



California Consumer Privacy Act 101



Presented by:

Travis LeBlanc

attorney advertisement

Copyright © Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. The content of this packet is an introduction to Cooley LLP's capabilities and is not intended, by itself, to provide legal advice or create an attorney-client relationship. Prior results do not guarantee future outcome.

cyber/data/privacy

Agenda

1. Background
2. CCPA Overview
3. FAQ
4. Questions

Background

Cooley

Summer 2018

2018



Privacy



GDPR (May)



California Consumer Privacy Act (June)



Adequacy for EU transfer (July)



LGPD (August)

California Consumer Privacy Act of 2018 (CCPA)

- Unanimously approved by CA legislature and signed into law on June 27, 2018
- “Technical amendments” (SB 1121) enacted on September 23, 2018 and more amendments expected to address drafting errors
- CA AG to adopt regulations
- High risk of enforcement by experienced AG & plaintiffs bar
 - Key distinction from GDPR
 - Points to more conservative approach to compliance

How Will CCPA Impact Business?

- Global impact
- Estimated 500,000 US businesses affected per IAPP
- Threat to ad-supported free services and data brokerage?
- California-specific websites/products may emerge
- Increased compliance costs (especially processing access/deletion/opt out requests)
- Increased potential liability and class action litigation
- Copycat laws in more than a dozen other states
- Push for preemptive federal legislation
- Is CCPA constitutional?

CCPA Overview

Cooley

CCPA Key Dates

- January-March 2019
 - California DOJ Public Forums
 - DOJ comment period - 1305 pages of public comments
- **January 1, 2020**
 - CCPA takes effect
 - 12 month “lookback”
 - Private right of action for security breaches
 - Cities and counties may bring § 17200 action for unlawful, unfair or fraudulent business practices
- **July 1, 2020**
 - Deadline for CA AG to adopt regulations
- **Earlier of July 1, 2020 or 6 months after final regulations**
 - CA AG may bring enforcement action

Who Must Comply with CCPA?

- For-profit “businesses” that collect Personal Information (“**PI**”) of California residents and:
 - Have annual gross revenues more than \$25 million;
 - Annually obtain PI of 50,000 or more California “residents”, households or devices; or
 - Derive 50% or more annual revenue from “selling” California residents’ PI.
- A covered business’s affiliates that use the same branding, even if those affiliates don’t surpass these thresholds themselves
- Possible exceptions for businesses that do not do business in California and whose commercial conduct takes place “wholly outside of California”

Who Must Comply with CCPA?

- Service Providers
 - For-profit legal entity that processes information on behalf of a business pursuant to a written contract
 - Contract must prohibit personal information use for any purpose other than for the specific purpose of performing the services specified in the contract
- Third Parties
 - Any party other than a “service provider” to which a “business” discloses Personal Information

What Data Does CCPA Cover?

- “Personal information” of “consumers” (i.e., California residents)

“Personal information” means 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.

What Rights Does CCPA Give Californians?

- Right to know
 - Categories of PI collected
 - Categories of sources of PI
 - Categories of PI disclosed for a business purpose or sold
 - Categories of third parties to whom PI was sold (broken down by category of PI sold) or disclosed
 - Business or commercial purposes for collecting or selling PI
- Right to obtain a copy of their PI (in a portable format where feasible)
- Right to opt out of the “sale” of their PI
- Right to require deletion of their PI
- Right to exercise their rights free from discrimination (e.g., different service or price)

What is a “Sale” of Personal Information?

- Broadly defined but there are exceptions for sharing with:
 - Affiliates (with same branding)
 - Service providers (if service necessary for business purpose and service provider contractually prohibited from using PI except to provide service)
 - Acquirers in M&A and similar transactions (but notice required if they make different use of PI)
- Implications
 - Most other commercial relationships caught in sale restrictions
 - Targeted online advertising / data brokerage = sale?
 - Names for wholly-owned subs matter if they have PI access
 - Need to ensure vendor contracts contain required wording
 - Need for careful M&A due diligence of target’s privacy practices and assessment of notice requirements

“Sell”...means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.

What Must Businesses Do to Comply?

