The Countdown Begins:
What You Need to Know About CCPA Compliance and Enforcement

December 2019

Proskauer

Roadmap

Background

Requirements and Compliance

Enforcement and Litigation

“There is a growing campaign by the plaintiffs’ bar to target data privacy and security in hopes of striking it rich in a new goldmine on the level of the asbestos litigation of the 1970s, 1980s, and 1990s.”

- The U.S. Chamber of Commerce Institute for Legal Reform

Overview of U.S. Patchwork of Privacy Laws

- State Laws
- Industry Specific Law
  - HIPAA
  - FERPA
  - GLBA
- Data Breach and Notification Laws
  - New York SHIELD ACT

Don’t Forget About the “Fourth Branch”

- Privacy and Cybersecurity Initiatives by Federal Agencies
  - SEC
  - FTC

Background

What is the CCPA?

Background

- Landmark Privacy Law
- Gives consumers certain rights with respect to their personal information—the rights to know about and control the personal information that a business collects about them
- Requires certain businesses to enable consumers to exercise their rights without discrimination

Key Terms

- **Consumer**: “a natural person who is a California Resident”
- **Personal Information**: “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”
  - Does not include publicly available information—information that is lawfully made available from federal, state, or local government records

Key Terms

- **Business**: for-profit entity "that does business in the State of California, and that satisfies one or more of the following thresholds:
  - Has annual gross revenues in excess of twenty-five million dollars
  - "[B]uys or receives for the business's commercial purposes, sells, or share for the commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices"
  - "Derives 50 percent or more of its annual revenues from selling consumers' personal information"

Key Terms

- **Verifiable Consumer Request**: request that is made by a consumer that the business can "reasonably verify"
  - Business has the responsibility for establishing and complying with a reasonable method
  - "Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business"
  - Consider factors relating to feasibility of verification, the nature of the information, and the likelihood of risk

General Requirements for Businesses

- **Notify** consumers about the categories of personal information it collects and why
- Upon request, **delete** requested consumer personal information
  - Permanently and completely erase the personal information on its existing systems with the exception of archived or back-up systems
  - Deidentifying the personal information
  - Aggregating the personal information

General Requirements for Businesses

- Post a **Privacy Policy** that provides a description of consumers' rights
- Allow consumers to exercise these rights without **discrimination**
- Not use the collected personal information for **any other purpose** than the purpose disclosed at the time of collection

Requirements and Compliance

Notices, Generally

- Must be:
  - Easy to read and understandable to an average person
  - Use plain, straightforward language and avoid technical or legal jargon
  - Noticeable
  - Available in the languages in which the business uses to communicate with consumers in its ordinary course
  - Accessible

Notices: Privacy Policy

- Must be available in an additional format that allows a consumer to print it out as a separate document
- Must be posted with a conspicuous link, using the word “Privacy” on the business’s website or landing page

Notices: Privacy Policy Requirements

- Must include:
  - Information about consumer's right to know about personal information collected, disclosed, or sold. Must also provide instructions for how a consumer can find this information
  - State whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months
    - List the categories of personal information, if any, that it disclosed to third parties
    - State whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization

Notices: Privacy Policy Requirements

- Must include information about:
  - Right to delete personal information
    - How to submit a verifiable consumer request to delete
    - Describe how the business will verify consumer requests
      - Have a two-step process for online requests to delete
  - Right to opt-out of the sale of personal information
  - Right to non-discrimination
- Business shall confirm receipt of the request within 10 days and provide information about how the business will process the request

Notices: When Collecting Information

- Must include:
  - List of categories of personal information, in a way that is understandable to the consumer
  - For each category of personal information, the business or commercial purpose(s) for which it will be used
  - If the business sells personal information—a link to opt out
  - The link should be titled: “Do Not Sell My Personal Information” or “Do Not Sell My Info”
  - Link to the business’s privacy policy

Notices: When Collecting Information

- If a business does not collect information directly from the consumer it **does not** have to provide a notice **at the time of collection**
- But, before it can **sell** a consumer's information, it must:
  - Contact the consumer to provide notice
  - Contact the source of personal information to:
    - Confirm the source provided a notice at collection
    - Obtain signed attestations about how the notice was given

Notices: Financial Incentives for Selling Information

- Succinct summary of the financial incentive or price or service or difference offered
- Description of the material terms of the financial incentive or price of service difference
- How consumers can opt-in to the financial incentive or price or service difference
- Notification of the consumer's right to withdraw, and instructions for how
- An explanation of why the financial incentive or price or service difference is permitted

