



SPOTLIGHT ON ***EDTECH***

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

August 27, 2019




Introductions



Emily Tabatabai

Partner
Cyber, Privacy & Data
Innovation

etabatabai@Orrick.com

[@EmilyTabatabai](https://twitter.com/EmilyTabatabai) 



Sulina Gabale

Managing Associate
Cyber, Privacy & Data
Innovation

sgabale@Orrick.com

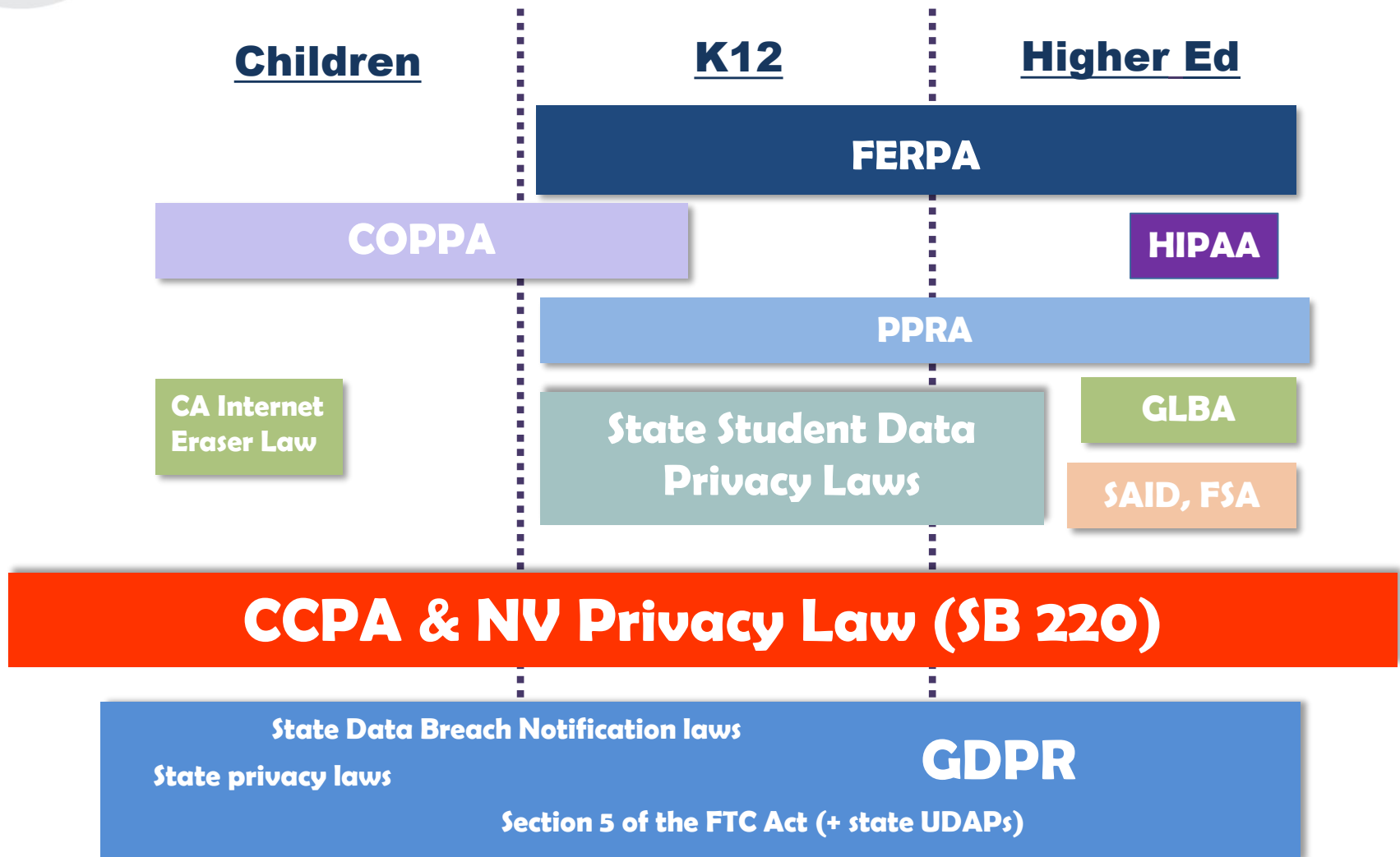
[@SulinaGabale](https://twitter.com/SulinaGabale) 

