MORRISON
FOERSTER

CRACKING THE CCPA CODE:
COMPLYING IN THE MIDST OF ITS AMBIGUITIES, HIDDEN "GOTCHAS," AND MISUNDERSTOOD PROVISIONS

Kristen Mathews
Miriam Wugmeister

June 12, 2019

The California Consumer Privacy Act

- Arguably the most significant U.S. privacy development ever
- Replaced the controversial privacy ballot initiative
- Fast tracked to the Governor's desk and signed into law June 28, 2018 (AB 375); amended September 23, 2018 (SB 1121)
- Government affairs efforts continue; amendments proposed; AG rulewriting deadline extended to July 1, 2020
- Operative on January 1, 2020

CCPA Overview

Enforcement begins: 2020

- Earlier of: 6 months after final regulations or July 1, 2020

"Business": for-profit businesses that collect and control California residents' personal information, and:

- (a) have annual gross revenues in excess of $25 million; or
- (b) receive or disclose the personal information of 50,000 or more California residents, households, or devices on an annual basis; or
- (c) derive 50 percent or more of their annual revenues from selling California residents' personal information.

"Doing business in California" = red herring

The Act also draws in corporate affiliates of such businesses that share their branding, even if they do not meet definition of "Business."

Consumer Rights

Consumer Rights: Detail

- CCPA gives consumers 4 basic rights:

1. Right to know what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
2. Right to "opt out" of a business selling their personal information to 3rd parties;
3. Right to have a business delete their personal information (with some exceptions); and
4. Right to receive equal service and pricing from a business, even if they exercise their privacy rights under the CCPA (with some exceptions).

POLL

GDPR is more rigorous than CCPA, so businesses that are in compliance with GDPR should also be in compliance with the CCPA.

True

False

CCPA vs. GDPR

- GDPR-style compliance measures can take businesses a long way toward compliance with CCPA, **but not all of the way**
- Although it doesn't cover everything from GDPR, **CCPA adds some new obligations not in GDPR**
  - Privacy policy/notices must use CCPA-enumerated PI categories
  - Must provide notice of whether (or not) PI may be sold
  - Separate listings of categories of PI collected, sold, or shared with third parties for business purposes
  - Must offer at least two designated methods for making CCPA requests
  - Businesses that sell PI must include a "Do Not Sell My Personal Information" link on their homepage and web pages that collect PI

"Personal Information" Means…

- Broad definition of Personal Information
  - "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
  - CCPA provides a non-exhaustive list of examples, some of which are expansive. Everything you would expect, plus:
    - Identifier of consumer, family, or device over time and across different services
    - Device identifiers
    - IP addresses
    - Online tracking technologies
    - Browsing history and search history
    - Geolocation data

The broadest definition of Personal Information of any U.S. privacy law

"Consumer" Means Californian

- A natural person who is a **CA resident**
  - A "resident," as defined in CA's income tax code, includes any individual who is:
    - In CA for other than a temporary or transitory purpose; or
    - Domiciled in CA, but outside of CA for a temporary or transitory purpose
- No customer-type nexus needed
  - Includes employees, independent contractors, and visitors to company premises
  - Anticipated amendment (AB 25) will carve out employees and independent contractors of the business

Companies will need to decide if they want to limit these rights to CA residents or expand beyond CA

A business subject to the CCPA must update its privacy policy every year.

True

False

Privacy Policy Requirements

- Online privacy policies and "California-specific description of consumers' privacy rights"
- Required content
  - **Description** of consumer privacy "rights"
  - **Categories** of PI collected, sold, and disclosed for a business purpose in the past 12 months
  - **Methods** for submitting rights requests
- Do not process additional categories of Personal Information or make additional uses of Personal Information without revising Privacy Policy
- Update Privacy Policy **at least once** every 12 months

POLL

If a California resident exercises her right to access her personal information (PI), a business does not have to disclose inferences that it has drawn about her because those are just guesses, not factual information.

True

False

Access to Specific PI

- A consumer has a right, **twice a year**, to request that a business provide the consumer with **"[t]he specific pieces of personal information"** collected about the consumer
  - Greatly affected by the breadth of the definition of PI (*e.g.*, IP addresses, online tracking identifiers, audio and video, inferences)
- Limited, however, to the PI collected in the past **12 months**

POLL

Like GDPR, CCPA provides consumers with data portability rights.

