SPOTLIGHT ON

FINTECH

How the New California and Nevada Privacy Laws Will Impact Data in Fintech

July 2019

orrick

Introductions

Heather Sussman

Global Co-Chair

Cyber, Privacy & Data Innovation

Barrie VanBrackle

Co-Leader

Fintech

David Curtis

Law Clerk

**Pending Admission to Washington State Bar*

Cyber, Privacy & Data Innovation

Agenda

- CCPA Applicability
- Key Compliance Obligations
  - Notice & Transparency
  - Data Subject Rights
  - “Do Not Sell” Requirements (incl. Nevada requirements)
  - Reasonable Security

orrick

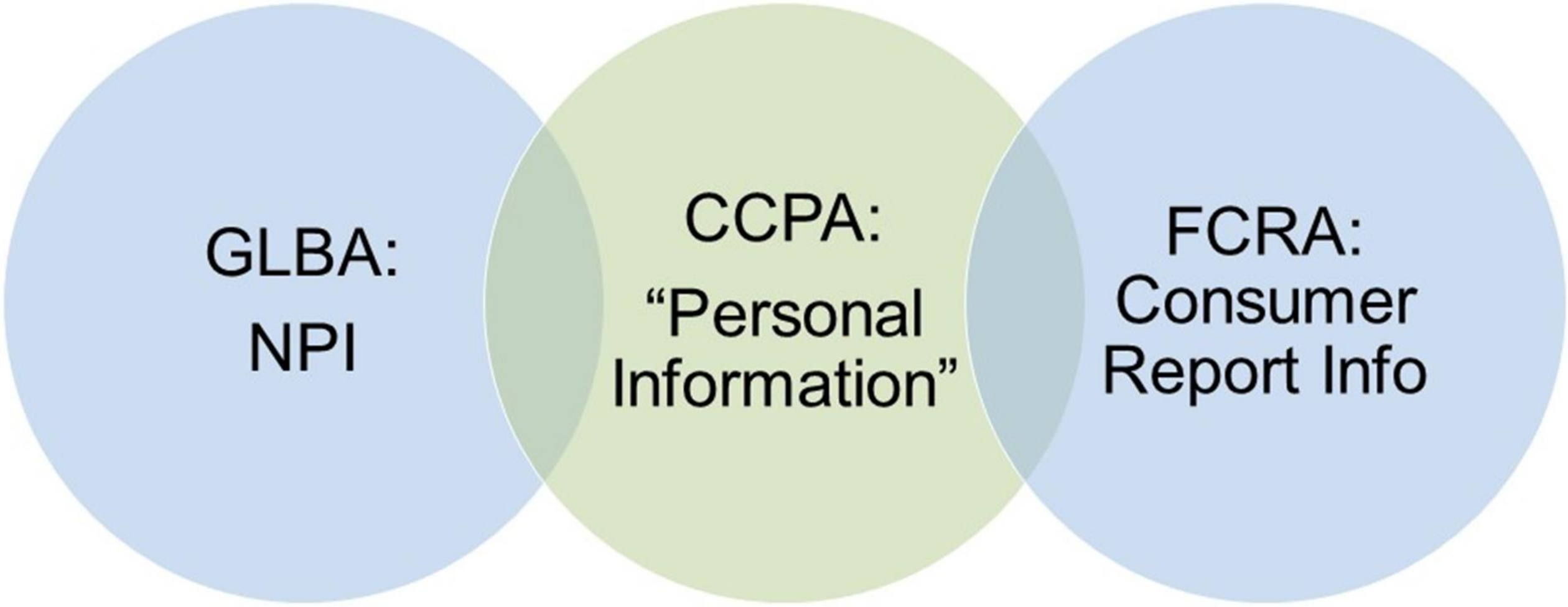
CCPA Applicability – "Business"

- The CCPA applies to any for-profit entity that:
  - Does business in California
  - Collects, receives, or accesses California residents' personal information
  - Decides **why and how** such personal information is used, AND
  - Satisfies at least one of the following criteria:
    - **$25 MM Revenue** – Has annual gross revenue over $25 million;
    - **Trades/Transfers Data** – Annually buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 consumers, households, or devices; or
    - **Data Broker** – Derives 50% or more of annual revenue from selling consumers' personal information
- The CCPA also applies to an entity that **controls** or **is controlled** by a covered business that shares **common branding**.

The CCPA does not apply to . . .