Agenda

- Scope and Applicability of CA and NV Privacy Laws
- Key Compliance Obligations & Enforcement
 - Notice & Transparency
 - Data Subject Rights
 - “Do Not Sell” Requirements
- Implications for EdTech: Child-Directed & School-Directed Services
 - COPPA and Opt-In to “Sale”
 - Categorization of EdTech Providers Under CCPA
 - Potential Conflicts of Laws
 - Contracting Implications

EdTech Legal Framework

Operators of child or student-related services face a patchwork of regulation





Scope and Applicability of the CCPA and NV SB-220

What's New?

California Consumer Privacy Act (CCPA)

Effective date: **January 1, 2020**
(enforcement unlikely before July 2020)

Anticipate statutory amendments and California AG regulations, coming "Fall" 2019

- Imports GDPR-style **consumer rights** around data ownership, transparency and control
- Right to Opt-Out: **Do Not Sell My Personal Information** link
- Pay-for-Privacy: may offer **financial incentives** for collection, sale and deletion of personal information but can't "**discriminate**" against consumers who exercise their rights
- **Private Right of Action for Data Breaches**: increased litigation risk (\$100 to \$750 per incident)

Nevada Privacy Law (SB 220)

Effective date: **October 1, 2020**

- **Right to Opt-Out**: Do not sell to recipient who will license or resell PI
- Much more limited in scope, burdens, risks



CCPA: Applies to a “Business”

- **A Business:**

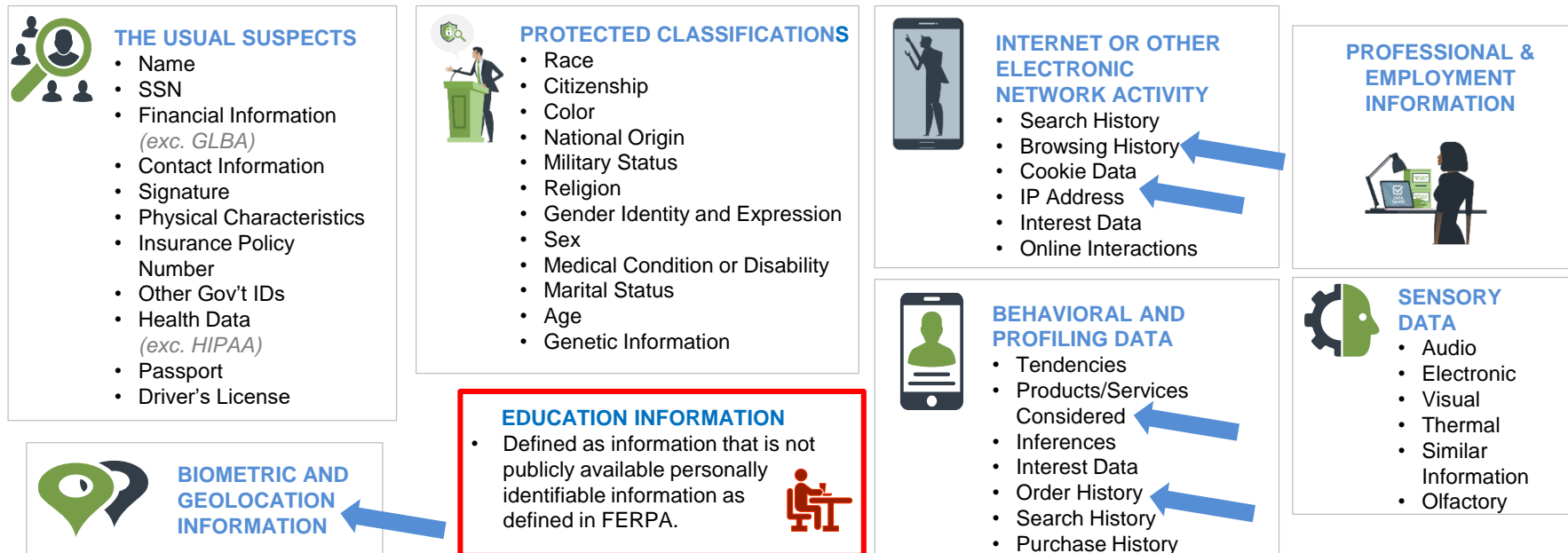
- **For-profit** entity
- Does business in California
- Collects, receives or accesses California residents’ personal information
- Decides **why and how** such personal information is used or processed,