True

False

Data Portability

- Unlike GDPR, CCPA doesn't provide a separate right of data portability
- In honoring a consumer's access right, however, the disclosure of PI must be provided free of charge and within 45 days of the request in a **readily useable** format that is also **portable**:
  - Through the consumer's account with the business (but cannot require consumer to create an account to make a request); or
  - If the consumer does not have an account, by mail or electronically at the consumer's option

POLL

If a California resident asks a business to delete all of the PI it has about her, it must do so.

True

False

Right to Deletion

- A consumer has the right to request that a business delete "any" PI about the consumer that the business has collected **"from the consumer"**
- A business also must **direct** its service providers to delete the consumer's PI from the service provider's records
- Exceptions to deletion right:
  - To continue transactions with consumer
  - To protect business and its products
  - To defend business's rights
  - Free speech
  - To comply with law enforcement subpoenas, etc., and other legal obligations
  - To conduct research in the public interest
  - Internal uses reasonably expected by consumer

POLL

A business subject to the CCPA must obtain the opt-in consent of a parent or guardian for the sale of PI of a consumer who is under 16 years old.

True

False

Opt-In Consent for Sale of PI

- May not sell PI of a consumer if the business has "actual knowledge" that the consumer is under 16 years old, unless:
  - For a consumer between the ages of 13 and 16: The consumer has "affirmatively authorized" the sale
  - For a consumer under the age of 13: The consumer's parent or guardian has "affirmatively authorized" the sale
- A business that "willfully disregards" the consumer's age shall be deemed to have had "actual knowledge" of the consumer's age.

What is a "sale" to which the opt-out right applies?

Does recipient have the right to use the personal info for its own, or third party, benefit?

If yes, but only in aggregated and de-identified form, does the aggregation and de-identification meet CCPA's standards?

Is there an exchange of money or other valuable consideration for the personal info?

E.g., a trade for other data? A lower price for services?

Complex cases:

- Online advertising partners, where price for ad services accounts for their use of data for benefit of ad ecosystem
- Mutual exchange of customer lists
- Cooperative customer information databases, where all participants share in benefits of pooled data

POLL

CCPA limits a business' ability to offer financial incentives to consumers for providing their PI.

True

False

Financial Incentives/Anti-Discrimination

- May offer financial incentives for **collection, sale, or deletion** of PI
- May also offer a different price, rate, level, or quality of goods or services **if that price or difference is directly related to the value provided to the consumer by the consumer's data**
- If a business offers any financial incentives, it must notify consumers of the financial incentives as part of its privacy disclosures
- But a business may only enter a consumer into a financial incentive program if the consumer gives prior **opt-in consent** in response to a clear description of the material terms of the financial incentive program
    - A consumer may revoke consent at any time

A company may not charge different prices to a consumer merely for exercising an individual right, but may charge different prices if the company can demonstrate the difference in value

POLL

CCPA exempts healthcare providers and other covered entities that are subject to HIPAA as well as financial institutions and other entities that are subject to GLBA.

True

False

Exceptions, or Lack Thereof

- Exceptions focused on specific federal privacy laws, e.g.:
  - HIPAA/CMIA exception applies to **data** covered by these laws, and to **entities** that are regulated by these laws with regard to **other patient information** that is maintained in accordance with these laws
  - GLBA exception applies to **NPI** as defined by, and treated pursuant to, the **GLBA**
- Exceptions focused on compliance with law and compliance with legal process (*e.g.*, subpoenas)
- Exception where compliance with the Act would violate an evidentiary privilege under California law

POLL

A consumer can sue a business for statutory damages under the CCPA in connection with a security incident of biometric information.

True

False

Private Right of Action

- A consumer can sue:
  - If nonencrypted or nonredacted "personal information" (as defined in the **CA disposal law**) is subject to an **unauthorized access and exfiltration, theft, or disclosure**
  - As a result of a "violation of the duty to implement and maintain reasonable security procedures and practices . . . to protect the personal information"
- SB 1121 clarifies scope limited to above
- Available relief:
  - Statutory damages of **$100 to $750** "per consumer per incident" or actual damages, whichever is greater;
  - Injunctive or declaratory relief; or
  - Any other relief the court deems proper

POLL

Before suing under the CCPA, a consumer must give notice to the business and to the California Attorney General.

