California Consumer Privacy Act (CCPA) and Other State Developments

Summary and Implications for Financial Institutions

January 8, 2019

Mark W. Brennan   Roshni Patel   Ashley Hutto-Schultz
What is the CCPA?
What is the CCPA? – Overview

- Regulates the collection, use, sale, and disclosure of information about Californian consumers and households.
  - Broadly scoped law with expansive definitions of key terms (e.g., “personal information”).
  - Requires businesses to provide detailed notice of personal data processing activities.
  - Grants individuals several rights including the right to opt out of the sale of personal information and the right to delete personal information.
  - Prohibits discrimination against consumers who exercise their rights.
  - Gives the California Attorney General authority to fine non-compliant businesses (up to $7,500 per intentional violation; uncapped liability, though there is a 30-day cure period).
  - Includes private right of action that allows consumers to sue after certain data breaches (allows for actual damages or statutory damages of $100-$750 per consumer per incident).
What is the CCPA? – Key Definitions

- **Personal information**: Any information associated with, relating to, or capable of being associated with, or that could reasonably be linked, directly or indirectly, with a particular consumer or household.
  - E.g., name, email address, purchasing histories, internet browsing or search history even if associated only with a IP address or online identifier like a cookie ID (without traditional identifying information), geolocation data, employment-related information, inferences drawn from other personal information, etc.
  - But excludes information that is collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (“GLBA”), and implementing regulations, or the California Financial Information Privacy Act (“CFIPA”).

- **Consumer**: A natural person who is a California resident. As drafted, it includes employees.

- **Collecting**: Buying, renting, obtaining, accessing, or receiving any personal information pertaining to a consumer by any means.

- **Sale**: Selling, renting, releasing, disclosing, transferring, making available, or otherwise communicating a consumer’s personal information to another business or a third party for monetary or other valuable consideration. “Sale” does not include transfers to service providers for “business purposes” if certain requirements are met.

- **Disclosure of personal information for business purposes**: Providing personal information to another person for operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected (e.g., building a profile on an consumer for other uses is outside of the definition of business purpose).
What is the CCPA? - Enforcement

• Attorney General
  – California’s Attorney General can enforce all provisions of the CCPA and its regulations.
    – AG is required to draft regulations by July 1, 2020. AG can’t enforce before July 1, 2020, but law takes effect Jan. 1, 2020 and can enforce violations back to that time.
  – Businesses will have 30 days to cure any alleged violations.
  – If violations not cured, AG can impose penalties of up to $2,500 per violation, or $7,500 per intentional violation.
  – Total liability is uncapped.

• Private Right of Action
  – Consumers are able to sue a business if certain types of their personal information (e.g., SSNs) are subject to unauthorized access, exfiltration, theft, or disclosure and the information was not encrypted or redacted.
  – Consumers are able to sue only if the breach was the result of the business failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.
  – Consumers may recover the greater of actual damages or statutory damages ($100-$750 per consumer per incident).
What is the CCPA? - Exceptions

- The CCPA does not interfere with a business’s ability to:
  - comply with federal, state, or local law;
  - comply with government requests;
  - cooperate with law enforcement agencies; and
  - exercise or defend legal claims.

- Some data and practices are exempted:
  - Health information governed by HIPAA or the Confidentiality of Medical Information Act;
  - the sale of information that is regulated under the Fair Credit Reporting Act (“FCRA”);
  - the collection, processing, sale, or disclosure of personal information pursuant to the Gramm-Leach-Bliley Act (“GLBA”); and
  - the collection, processing, sale, or disclosure of personal information pursuant to the Driver’s Privacy Protection Act of 1994.
Who is covered?
Who is covered?

- **Businesses**
  - The primary type of entity that is regulated by the CCPA.
  - “Business” means:
    - (1) Any for-profit entity that:
      - collects consumers’ personal information;
      - determines the purposes and means of processing that information;
      - does business in the State of California; and
      - satisfies one or more of the following thresholds:
        - Gross revenues exceeding $25,000,000;
        - Buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices per year; or
        - Derives at least 50 percent of its annual revenues from selling personal information.
    - (2) Any entity that controls, or is controlled by, a qualifying business if it shares common branding.
Who is covered? (cont’d)

• **Service providers**
  - Have limited direct obligations under the CCPA.
  - Relevant definition because certain transfers of personal information to service providers will not qualify as “sales” and can therefore be protected from the consumer opt-out right.
  - “Service provider” means any for-profit entity that:
    - processes personal information on behalf of a business; and
    - to which a business has disclosed personal information for a business purpose pursuant to a written contract that prohibits the provider from retaining, using, and disclosing personal information other than for the specific purpose of perform the service specified in the contract; or as the CCPA otherwise allows.