AND

- Satisfies at least one of the following criteria:
 - **Gross revenue over \$25M** per year;
 - Collects or shares the personal information of **>50,000 CA consumers, households or devices** per year; **or**
 - Derives **50% or more of its revenue from selling CA consumers’** personal information

CCPA “Personal Information” Defined

Expansive Definition of “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**.



“Personal information” includes “education information, defined as information that is not publicly available personally identifiable information as defined in the FERPA.”



CCPA Exemptions and Exceptions

Exemptions for personal information processed pursuant to federal privacy regimes:

- the Gramm-Leach-Bliley Act (GLBA);**
- the Driver's Privacy Protection Act (DPPA);**
- the Health Insurance Portability and Accountability Act (HIPAA);
- clinical trial information collected under the Common Rule.

***The data collected under these exemptions can arguably serve as the basis of a private right of action under the CCPA in the event of a qualifying data breach.*

Efforts to add exemption for FERPA-covered data have not been successful (yet)

PRACTICE NOTE: CCPA exempts only the personal information collected pursuant to these statutes, but a business may collect other types that are subject to the CPPA (e.g., IP address, cookie data, employee data, etc.).



Nevada: Applies to an “Operator”

- An Operator:
 - Owns or operates a website or online service **for commercial purposes**;
 - Collects and maintains covered information from **consumers who reside in Nevada** and use or visit the Internet website or online service;
- **AND**
 - Purposefully directs its activities toward Nevada, consummates transactions with Nevada or its residents, purposefully avails itself of the privilege of conducting activities in Nevada **or otherwise engages in any activity that constitutes a sufficient nexus** with Nevada.
- 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 Gramm-Leach-Bliley Act (“GLBA”);
 - An entity subject to the Health Insurance Portability and Accountability Act (“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.

Nevada: “Covered Information” is Defined Less Broadly

DEFINITION — 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



Social Security
Number



Identifier Allowing
Physical or Online
Contact



Key Compliance Obligations



Under the CCPA, a “Business” must:

DISCLOSE online:

- categories of PI it collects, sells and otherwise discloses for a business purpose;
- categories of sources of the PI;
- business or commercial purposes for collecting or selling the PI;
- categories of third parties to whom the business “sells” or otherwise discloses the PI; and
- description of the consumers’ rights and the designated methods for submitting requests.

PROVIDE ACCESS:

- to the PI collected over past 12 months in a **portable** format, in response to a “verifiable consumer request”

DELETE:

- PI upon a “verifiable consumer request” (and direct “service providers” to delete), subject to exceptions

PERMIT OPT-OUT:

- of data “sales” to third parties (including via “Do Not Sell My Personal Information” link), subject to exceptions

OBTAIN OPT-IN CONSENT:

- for children 13-16, for “sales” of PI to a third party (“actual knowledge” and “willfully disregard” standard)

TRAIN EMPLOYEES:

- about the business’ privacy practices, compliance and how to direct consumers to exercise their rights

NOT DISCRIMINATE:

- Against consumers who exercise their rights under the CCPA, **but** some financial incentives permissible (“Pay-for-Privacy”)

CONTRACT effectively:

- relative to “service providers” to establish scope of permissible data uses and mechanism for complying with consumer access/deletion requests



Under Nevada's law, an “Operator” must:

DISCLOSE

- Establish a designated address through which a consumer may submit a **verified request** directing the operator not to make any **sale** of any covered information.

PERMIT OPT-OUT OF SALE

- Refrain from making any **sale** of any covered information after receiving a **verified consumer request**.

RESPOND

- Respond to a verified consumer request within **60 days** after receipt, or within an additional 30 days if reasonably necessary and with notice to the consumer.