True

False

Procedural Hurdles for Consumers

- Pre-suit notice to business for **statutory damages**
  - 30 days' written notice identifying the "specific provisions of this title" allegedly violated
- Opportunity to **cure**
  - No lawsuit if the business cures the violation and provides an **"express written statement"** that the violation has been cured and "no further violations [will] occur"
  - Ability to sue if the business continues to violate "this title" in breach of the express written statement
- SB 1121 amendment eliminated requirement to notify the California AG within 30 days of filing the action

Enforcement

- Enforcement authority vested in the California AG
- A business violates the CCPA if "it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance"
  - Unclear whether the AG can bring an enforcement action only after providing an opportunity to cure
- Remedies:
  - Injunction
  - Civil penalties of **$2,500** (unintentional) and **$7,500** (intentional) per violation

POLL

The earliest the AG can bring an enforcement action under the CCPA is January 1, 2020.

True

False

Enforcement

- SB 1121 delayed the AG's authority to bring enforcement actions until **July 1, 2020, or six months after the AG issues final rules** (whichever is sooner)
- But the CCPA will be **operative** as of January 1, 2020
  - If the AG does not issue final rules **until January 1, 2020, or later**, no enforcement action until July 1, 2020
  - If the AG issues final rules **before January 1, 2020**, the AG could theoretically bring an enforcement action between January 1, 2020, and June 30, 2020 (depending on the exact date of final rulemaking)

CCPA To Do List

Prepare to receive, process and respond to individuals' requests

- Have internal written procedures for reviewing, processing, and responding to requests (e.g., website form, email address, automated vs. manual?)
- How to authenticate requestors
- Validate legality of requests (e.g., does the law afford them what they are asking for?)
- Determine whether an exception applies
- Required time frames for response
- Direct service providers to delete as well
- Do not add PI from individual rights request into CRM, or use it for anything else
- Don't ask for permission to sell again for 12 months

CCPA To Do List

Ensure that methods to aggregate, de-identify and pseudonymize personal information meet the Act's standards

- Definitional standards on aggregation, de-identification and pseudonymization are high
- Effective pseudonymization and de-identification are necessary to use data for research (plus other conditions on research)
- Effective aggregation and de-identification can avoid the Act altogether
  - Aggregate: Pool x records together and remove identifiers of consumer, household or device. ("x" is not defined.)
  - De-identify: numerous detailed tech safeguards and business processes must be in place.

CCPA To Do List

Ensure that business' use of publicly available personal information conforms to CCPA's standards

- "Publicly available" means information that is lawfully made available from federal, state, or local government records
- Information is not "publicly available" if used for purpose that is not compatible with the purpose for which the data is maintained by the government and made available to the business

CCPA To Do List

Agreements with Service Providers

- Does company disclose categories of its service providers and categories of personal information shared with them?
- Does business have a standard data protection agreement in place with the service provider (with prohibition on retention, use, or disclosure of personal information outside of scope of services)?
- If yes, there may not be a need to amend the service provider agreement

If amendment is necessary, add required provisions:

- Can only collect, retain, use and disclose data for specified purpose, and not outside the business relationship between the companies
- Can not resell data
- Delete PI upon direction
- Certification of compliance by service provider may be helpful

CCPA To Do List

Ensure that contracts with consumers (website terms of use, service contracts, etc.) do not waive or limit their rights under CCPA

- Limitation of liability provisions cannot preclude CCPA's statutory and actual damages provisions
- Alternative dispute provisions and limits on consumer redress cannot preclude consumers' enforcement rights under CCPA

Revise these provisions to give business maximum benefit

CCPA To Do List

Requirements When Buying or Selling Personal Information

- When buying personal information from another business, beware of duty to provide disclosures to consumers before reselling it
- When selling or buying a business, beware of limits on buyer's rights to alter data protection commitments (e.g., to change the privacy policy)

Other Key CCPA Considerations

- **Training**: Individuals responsible for handling PI and CCPA inquiries must be trained on CCPA requirements and how to direct consumers to exercise their rights
- **Security breaches**: No new requirements, but CCPA creates new civil penalties and private right of action
- **AG rule-making**: Many CCPA requirements will be clarified or expanded through upcoming Attorney General rule-making; stay tuned

