufacturers or Repair People: A manufacturer of a motor vehicle or a person who repairs or services a motor vehicle who collects, generates, records, or stores covered information that is: (a) Retrieved from a motor vehicle in connection with a technology or service related to the motor vehicle; or (b) Provided by a consumer in connection with a subscription or registration for a technology or service related to the motor vehicle.

3 A "designated request address" is an "electronic mail address, toll-free telephone number or Internet website established by an operator through which a consumer may submit to an operator a verified request."

4 A "verified request" is a request that is (1) submitted by a consumer to an operator; and (2) for which an operator can reasonably verify the authenticity of the request and the identity of the consumer using commercially reasonable means.

5 "Sale" is defined as "the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons." The term "Sale" does not include: "(a) the disclosure of covered information by an operator to a person who processes the covered information on behalf of the operator; (b) the disclosure of covered information by an operator to a person with whom the consumer has a direct relationship for the purposes of providing a product or service requested by the consumer; (c) the disclosure of covered information by an operator to a person for purposes which are consistent with the reasonable expectations of a consumer considering the context in which the consumer provided the covered information to the operator; (d) the disclosure of covered information to a person who is an affiliate, as defined in Nev. Rev. Stat. §686A.620, of the operator; OR (e) the disclosure or transfer of covered information to a person as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the person assumes control of all or part of the assets of the operator."

6 The definition of "covered information" is narrower than comparable state laws, like the CCPA, and means "any one or more of the following items of personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator in an accessible form: (1) a first and last name; (2) a home or other physical address which includes the name of a street and the name of a city or town; (3) an electronic mail address; (4) a telephone number; (5) a social security number; (6) an identifier that allows a specific person to be contacted either physically or online; (7) any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable." Nev. Rev. Stat. §603A.320.

3. An operator that receives a verified request is prohibited from making any sale of any covered information the operator has collected or will collect about the consumer.

4. An operator must respond to a consumer's verified request within 60 days. The operator may extend the response period no more than 30 days if (a) the operator determines that such an extension is reasonably necessary; and (b) an operator that extends the response period notifies the consumer of such an extension.

The Nevada Attorney General has enforcement power over SB 220's provisions. If the Attorney General believes that an operator directly or indirectly violated SB 220, the Attorney General may seek a temporary or permanent injunction or seek to impose a civil penalty not to exceed $5,000 for each violation. Unlike the CCPA, SB 220 does not establish a private right of action against an operator.

Although some consumers may welcome greater opportunities to stop certain sharing of their personal information, businesses developing compliance programs will face a new hurdle from SB 220, with its differing definitions, exceptions, and requirements. Even companies that do not sell personally identifiable information for monetary consideration will need to create the request mechanism and respond to consumer requests and may be left feeling like Nevada has missed the break.

About Dorsey's California Consumer Privacy Act (CCPA) Practice

Coming into effect in 2020, the California Consumer Privacy Act will impose significant privacy requirements on any business conducting business in California or gathering data on California residents. Dorsey's expert privacy team has already begun to assist clients in developing their internal privacy practices and external privacy policies so that they will be ready for compliance on day 1 of the CCPA's term.

What is happening?

New privacy law governing collection, use, and sharing of personal information from California residents that includes massive financial risk for non-compliance. The CCPA includes extensive rights, including rights of access, opt-out, deletion, and anti-discrimination, among others, necessitating profound changes to corporate organization and technological infrastructure.

Who needs to comply?

Businesses that collect the personal information of California residents, and additionally either: (a) exceed $25 million in annual gross revenue, or (b) buy, receive, sell, or share (for commercial purposes) the personal information of 50,000 or more consumers, households, or devices per year, or (c) derive at least 50% of their annual revenue through sharing of personal consumer information. The CCPA also applies to entities that control or are controlled by such businesses, and share a common name, service mark, or trademark.

1. Businesses without a physical presence in California are not insulated from liability, so long as they are doing business in California. The standard is a lenient one, and the International Association of Privacy Professionals estimates that 500,000 U.S. companies are likely to come under the law's purview.

2. Importantly, the CCPA embraces both online and offline collection and sharing, and protects the personal information of not only California residents, but also employees of covered businesses.

When will the new law take effect?

January 1, 2020

What are the risks in connection with non-compliance?

1. Civil penalties of up to $2,500 for each unintentional violation and up to $7,500 for each intentional violation.

2. In the event of a data breach, private right of action (with potential for class action aggregation) compensable in the statutory amount of $100-$750 per incident, per consumer, or actual damages, whichever is greater.

What are the benefits of complying?