- The sale of PI to or from a consumer reporting agency if:
  - that information is to be reported in, or used to generate, a consumer report as defined by the Fair Credit Reporting Act (FCRA); **and**
  - use of that information is limited by FCRA.
- PI collected, processed, sold, or disclosed pursuant to:
  - the Gramm-Leach-Bliley Act (GLBA) and the California Financial Information Privacy Act (FIPA)
  - **BUT**: such PI can arguably serve as the basis of a private right of action under the CCPA in the event of a qualifying data breach
- Certain health-related PI and drivers' license PI processed pursuant to other federal statutes and regs (HIPAA, the Common Rule, CMIA, DPPA)

CCPA "Personal Information" – Gaps



CCPA "Personal Information" is Defined Broadly

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

THE USUAL SUSPECTS

- Name
- SSN
- Financial Information *(exc. GLBA)*
- Contact Information
- Signature
- Physical Characteristics
- Insurance Policy Number
- Other Gov't IDs
- Health Data *(exc. HIPAA)*
- Passport
- Driver's License

PROTECTED CLASSIFICATIONS

- Race
- Citizenship
- Color
- National Origin
- Military Status
- Religion
- Gender Identity and Expression
- Sex
- Medical Condition or Disability
- Marital Status
- Age
- Genetic Information

INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY

- Search History
- Browsing History
- Cookie Data
- IP Address
- Interest Data
- Online Interactions

BEHAVIORAL AND PROFILING DATA

- Tendencies
- Products/Services Considered
- Inferences
- Interest Data
- Order History
- Search History
- Purchase History

BIOMETRIC AND GEOLOCATION INFORMATION

SENSORY DATA

- Audio
- Electronic
- Visual
- Thermal
- Similar Information
- Olfactory

PROFESSIONAL, EMPLOYMENT AND EDUCATION-RELATED INFORMATION

GLBA NPI is Carved Out of the CCPA

- What is NPI (nonpublic personal information)? It includes:
  - PIFI (personally identifying financial information), which in turn includes:
    - Any information that You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer; and
  - A list derived from PIFI

- In other words, GLBA carveout to CCPA applies if:
  - **You** (Financial Institution)
  - Collect **NPI** (any info received from consumer in connection with providing a financial product or service to that consumer, or derived from such info).
  - From a **CA Consumer** (someone who obtains financial product or service from you to be used primarily for personal, family, or household purposes)

- *See, e.g.*, 12 C.F.R. § 1016.3

Key Compliance Obligations

1. Notice & Transparency
2. Data Subject Rights
3. “Do Not Sell” Requirements (incl. Nevada requirements)
4. Reasonable Security

Notice & Transparency – Required Disclosures

- A **Business** must update its privacy notice to **DISCLOSE**:
  - the categories of PI it collects, sells, and otherwise discloses for a business purpose;
  - the categories of sources of the PI;
  - the business or commercial purposes for collecting or selling the PI;
  - the categories of third parties with whom the business sells or otherwise discloses the PI; and
  - a description of the consumers' rights and the designated methods for submitting requests.

Important Note: Purpose Specification and Use Limitation (*See* 1798.100(b))

Effective: ***January 1, 2020*** *(+12 Month Lookback)*

Personal Information Inventory

Categories of PI Collected *Check all that apply*	Purposes for Collecting PI *How and why is PI collected?*	Categories of PI Disclosed *Check all that apply*	Purposes for Disclosing PI *How and why is PI disclosed?*
☒ Identifiers ☐ CA Customer Records ☐ Protected Classification Characteristics ☒ Commercial Info ☐ Biometric Info ☐ Internet/Network Info ☒ Geolocation Data ☐ Sensory Info ☐ Professional/ Employment Info ☐ Education Info ☐ Other PI ☐ Inferences	*We collect name, email, phone number, Ad IDs, transaction info and GPS location data using our mobile app in order to provide our services and target ads.*	☒ Identifiers ☐ CA Customer Records ☐ Protected Classification Characteristics ☐ Commercial Info ☐ Biometric Info ☐ Internet/Network Info ☒ Geolocation Data ☐ Sensory Info ☐ Professional/ Employment Info ☐ Education Info ☐ Other PI ☐ Inferences	*We share Ad IDs and GPS location with third parties who use this info for market research purposes.*

Data Subject Rights – Highlights

- Must **PROVIDE INFORMATION**:
  - requested by the consumer about the processing of that consumer's PI (tailored version of privacy policy disclosures)
- Must **PROVIDE ACCESS**:
  - to the PI collected over the past 12 months in a portable format w/in 45 days, in response to a "verifiable consumer request"
- Must **DELETE**:
  - PI upon a "verifiable consumer request" (and direct "service providers" to delete), subject to exceptions
- Right to **OPT OUT**:
  - of the "sale" of PI (more on this in a few slides)

Effective: ***January 1, 2020*** *(+12 Month Lookback)*

Consumer Request Protocols

CCPA CONSUMER REQUEST PROTOCOL

I. PURPOSE AND SCOPE

The California Consumer Privacy Act ("**CCPA**") creates rights for California consumers under certain circumstances to exercise control over their personal information. These consumer rights are not absolute and can be limited when a specific set of exceptions apply.