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**.
- **Does Not Include:**
 - If a consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party;
 - Sharing an identifier to alert third parties that the consumer has opted out of sales;
 - Sharing with a service provider that is necessary to perform a business purpose, pursuant to contractual restrictions;
 - Transferring to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the business.

Nevada

- 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.
- **Does Not Include:**
 - Disclosure to a person processing the covered information on behalf of the operator;
 - Disclosure to a person with a direct relationship with the consumer for the purpose of providing a product or service requested by the consumer;
 - Disclosure consistent with a consumer’s reasonable expectations;
 - Disclosure to affiliates; or
 - Disclosure as part of a merger, acquisition, bankruptcy or other asset transaction.



Enforcement & Liabilities

CCPA

AG Enforcement: Civil penalty of \$2,500 (per violation) to \$7,500 (per intentional violation) and injunctive relief.

- Enforcement is triggered upon violation(s) of CCPA.
- 30-day notice and cure period before AG may bring an enforcement action.

Limited Private Right of Action for Data Breach: Statutory damages not less than \$100 and not greater than \$750 “per consumer per incident,” or actual damages (whichever is greater); injunctive or declaratory relief.

- Consumers may bring an action when personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a failure to implement and maintain reasonable security measures.
- 30-day notice and cure period before filing.

NV Law

AG Enforcement: Injunction; civil penalty not to exceed \$5,000 per violation or injunctive relief.



Potential Impact on EdTech

For School-Directed Services

Quick Recap: Regs for School-Directed Services

	COPPA	FERPA	40+ State Student Privacy Laws
	<ul style="list-style-type: none"> Online operators PI broadly defined (incl. image, audio, persistent IDs, IP address, etc.) Children <13 (K-8) 	<ul style="list-style-type: none"> EdTech “School Officials” (imposed via contract) PI from educational records K12 + Higher Ed students 	<ul style="list-style-type: none"> EdTech providers or K12 online services PI or “covered data” (much more broad) K12 students
Notice	✓ Notice of data practices	✓ Implicit	✓ Specific contract terms
Consent	✓ Can rely on School to provide necessary consent in limited circumstances	☒ No parental consent	☒ No parental consent
Use	✓ <i>Solely</i> for use and benefit of school and for no other commercial purpose	✓ <i>Solely</i> for educational purpose described in contract, subject to school control	✓ <i>Solely</i> to provide service described in agreement on behalf of school
Rights	✓ Right to review or delete PI or withdraw consent	✓ Rights to inspect, review, amend	✓ Generally, yes, subject to school direction
Deletion	✓ Upon request or when no longer needed for school purpose ! \$40,000 per violation	✓ Upon request or when no longer needed for school purpose	✓ Upon request or when no longer needed for school purpose ! Strict contracts

For School-Directed Services

CCPA Service Providers

CCPA imposes very different obligations, depending on the Company's role (Business, Service Provider, Third Party)

"Business"

A for-profit entity that does business in California, collects personal information of California residents and **determines why and how** personal information is processed, and meets size thresholds

CCPA obligations apply primarily to **Businesses!**

"Service Provider"

A for-profit entity that receives PI for a **business purpose** and processes PI **on behalf of a business** pursuant to a **contract** that **prohibits** the service provider from:

- retaining, using or disclosing PI for any purpose other than performing the contracted services, **including using the PI for a commercial purpose** other than the contracted service.

- ☒ Disclosures: not required, but good practice
- ☒ Access/Portability (may need to assist Business response)
- ✓ Businesses must pass through deletion requests to service providers
- ☒ Data sales opt-outs (n/a)

"Certified Partner"

A person who receives PI for a **business purpose** pursuant to a **contract** that prohibits the person from:

- retaining, using or disclosing PI for any purpose other than performing the contracted services, **including using the PI for a commercial purpose** other than the contracted service;
- retaining, using or disclosing PI **for any purpose outside of the direct business relationship** between the parties;
- Includes a **certification of compliance**.

"Third Party"

A person or business who is not a business, a service provider or a person and **does not receive personal information subject to a restrictive contract**.

Service Providers have few obligations to *consumers*. Instead, they answer to the Business.

