MINTZ

Navigating Today's Privacy Compliance Landscape

December 8, 2022

Speakers

Cynthia J. Larose
Chair, Privacy & Cybersecurity Practice, Mintz

CJLarose@mintz.com

- Chair of Mintz's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E)
- Represents companies in information, communications, and technology, including e-commerce and other electronic transactions
- Counsels clients through all stages of the "corporate lifecycle," from start-ups, through mid- and later-stage financings, to IPO, and has broad experience in technology and business law, including online contracting issues, licensing, domain name issues, software development, and complex outsourcing transactions

Maureen Hernberg
Leader – Privacy Compliance
McKinsey

Maureen_Hernberg@mckinsey.com

- Spent decades in the health care industry and is a privacy expert. Holds, two privacy certification from IAPP; CIPP and CIPM, and is active in local and international privacy circles
- Has held numerous roles in data privacy including global privacy leader for Medtronic's Minimally Invasive Therapy Group and, currently leads McKinsey's Privacy Compliance function.
- Solution oriented privacy practitioner, who is passionate about the intersection of business, law, and technology. Enjoys partnering with teams to navigate privacy by design and data governance issues.

Housekeeping Notes for Audience

- The webinar will be recorded.
  - The recording and slides will be sent to all participants after the webinar.
- If you cannot hear the presentation, please go to the “Audio & Video" tab or click on the Microphone icon to receive other options for connecting your audio.
- If you are calling in through your computer, please be sure to turn up the computer's volume.
- Attendees will be muted throughout.
- Questions will be answered after the presentation in the interest of time.
  - Use the Q&A application to submit a question.

How are the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) Related?

- CPRA amends CCPA, and expands several important areas of CCPA.
- CPRA creates a new regulatory authority – California Privacy Protection Authority (CPPA) who, along with the California AG, is drafting regulation and will have civil enforcement authority.
- CPPA has issued modifications and is currently in comment period.

Does the CPRA Apply to My Business?

- "A sole proprietorship, partnership, limited liability company, corporation, or other legal entities organized or operated **for the profit** or financial benefit of its shareholders or other owners, **that collects consumers' personal information, or on the behalf of which such information is collected**, and that alone, or jointly with others, **determines the purposes and means of the processing of consumers' personal information,** that does business in the State of California, and that meets one of the three thresholds described below:
- Annual gross revenues in excess of $25 million dollars
  - Applies to global revenue – not limited to California
- Annually buys, receives, sells, or shares for cross-contextual behavioral advertising, the personal information of 100,000 or more consumers or households
  - "Consumer" = California resident
- Derives 50% or more of its annual revenues from selling or sharing personal information of consumers

ONLY ONE OF THESE THREE MUST BE MET FOR THE CPRA TO APPLY

CPRA's Path: Enactment to Enforcement

California Privacy Rights Act of 2020

11/3/2020	CPRA approved by California voters
12/16/2020	CPRA takes effect but most provisions not operative until 2023
1/1/2022	"Look back period: CPRA's right to know or right of access applies to personal information collected after this date.

California Privacy Rights Act of 2020

7/1/2022	CPRA deadline for adopting final regulations*
1/1/2023	CPRA in full effect. B2B and employee exemptions expire
7/1/2023	Enforcement of CPRA to begin

New Category: "Sensitive Personal Information"

- SSN, driver's license, state ID card, or passport number;
- Account log-in, financial account, debit/credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- Precise geolocation;
- Racial or ethnic origin, religious or philosophical beliefs, or union membership;
- *Contents of a consumer's mail, email, and text messages, unless the business is the intended recipient of the communication;*
- Genetic data;
- Processing of biometric information for the purpose of uniquely identifying a consumer;
- Personal information collected and analyzed concerning a consumer's health; or
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation

What Happened to the CCPA's employee and "B2B" exemptions?

The exemptions will cease to exist on January 1, 2023

Many businesses must now evaluate vast employee and B2B transactions to understand implications and take action to comply.

There are Significant Operational Implications

- Consider whether sensitive personal information is collected or processed "for the purpose of inferring characteristics about the consumer" – regulations may amplify on this.
- Separate disclosure required "at or before the point of collection", including purpose for collection and use, and whether such information is sold or shared.
- Business must **notify users** about their collection and use of cookies and create **a *simple* way to opt out** of selling or sharing their data within the context of cookies.
- Create a "Limit the Use of My Sensitive Personal Information" link and allow consumers to limit
- If the use or disclosure of sensitive PI changes, business must notify the consumers and provide them the right to limit use and/or disclosure
- *Requires businesses to flow these obligations down to service providers and contractor via contract*
- *Service providers and contractors are required to comply with these obligations after receiving instructions from the business*

Practical changes are required
Notices Required for Employees and Job Applicants

✓"Notice at collection" and Privacy Notice

✓The Employee/Applicant Privacy Notice will be different than the public-facing website notice

✓If you are a "business" for purposes of the CCPA, all employee residing in California (including remote employees) will be considered "consumers" for purposes of notice, rights, etc., regardless of whether the employer has a physical presence in California

The Notice At Collection Must

- Reflect the means through which a business collects the information itself.
- Outline the purpose for collecting and using sensitive personal information and personal information.
- Indicate if collected information is sold or shared.
- Include the length of time the business intends to retain each category of personal information, or where this is impossible, the criteria used to determine retention.
- NOTE: The CPRA codifies the obligation for covered businesses to establish strong data hygiene. Data retention and destruction policies are required.