This CCPA Consumer Request Protocol (the "**Protocol**") outlines the specific consumer rights granted under the CCPA and the general procedures to follow for efficiently and effectively receiving, analyzing and responding to requests to exercise consumer rights. The CCPA grants two categories of consumer rights: (1) those that are granted automatically, without the need for the consumer to submit a request; and (2) those that consumers must submit a request to exercise. This Protocol applies to the latter category where Company will receive, analyze and respond to consumer requests.

All personnel should be aware of this policy, but it is directly applicable to personnel with privacy program oversight, including those in Legal and HR, and those personnel with direct contact with consumers.

II. CONSUMER REQUESTS

A "**consumer**" is defined in the CCPA as an identified natural person (i.e., not an entity) who is a California resident. If Company collects and processes a consumer's personal information, the consumer may contact Company with a request to exercise one or more of their consumer rights provided under the CCPA:

a. The Right to Access

b. The Right to Knowledge

c. The Right to Deletion

d. The Right to Opt Out

e. The Right to Opt In

Please see the ***CCPA Consumer Rights Guidelines*** for more information on the rights available to consumers under the CCPA.

orrick

III. RECEIVING A REQUEST

The Company privacy notice provides consumers with a general explanation of their rights under the CCPA as well as the designated methods for submitting such requests, including:

a. Toll-Free Number: [INSERT NUMBER]

b. Online Platform: [INSERT URL]

c. Email: [INSERT EMAIL ADDRESS]

d. Postal Address:

COMPANY, LLC

ATTN: [PRIVACY LEAD OR PRIVACY TEAM OR APPLICABLE DEPARTMENT]

[INSERT ADDRESS]

Consumers may submit requests through other means, such as by contacting their primary contact person within the organization or by reaching out directly to [APPLICABLE DEPARTMENT OR PERSONNEL] (the "**Privacy Team**"). All requests should be forwarded to the Privacy Team at [INSERT EMAIL ADDRESS]. All received consumer requests should be stored and retained in accordance with ***Section VII – Record Retention***.

The Company employee privacy notice provides employees with a similar explanation of their rights under the CCPA and instructions to forward all such requests to the employee's HR representative. The HR representative should forward the request to the Privacy Team at [INSERT EMAIL ADDRESS] and assist the Privacy Team with the analysis and response to the request on a confidential basis.

The Privacy Team will make reasonable efforts to respond to the consumer and acknowledge receipt of his or her request. Wherever technically reasonable, the acknowledgment should be sent automatically. For example, requests received through the Online Platform should send an automatically generated email to the consumer confirming receipt. Examples of language for acknowledgment of receipt can be found in the ***Sample Consumer Request Responses*** (***Appendix B***).

IV. ANALYZING A REQUEST

Upon receipt of a request, the Privacy Team will:

a. verify the consumer request;

b. determine whether the consumer request is manifestly unfounded or excessive;

c. determine whether any exceptions apply to the request; and

d. coordinate with the relevant contacts to take all actions required by the request.

orrick

CCPA – Service Provider v. Certified Partner v. Third Party

Service Provider	• A for-profit entity that processes PI **on behalf of a business** and for a "business purpose"
	• Must have a **written contract** that prohibits retaining, using, or disclosing the PI for any purpose (including any commercial purpose) other than:
	  • performing the services specified in the contract for the business; OR
	  • **as otherwise permitted by the CCPA**
		Liability Shifting
		
		Deletion Requirements

Other "Person" (also called a **"Certified Partner"**)	• A **person** that receives PI for a **"business purpose"**
	• Must have a **written contract** that:
	  • prohibits the person from **selling the PI**;
	  • prohibits retaining, using, or disclosing the PI for any purpose (including any commercial purpose) other than performing the services specified in the contract;
	  • prohibits retaining, using, or disclosing the PI **outside of the direct business relationship** between the person and the business; AND
	  • **includes a certification** that the person understands the above restrictions and will comply with them
		Liability Shifting
		