Notice & Transparency

Update privacy policy to provide required disclosures (covering prior 12 months' activity)

On homepage put [Do Not Sell My Personal Information](#) link to instructions to opt out of sale of PI

Provide privacy notice at point of PI collection, including at brick and mortar stores

Establish toll-free phone # for individuals to call to opt out of sale of PI

Individual Rights

Verify identities of individuals requesting to exercise rights

Honor requests to exercise rights within 45 days (+45 day extension when reasonably necessary)

Train relevant employees to assist individuals with privacy-related questions and requests

Consent

Obtain prior opt in consent to enter consumer into financial incentive (e.g., rewards) programs

Obtain “affirmative authorization” to sell PI of minors - from minor if under 16 and of parent if under 13

Avoid asking for opt-in consent to sell PI for 12 months after opt out

What Must Service Providers and Third Parties Do to Comply?

- Third parties
 - A third party that purchases PI from a business cannot resell unless the third party provides the consumer with explicit notice AND an opportunity to opt out of such resale
 - Third party vis-à-vis another business is also a business in its own right
- Service providers
 - No direct obligations and no liability for obligations of “business” for which it provides service
 - But must comply with its contracts with the business

FAQ

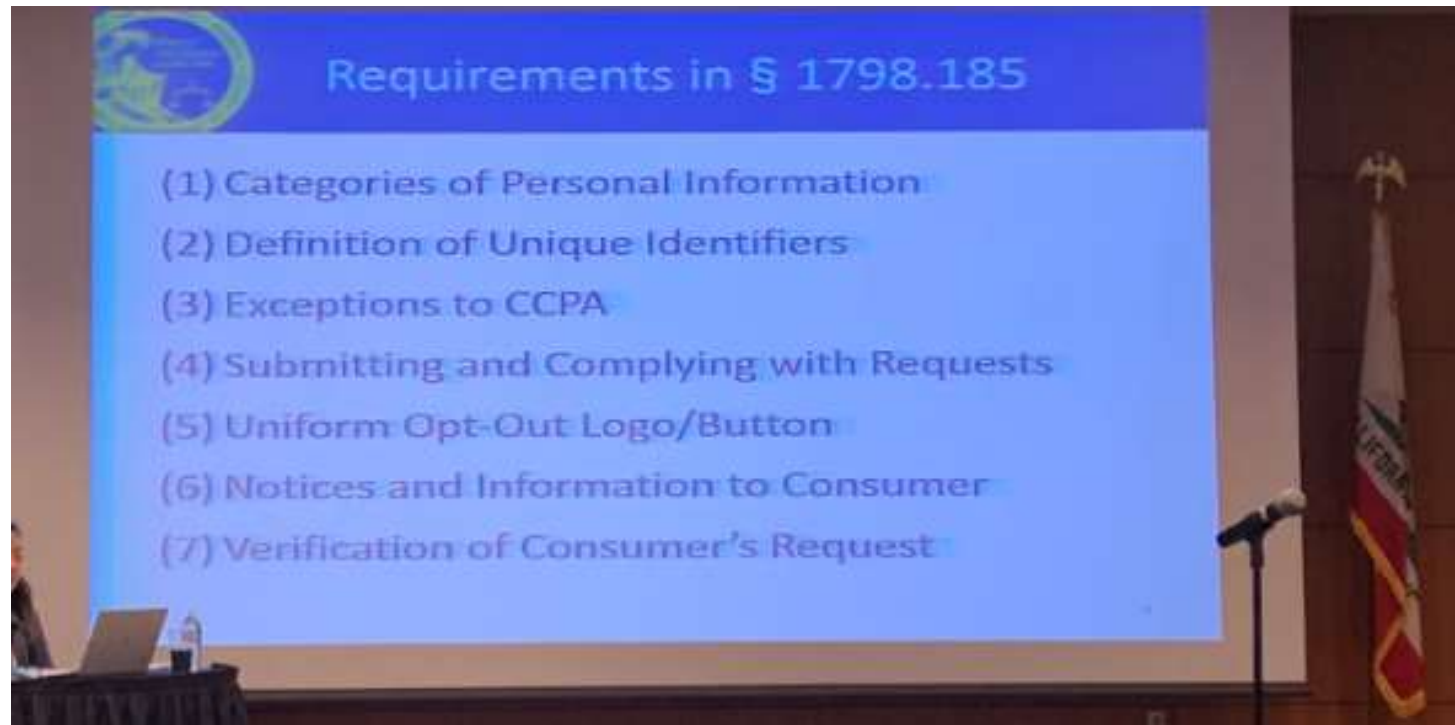
Cooley

What Are the Penalties?