Employee “Sensitive Personal Information” Disclosure

- Employers should audit categories of sensitive personal information that are collected and document reasons for such collection.
- CPRA does not require an employer to present the categories of personal information collected as a matter of course as “sensitive” unless the information is collected or processed for the purposes of “inferring characteristics” about the individual.
- Businesses generally do not collect or process sensitive PI with the purposes of inferring characteristics of employees.
- Typical processing purposes of sensitive PI: fulfill traditional HR functions such as processing payroll and providing benefits.

Privacy Notice for HR Data

- Subtle difference between “notice at collection” and the “privacy notice”
- “Notice at collection” = forward looking
- “Privacy Notice” = disclosure of information collected by the employer in the 12 months prior to the effective date of the policy
  - Notice effective as of January 1, 2023 must cover the collection and handling of PI starting January 1, 2022
  - Must be comprehensive

Consumer Rights under the CPRA (Modified CCPA Rights)

- **Right to Delete**
  - Businesses now required to notify third parties to delete any consumer PI bought or received, subject to some exceptions
- **Right to Know**
  - PI that must be reflected in a “right to know” response is expanded to include PI collected beyond the prior 12 month period, if collected after 1/1/22
- **Right to Opt Out**
  - Opt-out right now covers “sharing” of PI for cross-contextual behavioral advertising
- **Opt in Rights for Minors**
  - Extends the opt-in right to explicitly include the sharing of PI for behavioral advertising purposes. Must wait 12 months before asking a minor for consent to share or sell PI after the opt out.
- **Right to Data Portability**
  - Consumers may request that the business transmit specific pieces of PI to another entity, to the extent technically feasible

Consumer Rights under the CPRA (New Rights)

- **Right to Correction**
  - Consumers may request any correction of their PI held by a business if that information is inaccurate
- **Right to Opt Out of Automated Decision Making Technology**
  - Regulations will address ability of consumers to opt out of automated decision making technology, including "profiling," in connection decisions related to a consumer's work performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements
- **Right to Access Information About Automated Decision Making**
  - Authorizes regulations allowing consumers to make access requests seeking meaningful information about the logic involved in the decision making processes and a description of the likely outcome based on that process
- **Right to Restrict Sensitive PI**
  - Consumers may limit the use and disclosure of sensitive PI for certain secondary purposes, including prohibiting businesses from disclosing sensitive PI to third parties, subject to certain exceptions

Comparison of State Laws to CCPA/CPRA

CCPA/CPRA vs. Virginia Consumer Data Protection Act

	California	Virginia
Scope	**$25 million in annual gross revenue** **OR** **Process data of at least 100,000 consumers** **OR** **Derive at least 50% of revenues from *selling or sharing* data**	Process data of at least 100,000 consumers OR Process data of at least 25,000 AND derive at least 50% of gross revenue from *selling* data
Effective Date	January 1, 2023	January 1, 2023
Definition of Sale	Money or other valuable consideration	Money
Definition of Personal Data	Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.	Information that is linked or reasonably liked to an identifiable natural person

CCPA/CPRA vs. Virginia Consumer Data Protection Act

	California	Virginia
Definition of Personal Data (cont)	Excludes de-identified or publicly available data. Publicly available data = information that is lawfully available from government records	Excludes de-identified or publicly available data Publicly available data = information that is lawfully available from government records or information that a controller reasonably believes the consumer has lawfully made available to the general public
Sensitive Data	Includes: race or ethnicity, religion, sexual orientation, citizenship, genetic data, biometric data used to identify a person, precise geolocation, union membership, SSN, Driver's license or passport number, financial account with password or security code, and *contents of mail, email or texts (unless the business is the intended recipient)* Process must self-restrict to certain uses, or provide notice and opportunity to opt out	Includes: race or ethnicity, religion, health, sexual orientation, citizenship, genetic or biometric data used to identify a person, precise geolocation, and personal data of children Processor needs consent to process