		Contractual Certification

Third Party	• An entity or person that **is not a "business"** and **does not receive PI subject to a written contract** with a "**service provider**" or "**certified partner**."	***Selling PI? → Notice & Opt-Out***

"Do Not Sell" Obligations – CCPA

- Must **ENABLE OPT-OUT**:
  - of data "sales" to third parties (including through a "Do Not Sell My Personal Information" homepage link), subject to exceptions

- Must **OBTAIN OPT-IN CONSENT**:
  - for the "sale" of a child's PI to a third party
    - Children <13 – affirmative authorization of a parent
    - Children 13-16 (or <16?) – affirmative authorization of a child
  - *Applies when a business has **"actual knowledge"** of a child's age; business cannot **"willfully disregard"***

PRACTICE NOTE: consider creating a separate "homepage" dedicated to California residents.

Nevada SB-220 Applicability – "Operator"

- Owns or operates a website or online service **for commercial purposes**;
- Collects and maintains covered information from **NV consumers** who use the site/service; **AND**
- Engages in any activity that has a **sufficient nexus** with NV (*e.g.*, does business with NV or NV residents, or "purposefully directs" activities at NV).

- An Operator **IS NOT**:
  - A **third party** acting on behalf of an owner of an Internet website or online service;
  - A **financial institution** subject to the GLBA
  - An **entity subject to HIPAA**
  - A **manufacturer, repairer, or servicer of motor vehicles** where data is retrieved from a connected vehicle or provided by a consumer in connection with a motor vehicle technology or service.
- ******Effective: October 1, 2019******

Nevada "Covered Information" – Defined Narrowly

"Covered Information" – Any one or more of the following items of PII about a consumer collected by an operator through a website or online service and maintained by the operator in an accessible form:

First and Last Name

Home or Other Physical Address with a Street and City or Town Name

Email Address

Any other information concerning a person collected from the person online that **in combination with an identifier makes the information personally identifiable**

Telephone Number

SSN

Identifier Allowing Physical or Online Contact

"Do Not Sell" Obligations – Nevada SB-220

- Establish a **DESIGNATED ADDRESS** for Nevada consumers to submit "do not sell" requests
- **DO NOT SELL** any "covered information" after receiving a "verified" consumer request
- **RESPOND** to verified requests within 60 days of receipt
  - subject to 30 day extension if "reasonably necessary," with notice to the consumer

******Effective: October 1, 2019******

What is a "Sale"?

CCPA

- Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal information to another business or a third party for **monetary or other valuable consideration.**
- Exceptions:
  - Intentional disclosure by consumer to **intentionally interact with a third party**
  - Sharing with a **service provider** that is **necessary to perform a business purpose**
  - Sharing an identifier to alert third parties that consumer has **"opted out"** of sales
  - Transfer as part of a merger, acquisition, bankruptcy, or other asset transaction

Nevada SB-220

- 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.
- Exceptions:
  - Disclosure to a person **processing covered information on operator's behalf**
  - Disclosure to a person with a **direct relationship** with the consumer for the purpose of providing a **consumer-requested product or service**
  - Disclosure to **affiliates**
  - Disclosure consistent with consumer's **reasonable expectations**
  - Disclosure as part of a merger, acquisition, bankruptcy, or other asset transaction

What is a "Verified Request"?

CCPA

- Request **1)** that is made by a consumer, a consumer on behalf of the consumer's minor child, or a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, **and 2)** that the business can **reasonably verify, pursuant to regulations adopted by the Attorney General to be the consumer about whom the business has collected personal information.**
- A business is not obligated to provide **access** or **information disclosures** to the consumer if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

Nevada SB-220

- Request **1)** submitted by a consumer to an operator for the purposes of directing the operator not to make any sale of any covered information about the consumer, **and 2)** for which the operator can **reasonably verify the authenticity of the request and the identity of the consumer using commercially reasonable means.**

Penalties

State AGs have broad authority to enforce the laws.

CA: Each business has a 30-day cure period before the AG may bring an enforcement action.

REGULATIONS: AG must develop rules for enforcing and updating the CCPA by July 1, 2020.

PENALTIES:

- **CA**: Injunction; civil penalty of **$2,500** or (if intentional) **$7,500** per violation.
- **NV**: Injunction; civil penalty not to exceed **$5,000** per violation.