Freedom from potentially crippling financial penalties, increased attractiveness to business partners, and reputational currency in an age of increasing consumer distrust of covert data collection.

What do I need to do to comply?

Compliance will require significant business unit and information technology investment. Businesses will likely need to inventory current data collection, use, and sharing, make software changes to effect required opt-out and opt-in functionality, update privacy policies, and establish procedures to respond to requests for consumer and employee information, among other imperatives.

What should I do now?

With class actions with statutory damages available beginning January 1, 2020, we advise focusing on security first. Businesses should assess, strengthen, and document their data security regimes, working to develop written security policies and incident response plans, revise vendor agreements, evaluate insurance coverage, and adopt industry standards and frameworks. Next steps will address the other statutory requirements. With our compliance team of privacy and cybersecurity lawyers, Dorsey stands ready to help.

California Consumer Privacy Act (CCPA)

CCPA imposes **statutory damages of $100-$750/record** and may result in **class action liability**

In effect **January 1, 2020**

You must have **reasonable security** practices & procedures in place

Get ready with Dorsey's fixed-fee packages!

BASIC

- Security & Privacy Assessment Questionnaire
- External Vulnerability Assessment
- Gap Analysis

READY

- Complete Infosec Policies
- Build Processes
- Remediate Gaps
- Incident Response Plan
- Complete Readiness

BASIC+

- Everything in the Basic Package *plus*
- Evaluate Infosec Policies
- Opt-In / Opt-Out Processes
- Website or App Privacy Policy
- Contract Language
- Authenticated Vulnerability Assessment

About Dorsey's Cybersecurity, Privacy & Social Media Practice

In a world dependent on information technology, networked operations and mobile connections, businesses face an increasing array of cybersecurity and data privacy challenges. Dorsey offers a coordinated worldwide team that helps assess your data flows and guide compliance efforts. When a security incident occurs, Dorsey's team can respond immediately with a complete range of services to help you meet this challenge. Increasingly, privacy compliance is table stakes in vendor relationships and mergers and acquisitions. Dorsey helps its clients negotiate contracts, draft privacy and security policies, and consider privacy challenges raised by cutting-edge technologies.

Dorsey provides proactive planning and assessment of rapidly-evolving legal requirements and can handle cyber threats and incident response whether you are a Fortune 100 multinational company or a start-up. We stay on the forefront of evolving technologies, regulatory requirements, and industry best practices to provide you with comprehensive and practical legal solutions.

Biometrics

Emerging personal technologies are leveraging biometric data such as fingerprints, iris scanning, and facial recognition for authentication and cutting-edge service offerings. Dorsey's biometric experts assist clients in navigating emerging state and international privacy regulations and laws related to the collection and processing of biometric data to ensure that the deployment of these new technologies remains compliant with such legal protections. Dorsey's team also has the pulse on emerging biometrics such as behavioral biometrics and the most recent case law in class actions regarding use of biometric data in business.

Conducting Business in Compliance with Global Data Privacy Laws

Doing business internationally requires a global data privacy compliance program. Dorsey's offices in the US, Asia, and the EU work together to advise our clients on the increasingly important international data protection laws and regulations. Companies collecting, storing, and sharing personal information of their customers, users, or employees or transferring personal information across national borders rely on Dorsey to help navigate the technological and legal complexities of doing so.

With the EU's General Data Protection Regulation (GDPR) the EU's approach to data privacy and security expanded considerably. This involves not only an expansion of companies' obligations when they collect, store, and share personal data of people in the EU but also an expansion of the number of companies subject to these requirements. Any company doing business in any of the EU member states, whether or not it has any physical presence in the EU, should be aware of the obligations imposed by the GDPR. To comply with the GDPR's requirements, companies collecting, storing or sharing personal information need to review and

in many cases revise their internal data practices and privacy policies as well as their consent forms, contracts with vendors, and the information provided to employees and customers when personal information is collected. Companies should also review and potentially need to improve measures to assure the security of personal data and to be prepared to respond to a security incident even more rapidly than in the past.