CCPA/CPRA vs. Virginia Consumer Data Protection Act

	California	Virginia
Notable Exceptions	HIPAA Data GLBA data Nonprofits Higher Education FCRA	HIPAA entities GLBA entities Nonprofits Higher Education FCRA Employment data Commercial B2B data
Consumer Rights	Right to access Right to correct Right to delete Right to portability Right to opt out of sale *or sharing* Right to nondiscrimination Right to notice at or before collection	Right to access Right to correct Right to delete Right to portability Right to opt out of sale, *profiling, or targeted ads* Right to nondiscrimination **Right to appeal**

CCPA/CPRA vs. Virginia Consumer Data Protection Act

	California	Virginia
Timing to Respond	45 days, with an additional 45 when reasonably necessary 15 days for opt-out requests	45 days, with an additional 45 days when reasonably necessary Right to Appeal – 60 days to respond
Controller Duties	Transparency Purpose specification Data minimization Data security/care Nondiscrimination Sensitive data caution Avoid secondary use Pass requests to delete on to third parties	Transparency Purpose specification Data minimization Data security/care Nondiscrimination Sensitive data consent Avoid secondary use

CCPA/CPRA vs. Virginia Consumer Data Protection Act

	California	Virginia
Privacy Notice Requirements	Categories of data Purpose for processing each category How to exercise consumer rights Categories of data shared with third parties Categories of third parties with whom data is shares Any sale or sharing of data and how to opt out Clear and conspicuous link to opt of sale *on homepage* Duration of retention of each data category Categories of sources of data Categories of sensitive PI, including any extraneous use and consumer's right to opt out	Categories of data Purpose for processing each category How to exercise consumer rights Categories of data shared with third parties Categories of third parties with whom data is shared Any sale of data *or targeted advertising* and how to opt out

CCPA/CPRA vs. Virginia Consumer Data Protection Act

	California	Virginia
Private Right of Action	Yes; in the event of a data breach only. Up to $750 per consumer per incident, or actual damages	No
Enforcement	AG and California Privacy Protection Agency	AG – can impose up to $7,500 fine per violation
Safe Harbor	None	30-day cure period

CCPA/CPRA vs. Virginia Consumer Data Protection Act

	California	Virginia
Required Terms in Data Processing Agreements	Limited and specific processing instructions Obligate the service provider to comply with CPRA Assist controller with auditing and complying Allows controller to halt and remediate improper processing Notice to controller if processor cannot comply	Processing instructions Purpose of processing Type of data processed Duration of processing and obligations of both parties Confidentiality duties Duties to return or delete data Assist controller with auditing and complying Flow down compliance obligations to subcontractors, in writing

CCPA/CPRA vs. Virginia Consumer Data Protection Act

	California	Virginia
Data Processing Impact Assessments	Required when: Processing sensitive data Data presents significant consumer risk Risks of processing outweigh the consumer benefits	Required when: Processing sensitive data Data presents a heightened risk of harm Data is used for targeted advertising Data is for sale Data is used for profiling when it creates harm; unfair, deceptive, or disparate treatment; or an offensive intrusion on the solitude or private affairs of consumers

CCPA/CPRA vs. Connecticut Data Privacy Act

	California	Connecticut
Scope	$25 million in annual gross revenue OR Process data of at least 100,000 consumers OR Derive at least 50% of revenues from selling or sharing data	Process data of at least 100,000 consumers (excluding purely payment transactions) OR Process data of at least 25,000 AND derive at least 50% of gross revenue from selling data
Effective Date	January 1, 2023	July 1, 2023
Definition of Sale	Money or other valuable consideration	Money
Definition of Personal Data	Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.	Information that is linked or reasonably liked to an identifiable person

CCPA/CPRA vs. Connecticut Data Privacy Act

	California	Connecticut
Definition of Personal Data (cont)	Excludes de-identified or publicly available data. Publicly available data = information that is lawfully available from government records	Excludes de-identified or publicly available data Publicly available data = information that is lawfully available from government records or information that a controller reasonably believes the consumer has lawfully made available to the general public
Sensitive Data	Includes: race or ethnicity, religion, sexual orientation, citizenship, genetic data, biometric data used to identify a person, precise geolocation, union membership, SSN, Driver's license or passport number, financial account with password or security code, and contents of mail, email or texts (unless the business is the intended recipient) Process must self-restrict to certain uses, or provide notice and opportunity to opt out	Includes: race or ethnicity, religion, health, sexual orientation, citizenship, genetic or biometric data used to identify a person, precise geolocation, and personal data of children Processor needs consent to process

CCPA/CPRA vs. Connecticut Data Privacy Act

	California	Connecticut
Notable Exceptions	HIPAA Data GLBA data Nonprofits Higher Education FCRA	HIPAA entities GLBA entities Nonprofits Higher Education FCRA Employment data Commercial B2B data National securities associations
Consumer Rights	Right to access Right to correct Right to delete Right to portability Right to opt out of sale or sharing Right to nondiscrimination Right to notice at or before collection	Right to access Right to correct Right to delete Right to portability Right to opt out of sale, profiling, or targeted ads Right to appeal **Duty on controllers not to violate existing laws against discrimination**