California AG Regulations – Coming Soon

- Rules and procedures for:
  - Submitting and responding to **opt-out requests**
  - Recognizable **opt-out logo or button**
  - **Disclosure** requirements
  - Financial **incentives** for collection/sale/deletion of PI
  - **Verifying** consumer requests

- *See* Cal. Civ. Code § 1798.185

Private Right of Action – Data Breaches

- The CCPA provides consumers with a limited private right of action when their:
  - "nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the **duty to implement and maintain reasonable security procedures and practices** appropriate to the nature of the information."
- Violations of this provision are subject to statutory penalties of $100 to $750 per incident.

What is "Reasonable" Security?

- **CIS20 Controls (potential California baseline)?**
- **New York DFS Cybersecurity Regulation?**
- **Massachusetts Privacy Regulation?**
- **Common themes:**
  - written information security program
  - governance
  - ongoing risk assessment and management
    - table-top exercises
    - penetration tests
  - employee training
  - vendor management
  - an incident response plan

PRACTICE NOTE: consider maintaining attorney-client privilege during security assessments.

CIS20 Controls

Basic

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

Foundational

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

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

QUESTIONS?

orrick

Orrick's Privacy Law Webinar Series
Part #3: Spotlight on EdTech

Webinar | August 27, 2019 | 12pm – 1pm (Eastern Standard Time)

How the New California and Nevada Privacy Laws Will Impact Data in Education Technology

This webinar is the third in a series on U.S. privacy law developments in 2019 and will cover what the new era of data regulation means to the highly sensitive data that education technology companies, products, and services handle.

Presenters

Emily Tabatabai, Partner

Sulina Gabale, Managing Associate

Orrick's Privacy Law Webinar Series

- ✓ Want to learn about the new U.S. privacy laws and the impact they may have on your business?
- ✓ Missed a past webinar?
- ✓ Want to attend our next webinar?

California was the first U.S. state to enact a sweeping new privacy law, the CCPA, which comes into effect in January 2020. Nevada has now enacted a scaled-down version of the CCPA that is slated to take effect even sooner – as early as October 2019.

- ✓ Visit **https://www.orrick.com/Cyber-Privacy-Webinars-Videos**

Orrick's CCPA & GDPR Readiness Assessment Tools

Orrick's ccpa READINESS ASSESSMENT

Test your company against the provisions under the CCPA

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your CCPA project plan

Visit: orrick.com/Practices/CCPA-Readiness

Orrick's GDPR Readiness Assessment Tool

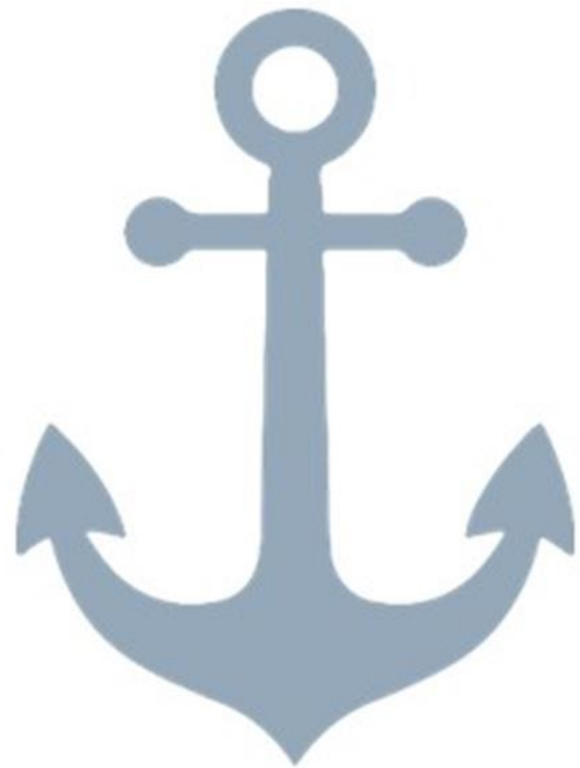
Stress test your company against the provisions under the GDPR

- Receive a complimentary report summarizing the likely key impacts
- Use the report to develop your GDPR project plan

Visit: orrick.com/Practices/GDPR-Readiness

Trust Anchor

An established point of trust in a cryptographic system from which a process of validation can begin



Blog: blogs.orrick.com/trustanchor
Twitter: @Trust_Anchor

Heather Egan Sussman

Partner
Boston

T 617 880 1830
E hsussman@orrick.com

Honors

- *Chambers USA* 2019
- *The Legal 500 United States* 2019
- *Cybersecurity Docket's* "Incident Response 30" 2016, 2018, 2019
- *Massachusetts Lawyers Weekly* "Top Women of Law" 2015
- *Best Lawyers* 2018-2019

Education

- J.D., Boston College Law School, 2000
- B.A., University of Massachusetts Dartmouth, 1996, *magna cum laude*

Heather Egan Sussman is Global Co-chair of Orrick's Cyber, Privacy & Data Innovation practice, and the leader of Orrick's Boston Office. Her practice focuses on privacy, cybersecurity and information management, and she is ranked by *Chambers USA* and *The Legal 500 United States* as a leader in her field. *Chambers* explains companies turn to Heather because she is "generous with her time and endeavors greatly to educate her clients and understand a given client's risk profile."