Dorsey's Cybersecurity, Privacy and Social Media Practice Group has handled numerous types of GDPR and ePrivacy Directive-related advice and drafting, including:

- Data Processing Agreements and Addenda (DPA)
- Advising on Lawful Basis for Processing Data
- Privacy Statements
- Advising on Data Flows and Controls
- Security Policies
- Process Change Management
- Options for Obtaining User Consent When Required
- Preparing to and Responding to Data Subject Requests
- Vendor Management
- Contract Assessment
- Cookie Policies
- Cross-Border Data Transfer Options including Standard Contractual Clauses, Privacy Shield, and Binding Corporate Rules
- Advising on When Data Protection Officer (DPO) Required
- Monitoring Enforcement Activity and Guidance Released by European Data Protection Board (EDPB) and Member State Data Protection Authorities (DPAs)
- Records Retention Requirements and Restrictions
- Incident Response Plans
- Website Policies
- Third Party Security Management Program Development
- Advising on Email, Text and App-Based Marketing Restrictions and Requirements

GDPR

Dorsey provides a full suite of services related to GDPR compliance and leverages its international team of privacy lawyers to ensure that clients receive the most up-to-date guidance on this hot topic.

HIPAA

Clients that deal with personal health information face increasing burdens to ensure that this information is protected. Dorsey's expert health privacy team assists clients in navigating the sometimes complex requirements under HIPAA, including developing internal privacy practices, business associate agreements, incident response, and responding to OCR inquiries.

Incident Response

Dorsey's expert team handles all manner of security incidents and data breaches. Starting from the time an incident is first detected, Dorsey's incident response team steps in and acts as a "breach coach" to guide clients through the entire process from arranging for forensic investigation, composing and sending required notifications, to drafting any follow up regulatory responses – all under attorney-client privilege. Dorsey has developed a top-of-class incident response plan offering that leverages best project management practices to enable not only security teams, but all relevant stakeholders to quickly determine their roles and responsibilities in the heat of an incident.

Information Security Policies

Through its representation of a wide range of global clients, Dorsey has the experience and has a significant library of policies that it can custom tailor to any client requirements to meet emerging regulatory requirements or other best practices. Dorsey's team of information security experts can also assist clients with navigating audits and certifications.

Mergers and Acquisitions

Privacy and security have become key parts of M&A transactions, especially where the target company has collected personal information or where there is an intent to integrate disparate systems post acquisition. Dorsey's expert team regularly assists clients with conducting diligence on target companies and helping target companies navigate and prepare for diligence by acquiring companies.

NIST Cybersecurity Framework Menu

Dorsey has mapped a variety of its offerings to the NIST Cybersecurity Framework to enable clients to quickly assess how each offering fits into its own compliance and maturity objectives.

Proactive Steps to Protect Data

A coordinated data protection plan is the first critical step necessary to minimize the likelihood of theft or illegal use, expedite investigation if misuse occurs, mitigate the damages and maximize success in potential future litigation. Standards of corporate governance require that directors and executives understand the adequacy of cybersecurity measures and liability protections. Dorsey can help your business:

- Develop and implement critical data protection policies, procedures and response plans, including cybersecurity assessments, privacy policies, information security programs, identity theft protection programs, website and mobile apps terms of use, social networking policies and username protection
- Protect intellectual property (patents, copyrights, trademarks and trade secrets) across networks, websites, mobile apps and mobile devices
- Prepare and negotiate key agreements with employees and third parties for licensing, confidentiality, outsourcing and cloud computing

Responding to a Data Breach

Today's maxim is that there are two kinds of companies in cyberspace: "those that know they have been breached and those that don't." Dorsey's experienced team understands the challenging dynamics of breach responses. We can provide:

- An immediate response – literally within hours and even with incomplete and imperfect information – using:
  - Live links to breach notification laws in all 50 jurisdictions
  - Template notification letters to customers and Attorneys General, incorporating each state's content, timing and sequencing requirements
  - Experienced PCI and vendor relationship issues
- Internal investigations and immediate legal steps required to secure stolen information
- Prompt responses to infringers, scammers and cybersquatters

Technology Contracts

Dorsey's world-class Technology Commerce group has significant expertise in drafting and negotiating cutting edge technology contracts. From purchase and licensing terms, to specific privacy and data security requirements, our clients save time and costs by leveraging our expert team to get to the heart of the matter with each transaction.

Vendor Management

Third party risk is quickly becoming the hot button issue in information security and Dorsey's expert team draws on years of experience in developing full third party risk programs to assist clients in both building their own third party risk programs and responding to inquiries from prospective customers. Dorsey's clients are able to close deals faster by leveraging expert third party risk advice.

Website and App Privacy Policies

The importance of having a proper website and app privacy policy cannot be overstated. From enforcement actions in the United States by the FTC to a growing body of actions taken in Europe under the GDPR to preparing for Attorney General enforcement in California, website and app privacy policies have become a focal point of scrutiny for businesses' privacy practices. Dorsey leverages its unique technical talent to conduct top-of-class diligence for its clients to ensure that their website privacy policies will meet these emerging requirements.