POLL

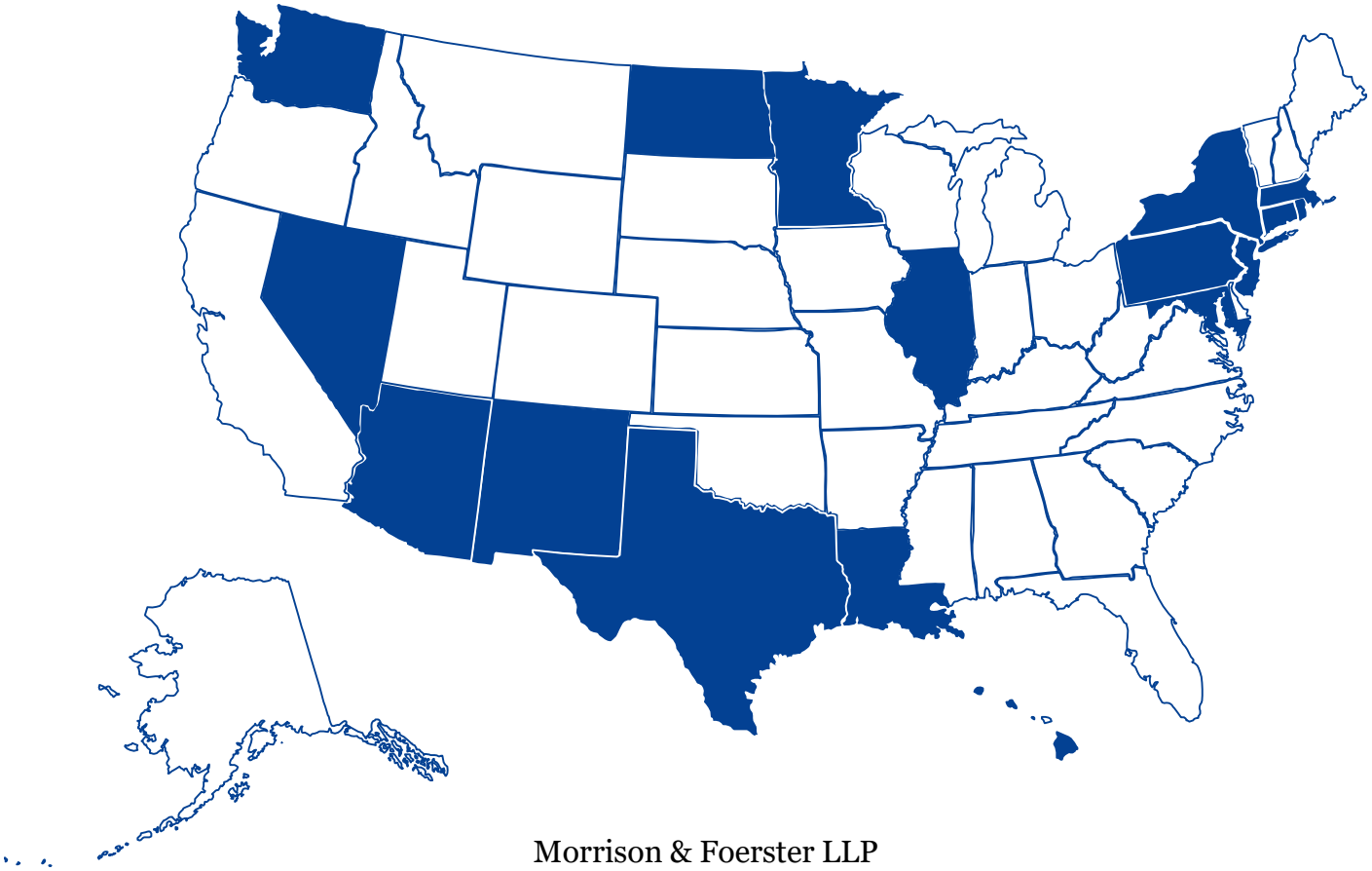
Since the CCPA passed, more than ten other states have introduced CCPA-like bills.

True

False

CCPA-like Bills

- Since the CCPA passed, **17 states** have introduced CCPA-like bills.
- Some of these bills have been significantly amended and/or limited in scope.



Additional Resources

- Visit MoFo's CCPA Resource Center for client alerts, checklists, and other resources
- View MoFo's on-demand webinars:
  - "Unpacking the California Consumer Privacy Act of 2018," July 2018
  - "Privacy Across the Atlantic: Comparing EU GDPR and California Consumer Privacy Act of 2018," September 2018