Heather's practice focuses on privacy, cybersecurity and information management. Heather routinely guides clients through the existing patchwork of laws impacting privacy and cybersecurity around the globe. In the United States this includes advising on federal and state laws such as CCPA, FCRA, ECPA, TCPA, HIPAA, CAN-SPAM, GLBA, state breach-notification laws, and state data-security laws, as well as existing self-regulatory frameworks, including those covering online advertising and payment-card processing. Outside of the United States she manages teams of talented counsel around the world to deliver seamless advice for clients that operate across many jurisdictional lines, developing comprehensive privacy and cybersecurity programs that address competing regulatory regimes. Heather drafts online privacy notices for global rollout and implements data-transfer mechanisms for the free flow of data worldwide. She helps clients develop and achieve their data innovation strategies, so they can leverage the incredible value of data and digital technologies in ways that not only meet compliance obligations but also support innovation, deliver value to the business, meet security needs and solidify brand and consumer trust. Heather helps clients reduce the risk of privacy and security incidents, and in the event of a privacy or security breach, she helps companies respond. She guides clients through comprehensive privacy and cybersecurity assessments worldwide. Heather also regularly counsels businesses on how to mitigate risks associated personal data.

Barrie VanBrackle

Partner
Washington, D.C.

T 202 339 8408
E bvanbrackle@orrick.com

Honors

- *AV (Preeminent) rating, Martindale-Hubbell*

Education

- J.D., Washington University School of Law
- B.A., Johns Hopkins University

Barrie VanBrackle, a partner in Orrick's Washington, D.C., office, is a member of the Cyber, Privacy & Data Innovation practice and co-leads Orrick's Fintech team.

An authority on payments and consumer financial services compliance, Barrie focuses on three areas at the cross section of the fintech space: consumer-facing financial and banking, regulatory counseling and investigations, payment card industry, including brand operating rules and data security standards; money transmission; and prepaid card access on behalf of leading merchants, payment processors and industry vendors. Barrie advises on transactions involving the payment systems participants, including large merchants and financial technology companies, with respect to payment acceptance, payment issuance, co-brand agreements, payment card industry data security issues, and payment regulatory matters. In addition, Barrie has deep experience advising corporate and private equity clients in M&A contexts and other investments in fintech. Barrie represents payment card issuing and merchant acquiring banks (including acquiring a card program for one of the Top 5 largest financial institutions, negotiating co-brand agreements for a large issuing bank and a sports franchise, and negotiating novel payment acceptance methods for more traditional merchants). She helps fintechs navigate the banking and money transmission rules, including representing new market entrants into the US.

David Curtis

Law Clerk
Boston

T 617 880 1923
E dcurtis@orrick.com

Honors

- *Harvard Law School, 2015, Dean's Award for Community Leadership*

Education

- J.D. Harvard Law School, 2015
- B.A., Yale University, 2011, *cum laude*

David Curtis is a member of Orrick's internationally recognized Cyber, Privacy & Data Innovation practice.

David's practice focuses on data privacy, cybersecurity, digital advertising, Internet law and consumer protection. David advises clients on data collection, storage, use, licensing and transfer issues. He also provides guidance on issues relating to the California Consumer Privacy Act of 2018 (CCPA), the Gramm-Leach-Bliley Act (GLBA), unfair and deceptive trade practices, the Fair Credit Reporting Act (FCRA), and other state and federal laws and self-regulatory frameworks. In addition, David has experience evaluating the applicability of European data protection requirements, including the General Data Protection Regulation (GDPR), to U.S. companies.

Before joining Orrick, David was an associate at Ropes & Gray LLP and an adjunct professor at Harvard Law School, where he taught legal research, writing and analysis. David clerked for Justice Barbara Lenk of the Supreme Judicial Court of Massachusetts.

**Only admitted to practice in Massachusetts and New York. Not admitted to practice in Washington.*