CCPA/CPRA vs. Connecticut Data Privacy Act

	California	Connecticut
Timing to Respond	45 days, with an additional 45 when reasonably necessary 15 days for opt-out requests	45 days, with an additional 45 days when reasonably necessary Right to Appeal – 60 days to respond
Controller Duties	Transparency Purpose specification Data minimization Data security/care Nondiscrimination Sensitive data caution Avoid secondary use Pass requests to delete on to third parties	Transparency Purpose specification Data minimization Data security/care Nondiscrimination Sensitive data consent Avoid secondary use

CCPA/CPRA vs. Connecticut Data Privacy Act

	California	Connecticut
Privacy Notice Requirements	Categories of data Purpose for processing each category How to exercise consumer rights Categories of data shared with third parties Categories of third parties with whom data is shares Any sale or sharing of data and how to opt out Clear and conspicuous link to opt of sale on homepage Duration of retention of each data category Categories of sources of data Categories of sensitive PI, including any extraneous use and consumer's right to opt out	Categories of data Purpose for processing How to exercise consumer rights and appeal Categories of data shared with third parties Categories of third parties with whom data is shared Any sale of data or targeted advertising Clear and conspicuous link to a webpage for opting out of sale or targeted advertising Active email address for how to contact the controller

CCPA/CPRA vs. Connecticut Data Privacy Act

	California	Connecticut
Private Right of Action	Yes; in the event of a data breach only. Up to $750 per consumer per incident, or actual damages	No
Enforcement	AG and California Privacy Protection Agency	AG – can impose up to $5,000 fine per willful violation
Safe Harbor	None	60-day cure period (ends January 1, 2025)

CCPA/CPRA vs. Connecticut Data Privacy Act

	California	Connecticut
Required Terms in Data Processing Agreements	Limited and specific processing instructions Obligate the service provider to comply with CPRA Assist controller with auditing and complying Allows controller to halt and remediate improper processing Notice to controller if processor cannot comply	Processing instructions Purpose of processing Type of data processed Duration of processing Rights and obligations of both parties Confidentiality duties Duties to return or delete data Assist controller with auditing and complying Flow down compliance obligations to subcontractors, in writing

CCPA/CPRA vs. Connecticut Data Privacy Act

	California	Connecticut
Data Processing Impact Assessments	Required when: Processing sensitive data Data presents significant consumer risk Risks of processing outweigh the consumer benefits	Required when: Processing sensitive data Data presents a heightened risk of harm Data is used for targeted advertising Data is for sale Data is used for profiling when it creates harm; unfair, deceptive, or disparate treatment; or an offensive intrusion on the solitude or private affairs of consumers

If we already comply with GDPR will we have more ‘to dos’ for CPRA?

Good news – bad news. If your privacy framework is anchored around compliance with GDPR and other key privacy regulation you will have a head-start. The bad news is there is more to do.

Highlights and important distinctions*

US - most significant legislative privacy development.

CCPA’s impact will be far reaching and is global like GDPR.

In terms of obligation and accountability GDPR places much more emphasis on ‘how to meet obligations’ e.g., appoint a data protection officer, conduct Data Privacy Impact Assessments (DPIAs), keep a Records of Processing Activity (ROPA).

CPRA is more focused on steps to comply versus accountability mechanisms.

*Not exhaustive

Aspect	GDPR	CPRA
Scope	All personal data is in scope Specifically defines sensitive personal data	Less comprehensive carves out certain personal data; health info. under HIPAA, clinical trials, credit related.
Key Definitions	Focus on natural persons No residency requirements extra territorial	Centered on consumers or who are natural persons *AND* California residents Unclear if it applies to businesses outside of CA collecting etc. such personal data
Legal Basis	Framed around having a legal basis for processing. Lawful basis are prescribed and must be documented	Focused on restrictions for collection, selling, processing does not call out that there must be a legal basis for processing
Data Management	Security safeguards, data minimization, and general data hygiene i.e. data retention is emphasized Carve out for anonymized data; some allowances for pseudonymization	Reasonable security standards required, principle of data minimization and adherence to data retention principles Allowances for pseudonymization
Individual Rights	Free of charge and enables requests for deletion or erasure with caveats i.e. balance with legal obligations Physical and environmental security Respond within 30 days; can extend (x2) Method: written,orally and by other means, i.e., electronic means	Free of charge and enables requests for deletion Respond within 45 days; potentially extend to 90 days Systems acquisition, development, and maintenance Businesses must minimally enable two mechanisms; toll free number and website (if applicable)

MINTZ

ACC Association of Corporate Counsel NORTHEAST

THANK YOU

Questions?