CCPA Definitional Oddities (& problems for EdTech)

“Business”

A for-profit entity that does business in California, collects personal information of California residents and **determines why and how** personal information is processed, and meets size thresholds

A school is not a for-profit entity and therefore cannot be a “business”

“Service Provider”

A for-profit entity that receives PI for a **business purpose** and processes PI **on behalf of a business** pursuant to a **contract** that **prohibits** the service provider from:

- retaining, using or disclosing PI for any purpose other than performing the contracted services, **including using the PI for a commercial purpose** other than the contracted service.

An EdTech provider cannot be a “service provider” because it does not process data on behalf of a “business” ... typically, it provides services on behalf of an educational institution (govt. agency)

“Certified Partner”

A person who receives PI for a **business purpose** pursuant to a **contract** that prohibits the person from:

- retaining, using or disclosing PI for any purpose other than performing the contracted services, **including using the PI for a commercial purpose** other than the contracted service;
- retaining, using or disclosing PI **for any purpose outside of the direct business relationship** between the parties;
- Includes a **certification of compliance**.

“Third Party”

A person or business who is not a business, a service provider or a person and **does not receive personal information subject to a restrictive contract**.

If EdTech provider is a:

“**Business**” → subject to CCPA consumer rights and obligations

“**Person**” → Exceptionally strict use limitations; may not be able to use for own operational or business purposes

“**Third Party**” → subject to CCPA consumer rights obligations

CCPA: Where Do EdTech Providers Fit?

Uncertainty for EdTech providers:

- While “School Official” seems similar to the CCPA “Service Provider” concept, legislators have not taken (and likely will not take) this position

If the EdTech Provider is a:

- **“Business”** → subject to CCPA consumer rights and obligations
- **“Certified Partner”** → Exceptionally strict use limitations; may not be able to use for own operational or business purposes
- **“Third Party”** → subject to CCPA consumer rights obligations

EdTech Provider vs CCPA Service Provider

- ✓ Describe data practices in contract
- ✓ use PI solely to provide the service to the School, for purposes described in contract and no other commercial purpose
- ✓ Subject to direction and control of the School
- ✓ Cannot retain or disclose PI to third parties except as directed by School
- ✓ Must assist School responding to access and deletion requests

CCPA & Conflicts with Laws: Data Subject Rights

- 1. Who has the right to access and delete student data held by an EdTech Provider?**
 - Can a student request deletion of grades and homework?
 - Could operator be required to delete data under CCPA while prohibited from deleting such data under FERPA and SOPIPA?
- 2. Who has the right to access PI created by the instructor or school about the student?**
 - Can students or parents request access to evaluations and assessments?
- 3. Could student opt-out of permissible disclosures to third parties? Would EdTech provider need to get opt-in consent from the student?**
 - Several activities permitted by FERPA, SOPIPA and AB 1584 could be considered a “sale” of student data to a third party, but the CCPA would require EdTech operator to request “consent” from a student age 13-16 or from a parent of a child under 13. This could inhibit legitimate disclosures of student data to third parties for research or educational purposes.

PRACTICE NOTE: The CCPA provides a general exception that the obligations imposed upon a business shall not restrict a business’s ability to “comply with federal, state, or local laws.” Important for school agreements to address how each party will comply with laws!

EdTech Contracting Recommendations

- ✓ Specify that student data is **owned and controlled solely by the school/district** (supports argument that the EdTech provider does not have the rights and licenses necessary to honor a consumer's requests but the school/district does).
- ✓ Specify that all Consumer Rights Requests will be passed through to the School
- ✓ Include specific **limitations on collection, use, processing and disclosure of student data** in line with "School Official" obligations under FERPA *and* the "Service Provider" definitions under CCPA.



In addition:

EdTech Provider Privacy Policy disclosures should specify that all CCPA **data subject requests must be verified with the school/district.**



Potential Impact on EdTech

For Child-Directed Services



Quick Recap: Regulatory Environment for Child-Directed Services

COPPA

- **Scope:** Applies to operators of commercial websites and online services (incl. mobile apps) where:
 - The website or online services is **directed to children under 13**, or
 - The general audience website or service **has actual knowledge** that it is collecting PI from children under 13, and
 - Operator collects PI from children under 13, (e.g., name, email, photo, video, voice, geolocation, persistent identifier)
- **Requirements:**
 - Must obtain **verifiable parental consent** before collecting PI from children under 13
 - PP disclosures; direct notice to parents; among others
 - Up to \$40,000 penalty per violation

CA Online Eraser Law

- **Scope:** Applies to operators of commercial websites and online services (incl. mobile apps) “directed to minors” (under 18)
- **Requirements:**
 - Must permit a **minor (under 18) in CA** who is a registered user of the service to **remove, or to request and obtain removal of, content or information that was posted on the service** by the minor.
 - **Clear instructions in PP** on requesting removal of content or information posted.

