GT GreenbergTraurig

BIGLAW REDEFINED.

Website and Mobile App Compliance Under the CPRA and New State Privacy Laws Effective in 2023

CPRA, CPA, CTDPA, UCPA, VCDPA

ACC Association of Corporate Counsel

GTLAW.COM

October 6, 2022

GT GreenbergTraurig

Speakers

Gretchen Ramos, CIPP/US/E, CIPM
Global Co-Chair Data
Privacy & Cybersecurity Group
Greenberg Traurig, LLP
San Francisco, California
415.655.1319 | ramosg@gtlaw.com

Darren Abernethy, CIPP, PLS, FIP
Shareholder – Data, Privacy &
Cybersecurity Group
Greenberg Traurig, LLP
San Francisco, California
415.655.1261 | abernethyd@gtlaw.com

GT GreenbergTraurig

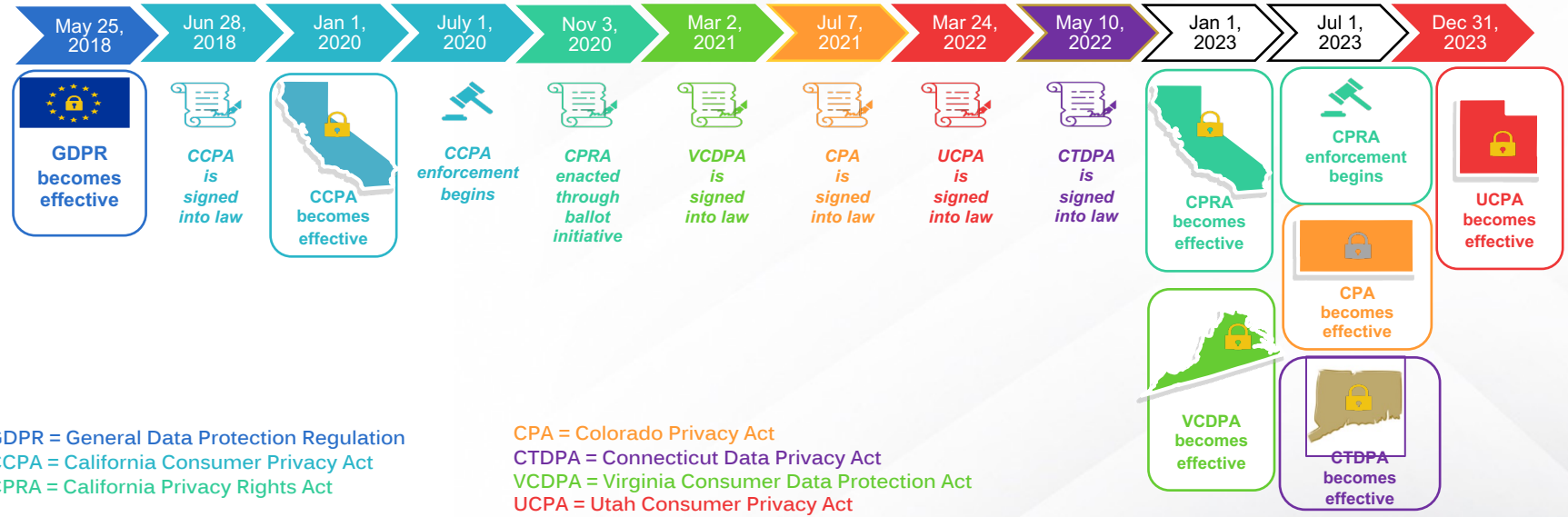
AGENDA

- 2023 State Privacy Laws
- Scope & Applicability
- Privacy Notice
- Data Minimization
- Selling & Sharing: Opt-out vs. Consent
- Global Privacy Control
- Sensitive Personal Information
- Enforcement
- Contracting Requirements
- Children’s Personal Information