- Private right of action for data breaches resulting from failure to maintain “reasonable security”
 - Greater of statutory damages (\$100-750 per consumer per incident) or actual damages
 - No actual harm requirement, but consumer must give businesses 30 days to cure
- CA Attorney General civil actions for violations after 30 day cure period
 - Injunctions
 - Penalties of \$2,500 per violation or \$7,500 per intentional violation
- Purported waivers of CCPA rights or remedies (class action waivers, arbitration agreements?) “void and unenforceable”

Will the California AG Issue Guidance?

- The CCPA requires California AG rules/guidance on the following areas:



- The California AG has discretion to offer guidance in other areas
- Sign up for updates from AG's office: <https://oag.ca.gov/privacy/ccpa/subscribe>

What is the Expected Enforcement Climate?

- AG is under-resourced and will be focused on low-hanging fruit
 - Large data sets
 - Sensitive data
- AG advocating to broaden private right of action to ease enforcement burden
- Cities and counties may bring § 17200 action for unlawful, unfair or fraudulent business practices
- Significant increase in the number of data breach class actions and the amount of settlements

Does CCPA Apply to Employees?

- Short answer: Yes, for now
- California ~~Consumer~~ Resident Privacy Act
- Implications
 - Employee rights to notice, access and deletion → employee trolling, leverage in disputes?
 - Unauthorized access to certain HR data → security breach liability to staff?
 - M&A transactions → Employee notice obligation?
- AB 25 would amend CCPA to carve out job applicants to, an employee of, a contractor of, or an agent on behalf of, the business

Should We Wait to See if CCPA is Amended?

- Selected bills proposing amendments

AB 25: Excludes job applicants and employees and other workers from the definition of consumer

AB 873: Excludes from definition of PI “household” information and information that “is capable of being associated with” an individual

AB 1760: Mandates businesses obtain consumers’ opt-in consent before “sharing” PI and expands enforcement to include county district attorneys and city attorneys

SB 753: Exempts from a “sale” the disclosure of a unique identifier in order to serve or audit an advertisement to a consumer

AB 1355: Revises nondiscrimination provisions to clarify that differential treatment of a consumer who has exercised CCPA rights must be reasonably related to value provided to the business by the consumer’s personal information

Will Congress Preempt the CCPA?

- Robust debate is currently underway in both the House of Representatives and Senate regarding crafting comprehensive federal privacy legislation
- Preemption of state privacy laws like as CCPA has emerged as a top issue but no guarantee that there will be agreement on language
- House and Senate Republicans are arguing for a uniform set of standards while Democrats are arguing that states are best positioned to protect consumers



Does GDPR Compliance = CCPA Compliance?

- **Bad news:** The short answer is no
 - CCPA “personal information” arguably broader than GDPR “personal data”
 - Access and deletion rights and exceptions differ
 - Disclosure requirements differ
 - Plaintiffs’ bar and CA AG is a different (and potentially more challenging) audience
- **Good news:** You can leverage the people, process and technology deployed for GDPR
 - Companies with strong privacy governance will adapt faster
 - GDPR Art. 30 registers can help with CCPA data mapping needs
 - Access and deletion requests pose similar technical and administrative challenges

What Should We Prioritize?

- Analyzing business model threats (e.g., ad supported free services, data brokerage, lead generation)
- Closing security gaps – private right of action is a strong incentive
- Building technical capability to respond to access/deletion/opt out requests
- True consumer data (business contact data is lower priority)
- Sensitive data sets (e.g., children's, health, biometric)
- Amend contract templates sooner than later to reduce amendment burden
- Assess level of effort to address employee/personnel data, but hold off as long as you can and see if proposed exemption passes

What Should I Be Doing Now?

Year	Actions
Q2 2019	<ul style="list-style-type: none">• Get started – deadline will come fast• Understand requirements• Monitor amendment activity and AG rulemaking; consider rulemaking participation• Consider CCPA in risk factor disclosures (e.g., in public filings)• Consider CCPA risk/issues in strategic transactions (e.g., M&A, financings)• Identify CCPA compliance resources and kick-off CCPA compliance projects• Perform due diligence and gap assessment
Q3-Q4 2019	<ul style="list-style-type: none">• Execute remediation plan• Build technical capabilities to honor access, deletion, opt out and other rights• Prepare privacy policy and other externally-facing updates to take effect on 1/1/2020
2020	<ul style="list-style-type: none">• January 1, 2020: CCPA takes effect• July 1, 2020: Deadline for final regulations• July 1, 2020 (or 6 months after final regs if earlier): AG may bring enforcement action

Follow CCPA at our Blog

cdp.cooley.com

Cooley

Questions?

Cooley