CCPA: Right to Opt-In to a Sale

- CCPA: A business shall not “sell” the personal information of a consumer to a third party for a non-business purpose unless:
 - **For children <13**, the child’s parent or guardian has affirmatively authorized the sale
 - **For children <16**, the child consumer has affirmatively authorized the sale
- Applies when business has **actual knowledge** of child’s age. A business cannot **willfully disregard** the child’s age or will be deemed to have actual knowledge.

QUESTIONS

1. Cannot “willfully disregard” – Is there an implicit obligation to age-screen if the site is directed to a child or teen audience? A mixed-audience?
2. How to get ‘affirmative authorization’? Synonymous with COPPA’s verifiable parental consent standard or something less?
3. Implications for general audience website that may be attracting teens with homepage cookies and interest-based ad trackers? Fact-specific inquiry, like COPPA?

Child-Directed Services: Consents and Obligations

	COPPA		CCPA		NV
16+	N/A		Must permit access, knowledge and deletion Must permit opt-out of data sales		Must permit ability to opt-out of data sales
13 – 16	N/A* *proposed COPPA amendment would require affirmative consent from minors 13-15		Sites with actual knowledge (cannot <i>willfully disregard</i>) Must obtain affirmative authorization from child before selling PI Must permit access, knowledge and deletion		Must permit ability to opt-out of data sales
< 13	Sites with actual knowledge Sites “directed to” children <13 or a mixed audience (may be required to age screen) Must obtain verifiable parental consent before collecting of PI Must permit parent access, deletion, withdrawal of consent		Sites with actual knowledge (cannot <i>willfully disregard</i>) Must obtain affirmative authorization from parent before selling PI		Must permit ability to opt-out of data sales

How to Obtain “Opt-In” to Sale

1. Obtain consent prior to “sale.”
2. Provide “clear and conspicuous” disclosures in line with general privacy principles for transparency (*CCPA is silent on content*), e.g.:
 - a. *The types of the PI that you “sell”;*
 - b. *Description of categories of third parties to whom you will sell PI and how third parties will use it;*
 - c. *Statement that consumer may revoke consent at any time and mechanism to revoke consent; and*
 - d. *Hyperlink to Privacy Policy.*
3. Obtain “affirmative authorization” (e.g., opt-in).
4. Enforce opt-outs, monitor complaints, and train employees.





QUESTIONS?



Orrick's Privacy Law Webinar Series

Part #4: Reasonable Security

Webinar | September 26, 2019 | 12pm – 1pm (Eastern Standard Time)

Defining 'Reasonable' Security under California's New Privacy Law

This webinar is the fourth in a series on U.S. privacy law developments in 2019 and will cover litigation strategies for defending CCPA class actions and steps that companies can take now to best position them to argue later that their security is “reasonable.”

Presenters

Michelle Visser, Partner

Nicole Gelsomini, Associate



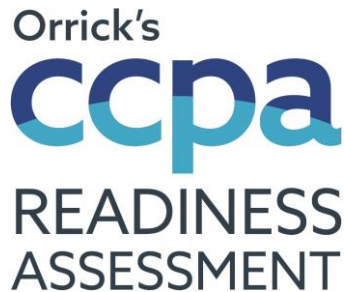
Orrick's Privacy Law Webinar Series

- ✓ 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 and GDPR Readiness Assessment Tools