The New State Privacy Laws

GT GreenbergTraurig

Privacy Legislation 2018 - 2023

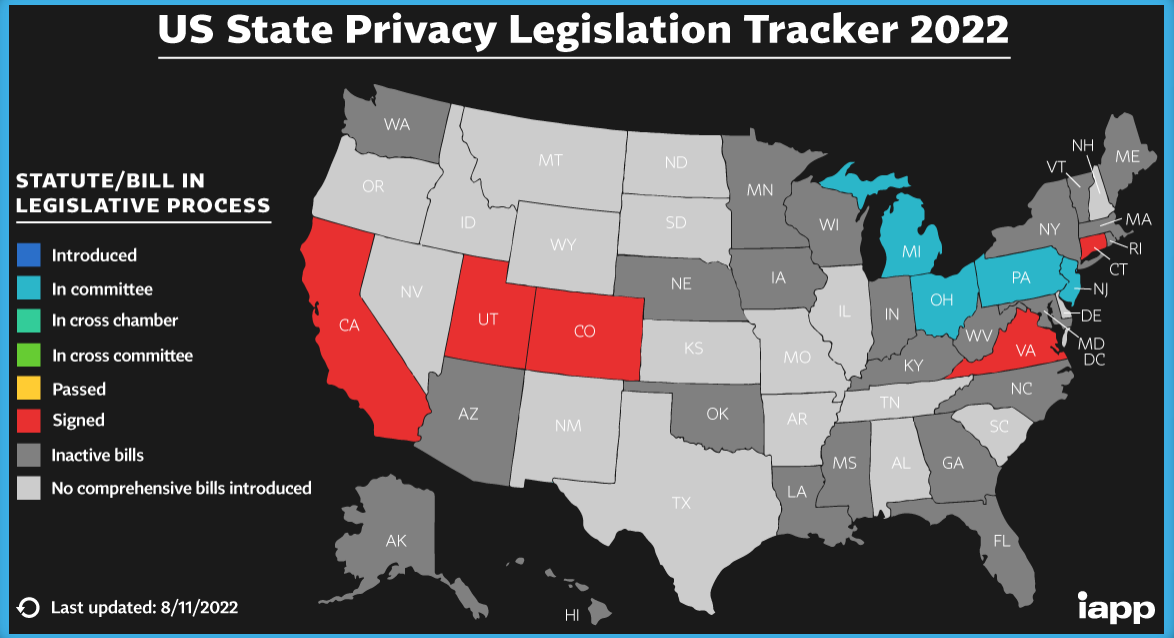


GDPR = General Data Protection Regulation
CCPA = California Consumer Privacy Act
CPRA = California Privacy Rights Act

CPA = Colorado Privacy Act
CTDPA = Connecticut Data Privacy Act
VCDPA = Virginia Consumer Data Protection Act
UCPA = Utah Consumer Privacy Act

GT GreenbergTraurig

And Some New Privacy Bills in the Works



Courtesy of the IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

GT GreenbergTraurig

Side-by-Side: GDPR & U.S. State Consumer Privacy Laws

Category		GDPR	CCPA	CPRA	CPA	CTDPA	UCPA	VCDPA
ABILITY TO ACCESS DATA	Permissible Purpose	X		X	X	X		X
	Data Minimization	X		X	X	X		X
INDIVIDUAL RIGHTS	Notices to Data Subjects	X	X	X	X	X	X	X
	Financial Incentive Disclosure		X	X				
	Right to Access Data	X	X	X	X	X	X	X
	Right to Fix Errors (aka Right to Correction/Rectification)	X		X	X	X		X
	Right to Deletion (aka Right to be Forgotten)	X	X	X	X	X	X	X
	Right to Opt Out of Sale	X*	X	X	X	X	X	X
	Right to Opt Out of Behavioral Advertising	X*		X	X	X	X	X
	Right to Object to Use of Sensitive Information	X*		X		X*		
	Right to Object to Automated Decision-making and Profiling	X		X	X	X		X
	Right to Object to other Uses	X						
	Right to Nondiscrimination		X	X	X	X	X	X
ACCOUNTABILITY AND GOVERNANCE	Documentation and Recordkeeping	X		X	X	X	X	X
	Risk Assessments	X		X	X	X		X
	Designate a DPO (if necessary)	X						
SECURITY	Appropriate Data Security to Safeguard Information	X	X*	X	X	X	X	X
	Breach Notification	X	X*	X*	X*	X*	X*	X*
DATA TRANSFERS OUTSIDE OF EEA	Adequacy measures required for any country determined to have laws that do not parallel EEA	X						
TRANSFERS TO THIRD PARTIES	Contractual Requirements in Service Provider	X		X	X	X	X	X
	Joint controllers should allocate responsibilities	X		X				
MARKETING AND ADTECH	Consent for AdTech Cookies	X						
	Consent obtained prior to direct marketing	X						

Scope & Applicability

GT GreenbergTraurig

CA: What Companies Are In-Scope?

