Deciphering the California Consumer Privacy Act of 2018 (CCPA)

Brian Liceaga, CISSP
Tim Kane, JD
1. Background on Privacy
2. CCPA
3. Analysis and Predictions
“Freedom of thought, control over one’s body, solitude in one’s home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogations.”

- Daniel J. Solove
Fair Information Practice Principles (FIPPs)

1. Collection limitation ✓
2. Data quality ✗
3. Purpose specification ✓
4. Use limitation ✓
5. Security ✓
6. Openness ✓
7. Individual participation ✓
8. Accountability ✓
CCPA Summary

• California’s “GDPR” (EU General Data Protection Regulation)
• Effective January 1, 2020
• Rulemaking – Attorney General
• Applies to
  – California Consumers
  – Businesses that collect PI
  – Service Providers
  – Third parties
CCPA Facts

- Own your personal information
- Control your personal information
- Secure your information
- Hold big corporations accountable
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
Categories

Identifiers
- Biometrics
  - Audio, electronic, visual, thermal, olfactory, etc.

Geolocation data
- Network activity information

Commercial information
- Characteristics of protected classifications

Inferences
- PI described in subdivision (e) of Section 1798.80

Professional or employment, related information

Education information
Exclusions to Personal Information

- publicly available information (lawfully made available from federal, state, or local government records)
- Consumer information that is deidentified or aggregate consumer information
Who’s Protected

- Consumers
  - natural person
  - resident of California
Business - Qualitative

• For-profit legal entity

• Collects* PI
  – or for whom collected

• Determines purposes and means of processing PI

• Does business in the State of California

• Plus
  – any parent that controls, or subsidiary controlled by, business, and
  – shares common branding with
Business - Quantitative

• Satisfies one or more of the following thresholds

1. annual gross revenues
   - > $25M

2. alone/combination annually buys or sells PI* (commercial purposes)
   - 50K or more consumers, households, or devices

3. annual revenues
   - 50% or more from selling PI
Service Provider

• For-profit legal entities
• Processes information for a business
• To which the business discloses a consumer’s personal information for a business purpose
Consumer Rights

• Right of notice
• Right to opt-out/opt-in
  – Rights of minors
• Right to access
  – Right to data portability
• Right to deletion
• Right to equal treatment
Consumer Rights – Notice & Opt-Out

• Right to notice
  – The categories of personal information collected
  – Purposes for which the personal information is collected
  – Categories of third parties with whom shared
  – If personal information sold or disclosed

• Right to opt-out of the sale of personal information
Consumer Rights - Minors

- Opt-in required for minors
- Applies if the business has actual knowledge or “willfully disregards” the consumer is a minor
- Between 13-16 years of age
- Less than 13 years of age
  - Parent or guardian consent
Consumer Rights - Access

• Right to access personal information
  – 2 or more methods for submitting requests
  – Deliver within 45 of verifiable consumer request (*plus extension*)
  – 12 month period preceding the request
  – Not more than twice per 12 month period

• Must provide
  – The categories as well as specific personal information it has collected
  – The purpose of collecting or selling this information
  – The categories of sources and third parties whom this information is collected, sold, or shared
Consumer Rights – Data Portability

• Mail
• Electronically
  – Portable
  – To the extent technically feasible, readily useable format that allows the consumer to transmit this information

• https://datatransferproject.dev/
Consumer Rights - Deletion

• Right to have personal information deleted
  – Business directs service providers to delete as well

• Exceptions
  – Complete ongoing transaction, service, or contract
  – Detect security incidents, protect against malicious activity; prosecute; debug
    • E.g. logs
  – Exercise free speech
  – Comply with a legal obligation
Consumer Rights - Equal Treatment

• No discrimination for exercising privacy rights:
  – Denying goods or services
  – Charging different prices or rates
  – Providing a different level or quality of goods or services

• Exceptions *
  – If that difference is reasonably related to the value provided to the consumer by the consumer’s data
  – Financial incentive programs
Private Right of Action

• Need not show actual damages

• Remedies
  – Damages — greater of
    • Statutory damages: $100 -> $700 / incident
    • Actual damages
  – Injunctive relief
  – “Any other relief the court deems proper”
Limitations

- Only for data breaches - unauthorized access to non-encrypted or non-redacted PI
- Consumer must notify business
  - Except in action solely for actual money damages
- Starts a 30-day *cure* period
- *PI* is really a subset of PI
- Business defense “reasonable security procedures and practices appropriate to the nature of the information”
Rulemaking & Enforcement by AG

• Guidance from Attorney General
  – Rulemaking
  – Advisory opinions

• Enforcement against business
  – 30 days to *cure* the alleged violation

• Violations
  – Injunctive relief
  – Penalties
    • Up to $2,500 per violation
    • $7,500 per intentional violation
Exceptions to Laws

• Federal and State Laws
  – e.g., HIPAA, GLBA, DPPA, FCRA

• Information collected as part of a clinical trial (+ qualifiers)
• Review and update
  – privacy practices/statements
  – agreements with third parties
• Create a data inventory and analyze data flows
• Training
• Define a process for consumer information access requests
  – Two or more designated methods for submitting requests
  – Consumer verification and data portability
• Create opt-out/opt-in mechanism
  – Address verification of minors
• Add a “Do Not Sell My Personal Information” link
• Implement and maintain “reasonable” security practices and procedures
  – Data protection, auditing/logging, incident response
A “Rough” Draft

• Terms that are not defined
  – “Household”, “cure”, “reasonable security”, etc.

• Errors and inconsistent language

• Ambiguities

• Guidance
  – Rulemaking Process has begun via public forms
    • “Today our goal is to listen. We are not able to answer questions or respond to comments.”
  – Advisory opinions
Trend Setting

• Other states to follow (cf data breach laws)
• A federal privacy law is unlikely any time soon
• International privacy law will continue to expand
• Companies will err on the side of caution
  – Make updated privacy rights available to larger customer base
• Large enterprises will be the first target and set precedent
Resources

- **CCPA**
  - [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121)

- **Data Transfer Project**
  - [https://datatransferproject.dev/](https://datatransferproject.dev/)
  - [https://github.com/google/data-transfer-project/](https://github.com/google/data-transfer-project/)

- **IAPP**

- **California Referendum Website**
  - [https://www.caprivacy.org/](https://www.caprivacy.org/)

- **Eric Goldman (criticisms)**