Consumer Requests

- Must provide consumers with a method for submitting requests to exercise their CCPA rights
  - Must give consumers two methods:
    - Toll-free phone number (mandatory)
    - If the business operates a website, an interactive webform accessible through the business's website or mobile app
- Must respond to the request within 45 days — the business can extend this period by an additional 45 days, if the business gives the consumer notice of the additional time in the first 45 days

Exemptions: GLBA

- Narrowly excludes “personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, and implementing regulations, or the California financial Information Privacy Act”
- Not a blanket exemption of business that are regulated by the GLBA
- GLBA-regulated entities are still subject to the CCPA data-breach consumer right of action

Exemptions: HIPAA

- Broadly exempts HIPAA-protected health information and HIPAA-covered entities
- HIPAA-covered entities are likely not subject to the CCPA data breach consumer right of action

Enforcement and Litigation

Enforcement: Generally

- Attorney General will not begin enforcing the CCPA until the earlier of July 1, 2020 or six months after the issuance of implementing regulations

Enforcement: Details

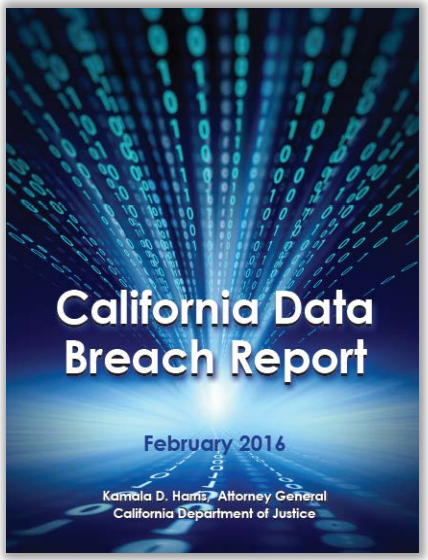
- The Attorney General will notify the business of an alleged violation
- The business has 30 days to cure the violation
- If not cured, the Attorney General will bring a civil action
- Penalties:
  - Injunction
  - $2,500 per violation
  - If intentional, $7,500 per violation

Litigation — Consumers, Generally

- Consumer may bring an action if their personal information is subject to a **data breach**
  - Personal Information must be nonencrypted and nonredacted
  - Subject to unauthorized access and exfiltration, theft, or disclosure
  - Data breach must be the result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information

Litigation — Consumers, Generally

What are “reasonable security” procedures and practices?



- Released by then-Attorney General Kamala Harris
- Analysis of reported data breaches from 2012-15
- Recommendation of a minimum level of information security to constitute “reasonable security”

Litigation — Consumers, Generally

What are “reasonable security” procedures and practices?

Recommendation 1:
The 20 controls in the Center for Internet Security’s Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.

Litigation — Consumer Requirements

- Before bringing an action, the consumer must give the business 30 days' written notice identifying the specific violations
- If the business cures and provides a written statement that the violations have been cured and that no further violations will occur, the consumer may not bring an action for statement of damages
  - If a written statement is provided, the consumer can, in the future, bring an action against the company of each breach of the written statement

Recommended Next Steps

Recommended Next Steps

- Step 1: Data Mapping
  - We developed a CCPA Questionnaire as a Tool
  - We can recommend and retain under attorney-client privilege data mapping third parties
- Step 2: Assess CCPA's Exemptions and document
- Step 3: Identify all service providers and third parties that client shares personal information with
- Step 4: Update Privacy Policies (Public facing). 12 Months

Recommended Next Steps

- Step 5: Update Privacy and Cybersecurity Procedures (Internal)
- Step 6: Prepare to receive and respond to data subject requests
- Step 7: Implement Reasonable Cybersecurity Protections and Breach Response Plan
- Step 8: Train Employees
- Step 9: Monitor CA AG Regulations, Other State Laws and Federal Legislation
- Step 10: Update Insurance Policies to Prepare for Privacy Litigation

Proskauer CCPA Team

Ryan R. Blaney
Partner
rblaney@proskauer.com

Christina H. Kroll
Associate
ckroll@proskauer.com

Lary Alan Rappaport
Partner
lrappaport@proskauer.com

Divya Taneja
Associate
dtaneja@proskauer.com

Proskauer