- Currently, the **CCPA** applies to any **(1)** for-profit business that **(2)** "collects" the PI of CA residents, **(3)** determines the purposes and means of processing that PI, **(4)** does business in CA, and **(5)** meets one of the following criteria:

  (a) Has annual gross revenue in excess of $25M;

  (b) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the PI of 50,000 or more CA consumers, households or devices; or

  (c) Derives 50% or more of annual revenue from selling PI.

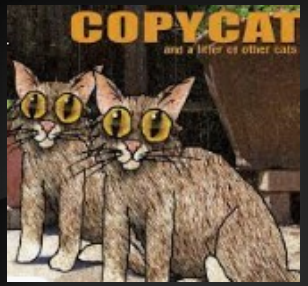
- The **CPRA** changes threshold requirement (b) above by

  - increasing the number of CA residents whose PI a covered business buys, sells or shares from 50,000 to 100,000. Helpful to SMEs.

  - clarifies that the regulated activity is only buying, selling or sharing personal information…removing inclusion or ambiguity as to entities that receive or share PI for "commercial purposes" (separately defined).

GT GreenbergTraurig

Other States: Companies In-Scope



Colorado, Connecticut, Utah and Virginia each use similar thresholds that have as a prerequisite doing business in that state, or producing or delivering commercial products there, or that offering services intentionally targeted to residents of that state. Plus:

- **CO:** Controls the PD of 100,000+ consumers in a CY **or** processes or controls the PD of 25,000+ consumers and derives revenue from it.
- **CT:** Controls or processes the PD of 100,000+ consumers in a CY **or** controls or processes the PD of 25,000+ consumers and derives 25% of its gross revenue from that sale of PD.
- **UT:** Has annual revenue of $25M+ **and** (a) controls or processes the PD of 100,000+ consumers in a CY or (b) controls or processes the PD of 25,000+ consumers and derives 50% of its gross revenue from sale.
- **VA:** Controls or processes the PD of 100,000+ consumers in a CY **or** controls or processes the PD of 25,000+ consumers and derives 50% of its gross revenue from sale.

GT GreenbergTraurig

Exemptions

- Drivers Information, Activities Protected by Free Speech/1st Amendment, Publicly Available, Deidentified Information, and Fair Credit Reporting Act (FCRA). Exempt.
- B2B Data & HR Data. Exempt, except in California starting with the CPRA on 1/1/2023.
- Non-profits: Exempt as a business, except in Colorado (but could be a service provider).
- Gramm-Leach-Bliley Act (GLBA). Personal information processed pursuant to GLBA (*or CalFIPA in CA*) exempt; entities subject to GLBA completely exempt, except in California.
- HIPAA. Personal information subject to HIPAA is exempt. CA adds color, plus the CMIA.
- COPPA. Virginia, Utah and Connecticut exempt controllers and processors that comply with verified parental consent requirements of COPPA; Colorado exempts personal data regulated by COPPA; CPRA only notes it shall not conflict with COPPA.
- FERPA. Virginia, Utah and Connecticut exempt institutions of higher educations and personal information regulated by FERPA; Colorado exempts personal information regulated by FERPA; California does not exempt FERPA entities or data.

Privacy Notice Requirements

Privacy Notice

Impact: Website/App Privacy Notices Must Be Updated

Requirements

- Categories of PI collected about the consumer
- Categories of sources from which the PI is collected
- Categories of PI shared or sold for targeted advertising
- Categories of PI sold or if the business has not sold PI, it shall disclose that fact
- Business or commercial purpose for collecting, sharing or selling such PI, or if the business has not disclosed such personal information for a business purpose, it shall disclose that fact
- Categories of third parties to whom PI was shared or sold
- Sensitive PI collected
- Right Retention periods
- Financial incentives
- A description of a consumer's rights (see next slides)
  - Right to opt-out of sale or sharing, and how to do so
  - Right to limit use of Sensitive PI and how to do so (CA only, if applicable),
- Method for submitting rights requests
- How to appeal a controller's action with regard to a consumer's request (CO, CT, VA)
- Authorized agent submissions