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



Emily S. Tabatabai



Partner
Washington, D.C., Houston

T 202 339 8698
E etabatabai@orrick.com
@EmilyTabatabai

Honors

- *Chambers USA* - Nationwide, Privacy & Data Security, Up and Coming attorney (2018-2019)
- *The Legal 500*, Cyber Law - Including Data Protection and Privacy (2017-2019)
- Member of IAPP Publications Advisory Board (2019)
- Member of Law360 Privacy Editorial Advisory Board (2018)
- *Law360*, Privacy Practice Group of the Year (2016)
- *The Legal 500*, Media Technology and Telecoms, Cybercrime (2014-2016)

Education

- University of Virginia School of Law, J.D., 2006
- Emory University, Goizueta Business School, B.B.A., 2001

Emily S. Tabatabai is a partner and founding member of the Cyber, Privacy & Data Innovation practice, which was named the Privacy & Data Security Law Firm of the Year by Chambers USA in 2019. She has been recognized by *The Legal 500* for her "extraordinary depth of knowledge in student data privacy matters," and by *Chambers USA* as "an invaluable resource to have when it comes to data privacy and security...on the student data side, she is unmatched."

Emily advises clients on an array of privacy and data management matters, helping clients navigate the complex web of privacy laws, rules, regulations and best practices governing the collection, use, transfer and disclosure of data and personal information. She works closely with client business teams and in-house counsel to assess and manage privacy risks, design and deploy compliance programs and implement privacy-by-design approaches to address key compliance objectives while supporting each client's data innovation strategies and the development and use of cutting-edge digital technologies.

Emily frequently guides child- and student-directed service providers through the complexities of compliance with the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA), California's Student Online Personal Information Protection Act (SOPIPA) and similar state student privacy laws and advises companies across the industry spectrum as they work towards compliance with the California Consumer Privacy Act (CCPA). She also represents clients subject to regulatory investigations and litigation involving a spectrum of federal and state laws, including under Section 5 of the Federal Trade Commission Act (FTC Act), COPPA, the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), the U.S.-E.U. Privacy Shield Program, the California Online Privacy Protection Act (CalOPPA) and others.

Sulina Gabale



Managing Associate Washington, D.C.

T 202 339 8420

E sgabale@orrick.com

Honors

- Emory Law Moot Court Society - First Amendment Team

Education

- Emory University School of Law, J.D., 2014
- New York University, B.A., Journalism and Politics (double major), 2010, *cum laude*, Founders Day Scholar

Sulina Gabale is a Managing Associate and founding member of the Cyber, Privacy & Data Innovation practice, named Band 1 in U.S. Privacy & Data Security in 2019, Privacy Practice Group of the Year by *Law360* in 2017 and is nationally ranked by *The Legal 500 US* for Cyber Law, Data Protection and Privacy.

As innovation pushes the limits of technology, those ideas challenge the boundaries of what is considered “personally identifiable information.” Sulina answers the question - how can we create tomorrow’s technology with yesterday’s privacy and consumer protection laws? Sulina works closely with innovators at all levels of a business – executives, engineers, marketing and product, HR and customer service teams – to gain a true understanding of their goals and the data they’re collecting, using and sharing. She places herself in her client’s shoes as well as in consumers’ mindset to devise creative privacy-by-design solutions, ensuring her client’s business and data innovation strategies withstand multi-national rules, government regulations, industry standards and consumer scrutiny.

With experience in both data privacy and consumer protection, Sulina utilizes a comprehensive approach to counsel clients on a myriad of issues affecting consumers and businesses. She routinely guides companies of all sizes through the existing patchwork of laws, self-regulatory standards and industry practice impacting data privacy and security including the Section 5 of the FTC Act, the CCPA and proposed state legislation, COPPA, biometric privacy laws, FCRA, GLBA, FERPA and related state student data privacy laws, the U.S. E.U. Privacy Shield Program, CalOPPA and others.

Sulina advises companies of all sizes on the development and deployment of cutting-edge technologies and services, including ad-tech, AI and machine learning, biometric tools, social media, robotics and IoT devices, marketing and promotions and more.

Sulina began her legal career focusing on consumer protection. She continues to counsel clients on marketing and promotional issues, including interest-based ads; sweepstakes and promotions; automatic renewal and subscriptions; advertising substantiation; influencer programs and social media; SMS text messaging and telemarketing (including matters involving the Telemarketing Sales Rule (TSR), the Telephone Consumer Protection Act (TCPA)); and other state and federal consumer protection laws.