GT GreenbergTraurig

Basic Individual Rights

- Right to Access. ! CPRA Modified by CPRA
- Right to Delete. ! CCPA Modified by CPRA
- Right to Opt-Out of Sale of PI to Third Parties
- Right to Nondiscrimination.
- Opt-In Rights for Minors. ! CCPA Modified by CPRA

GT GreenbergTraurig

New CPRA Individual Rights

- **Right to Correction**.. ***(Not recognized by UCPA)***
- **Right to Opt-Out of Use of Sensitive PI**. Consumers may limit the use and disclosure of sensitive PI for certain "secondary" purposes. ***(Not recognized by UCPA; VCDPA and CPA require opt-in consent for processing sensitive PI)***
- **Right to Opt Out of Automated Decision-Making Technology**. Consumers may opt out of ADM technology, including "profiling," in relation to decisions re: a consumer's work perf, economic situation, health, personal prefs, interests, reliability, behavior, location or movements. ***(Not recognized by UCPA)***
- **Right to Access Information About Automated Decision Making** ***(Not recognized by UCPA)***

Minimization

GT GreenbergTraurig

Data Minimization

California, Virginia, Colorado and Connecticut require:

A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data is processed.

Impact: Organizations must review every instance where they collect PI from consumers and assess if the PI collected is reasonably necessary, and in relation to any PI sought that is not necessary consumers should have a choice whether they want to voluntarily provide.

Sharing and Selling, Opt-outs and GPC

GT GreenbergTraurig

Selling & Sharing

- CCPA has a consumer PI sale opt out right, which CPRA extends to the sharing of PI…

- And CO and UT afford a right to opt-out of the sale of PD and targeted advertising…

- While VA and CT follow CO and UT – plus a consumer right to opt-out of profiling.

GT GreenbergTraurig

Selling & Sharing (cont.)

- The CPRA maintains the CCPA's "sale" definition and adds a new def for "sharing" PI, which involves "cross-contextual behavioral advertising." No monetary or other valuable consideration is required for sharing!
- Big implications for the use of 3rd party trackers on websites or 3rd party SDKs/integrations on mobile.
- Operational changes re: "Do Not Sell or Share My Personal Information" links and supporting tools and/or web forms.

GT GreenbergTraurig

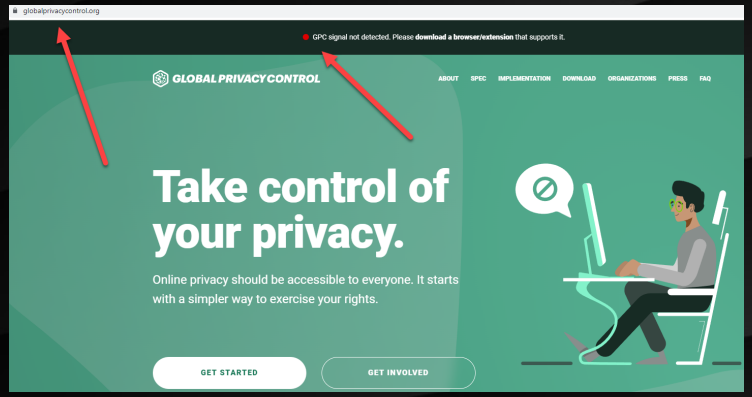
Global Privacy Control (GPC)

- CPRA describes two options for businesses to accept opt-out requests from consumers.
  - a business may provide an opt out link on its website; or
  - in lieu of these links, is for a business to allow consumers to opt out via a GPC.
- California Attorney General has contacted businesses about their status in relation to honoring a proposed GPC signal.
  - Despite the CPRA text, CA AG has taken the position that honoring the GPC signal is required of all companies.
- Virginia does not yet require honoring GPC-signal based sale opt-out requests (although the VCDPA's working group has recommended this).
- Colorado (by 7.1.24), and Connecticut (by 1.1.25) envision the use of a user-selected universal opt-out mechanism.

GT GreenbergTraurig

User-Enabled Opt-Out Preference Signals

- Available via browser or browser extension.
- Similar to DNT header…the browser sends the GPC signal via an HTTP header to all websites that consumer—er, browser—visits…which the server must recognize.
- Full implementation specs available here: https://globalprivacycontrol.github.io/gpc-spec/



GT GreenbergTraurig

Possible Approaches to Digital Compliance

- Inventory and categorize website trackers, mobile app SDKs & other 3Ps
- Review contracts/agmnts to determine SP/processor vs 3Ps
- Evaluate support for browser-level GPC or of other signals…
- The possibility of moving to an “opt-in” approach for all non-SP/processor third-parties, to attempt meeting the “sale” carve-out?

GT GreenbergTraurig

How to Actually Do This on Web or App

- Add DNSoSMPI link on website footer and app settings; and/or
- Honor GPC/opt-out preference signals (web-only for now!); and/or
- Assess technical options…IAB MSPA/GPP? Tag manager? Block lists? Cookie consent banner or other tool? In-app vs. mobile web? What is your time/date-stamp record for capturing an opt-out/in?; or
- Effectively stop using all third-party cookies and trackers?

Sensitive Personal Information

GT GreenbergTraurig

CA: Sensitive Personal Information Def.

Collection or processing of information for the purpose of inferring characteristics about a consumer and includes:

(1) Personal information that reveals the following information of a consumer:

- (A) social security number (SSN), driver's license, state identification card, or passport number;
- (B) account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- (C) precise geolocation;
- (D) racial or ethnic origin, religious or philosophical beliefs, or union membership;
- (E) mail, email, or text message content, unless the business is the intended recipient of the communication; or
- (F) genetic data.

(2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer.

- (B) Personal information collected and analyzed concerning a consumer's health.
- (C) Personal information collected and analyzed concerning a consumer's sex life, or sexual orientation.

GT GreenbergTraurig

CA Only - Limited Data Use of SPI /Opt-Out

- If a business processes SPI for uses that do not fit within performing the services set forth in § 1798.140(e)(2), (4), (5) and (8), for the purpose of inferring characteristics it must:

  (a) provide a notice to consumers explaining those uses; and

  (b) allow consumers to opt out of those uses by providing a "clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information."

GT GreenbergTraurig

Sensitive Personal Information

- States other than CA require opt-in consent to process SPI.
- However, SPI has more limited definition

COLORADO	CONNECTICUT	UTAH	VIRGINIA
§ 6-1-1303(24). "Sensitive Data" means: 1. Personal data revealing an individual's racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status; or 2. Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or 3. Personal data from a known child.	§ 1(27). "Sensitive data" means personal data that includes: (A) data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation or citizenship or immigration status, (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, (C) personal data collected from a known child, or (D) precise geolocation data.	§ 13-61-101(32). (a) "Sensitive data" means: (i) personal data that reveals: (A) an individual's racial or ethnic origin; (B) an individual's religious beliefs; (C) an individual's sexual orientation; (D) an individual's citizenship or immigration status; or (E) information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional; (ii) the processing of genetic personal data or biometric data, if the processing is for the purpose of identifying a specific individual; or (iii) specific geolocation data. "Sensitive data" does not include personal data that reveals an individual's: (i) racial or ethnic origin, if the personal data is processed by a video communication service; or (ii) if the personal data is processed by a person licensed to provide health care under Title 26, Chapter 21, Health Care Facility Licensing and Inspection Act, or Title 58, Occupations and Professions, information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional.	§ 59.1-575. "Sensitive Data" means a category of personal data that includes: 1. Personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; 2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person; 3. The personal data collected from a known child; or 4. Precise geolocation data.

Enforcement

Cure Periods, Fines & Penalties

GT GreenbergTraurig

Cure Periods

- **CCPA**: 30 days from being notified of alleged non-compliance.
- **CPRA**: 30-day cure period is removed. Instead, the CPPA has discretionary authority to provide a business a time within which is must cure—but the CPPA does not have to do so.
  - N.b. – it is not possible to cure a data breach by implementing and maintaining "reasonable security procedures and practices" *after* a breach.
- **CO**: Prior to any enforcement action, the CO AG or DAs must issue a notice of violation, after which the company has 60 days to cure or enforcement may ensue. This provision sunsets on 1/1/2025.
- **CT**: Same as Colorado.
- **UT**: 30-days from receipt of a written notice from the AG.
- **VA**: Same as Utah. No sunset.

GT GreenbergTraurig

Enforcement Matters

- **Enforcement authority:**
  - CA = Attorney General (AG) / California Privacy Protection Agency; CO = AG / DAs; CT/VA/UT = AG.
- **Private right of action:** No, except CA allows for a PRoA in relation to data breaches, which the CPRA expanded to include any consumer email address in combination with a password or security question.
- **Penalties:** Varies by state; most set a $7,500 limit per violation.
- **Rulemakings** all around, especially in the Golden and Centennial States, so far…

Contracting Requirements

GT GreenbergTraurig

Contracting Requirements

- All state data protection laws explicitly require businesses/controllers to enter into contracts with entities to whom they transfer PI.
  - The CPRA establishes three categories of recipients – service providers, contractors, and third parties – and sets forth a baseline set of prohibitions that must be contractually addressed when businesses sell or share PI to such entities.
  - Other states have one category of recipients called data processors.
- Virginia, Colorado and Connecticut allow controllers reasonable audits and inspection, and processors may opt to conduct an independent audit at their own expense annually if the controller agrees.

GT GreenbergTraurig

CPRA – Contractual Requirements

CPRA seeks to protect PI as it flows from businesses to (a) service providers, (b) contractors and (c) third parties.

- Third Party Contracts
  - Third party agrees to use limitation and CPRA compliance.
  - Third party agree to allow business to audit third party to ensure its processing remains compliant with CPRA and take appropriate steps to remediate unauthorized use of PI.
  - Requires third party to notify business if it can no longer meet CPRA obligations.
- Contractor and Service Provider Contracts. All of the above must be included, **plus must**
  - Prohibit the service provider from using, retaining or disclosing PI for any purposes than to perform business purpose(s)).
  - Prohibit the service provider from selling or sharing the PI.
  - Prohibit the service provider from retaining, using or disclosing PI outside of the direct business relationship between the service provider and the business.
  - Prohibit the service provider from combining PI from different sources.
  - Requires the service provider to notify the business of sub-processors.
  - Requires the service provider to bind sub-processors by written contract to the same obligations.
  - Requires the service provider to permit business to audit/monitor compliance ("may" used in relation to service providers).
  - Contractors must certify their understanding of and compliance with the contractual requirements (not required for service providers).

CPRA's Contractual Requirements

Under CPRA, Service Providers and Contractors are also required to:

- Refrain from using sensitive personal information upon instructions from the business.
- Assist the business in responding to a verifiable consumer request, including by:
  - Providing the business with the consumer's personal information in the service provider or contractor's possession.
  - Correcting or enabling the business to correct inaccurate information.
  - Deleting or helping the business delete personal information received, at the business's direction
  - Notifying any of its own service providers or contractors to delete personal information.
- Assist the business through appropriate technical and organizational measures in complying with the requirement to implement reasonable security procedures and practices, when it has collected personal information pursuant to a written contract with the business.

Children's PI

GT GreenbergTraurig

Differences in the State Laws

- All states except CA define child as being under 13; CA has different rules for under 13, and 13-15.
- California requires parental consent for any “sale” or “sharing” of personal data of child under 13, and opt-in consent from child 13-15 years of age.
- Virginia, Colorado and Connecticut follow COPPA, requiring opt-in consent for all online and offline processing of personal data of children under 13.

GT GreenbergTraurig

Practical Impact

Website/apps directed at children

- Age gate, and parental consent flow mechanism in place prior to collecting any personal data from children under 13 (in compliance with COPPA)
- California – Age Gate
  - Opt-in consent for sharing/selling cookies on sites directed to children 13-15
  - For any user that identifies as being under 13, do not have any sharing/selling cookies fire

GT GreenbergTraurig

Speaker Contact Information

Gretchen A. Ramos	Darren Abernethy
ramosg@gtlaw.com	abernethyd@gtlaw.com
T: 415.655.1319	T: 415.655.1261
https://www.linkedin.com/in/gretchenramos/	https://www.linkedin.com/in/djabernethy/