• **Third parties**
  - Have limited direct obligations under the CCPA.
  - Relevant definition because (1) notice obligations depend on identifying disclosures to “third parties” (e.g., list of categories of third parties to whom a consumer’s personal information was sold); and (2) the definition of “sale” includes all transfers of personal information to “third parties” for monetary or other valuable consideration.
  - “Third parties” include any person other than:
    - (1) the business that collects consumer personal information; or
    - (2) a person who receives personal information from a business pursuant to certain contractual limitations (similar to restrictions imposed on service providers).
How does the CCPA apply to Financial Institutions ("FIs")?
How Does the CCPA Apply to Financial Institutions?

• GLBA/CFIPA “consumers” and “customers” are a subset of CCPA “consumers”
  – The CCPA’s definition of “consumers” does not require a business to have a customer relationship with individuals in order for the CCPA to apply.
  – Under the CCPA, FIs will need to consider: employees; employees of business partners, service providers, etc.; individuals with whom the customer relationship has not yet been formed.

• The GLBA and CFIPA only protect “nonpublic personal information” (“NPI”), which is more narrowly defined than “personal information” under the CCPA
  – NPI is (i) personally identifiable financial information (“PIFI”); and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.”
  – PIFI is “any information: (i) a consumer provides to you to obtain a financial product or service from you; (ii) about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or (iii) you otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.”
How Does the CCPA Apply to FIs? (cont’d)

• **Employees and Applicants for Employment:** California residents who are employees or applicants for employment would be covered by the CCPA and their personal information would not be PIFI or NPI subject to the GLBA/CFIPA (absent providing a financial service to an employee).

• **Business Contacts:** Any information that a FI collects about employees of vendors or other business partners, such as contact information, would not be subject to the GLBA/CFIPA, so the exemption does not apply.

• **Commercial Customers:** The GLBA does not apply to information collected from commercial clients, including sole proprietorships or individuals seeking a product or service for a business purpose.

• **Customer Prospects and Leads:** If a FI obtains a list of leads for marketing activities or where it collects information about an individual who is interested in obtaining a product or service, but has not reached the threshold of becoming a GLBA consumer, information collected may not be covered by the exemption.

• **Website Visitors:** If a FI automatically collects certain information from a website visitor that is not a customer, the information (e.g., IP address, browsing history, search history) may not be covered by the exemption.
What does the CCPA require?
What does the CCPA require? – Notice Obligations

• At or before the point of collection, a business must inform consumers of:
  – Categories of personal information to be collected; and
  – Purposes for which it will be used.

• A business’s website privacy notice must include:
  – A description of consumer rights under the CCPA and the methods for exercising those rights;
  – A list of the categories of personal information the business has collected about consumers in the preceding 12 months;
  – A list of the categories of personal information the business has sold about consumers in the preceding 12 months, or the fact that it has not done so;
  – A list of the categories of personal information the business has disclosed about consumers for business purposes in the preceding 12 months, or the fact that it has not done so.
  – Categories of sources of personal information and commercial purposes for collecting or selling also required.

• Limited notice obligations imposed on third parties
  – A third party that receives personal information from a business via a sale is prohibited from subsequently selling that personal information unless the consumer:
    – Receives notice of the sale; and
    – Has an opportunity to opt out of the sale.
What does the CCPA require? – Consumer Rights

• Access Right
  – Right to be provided with certain information upon request, including:
    – The “specific pieces” of personal information” that the business has collected about the individual consumer over the prior 12 months;
    – The categories of personal information that the business sold about the individual consumer in the preceding 12 months, the categories of the third parties to whom such personal information was sold, and the specific categories of information that were sold to each category of third parties; and
    – The categories of personal information that the business disclosed about the individual consumer for a business purpose in the preceding 12 months, the categories of the third parties to whom such personal information was disclosed, and the specific categories of information that were disclosed to each category of third parties.

• Deletion Right
  – Right to delete personal information the business and its service providers hold about the consumer.
    – Several potential exceptions are available (e.g., information required for a transaction with the consumer, information that must be retained to meet legal obligation, information needed for internal use that is compatible with the context in which consumer provided the information, etc.).

• Sale Opt Out Right
  – Right to opt out of the sale of personal information.
    – Homepage must include a “Do Not Sell My Personal Information” link.
    – For minors under 16, must obtain opt-in consent for sales. If under 13, parental opt-in consent is required.
What does the CCPA require? – Discrimination & Financial Incentives

• Businesses may not “discriminate” against consumers for exercising their rights.
  – Discrimination includes (a) denying goods or services, (b) charging different prices or rates, (c) providing different level or quality of a good or service, or (d) suggesting exercising rights will lead to a different price or quality.
  – A business may charge different prices or provide different quality if the difference is reasonably related to “value provided to the consumer by the consumer’s data.”

• Businesses may offer financial incentives to consumers for the collection, sale, or deletion of the consumer’s personal information.
  – Consumers must have notice of the material terms of the program, provide opt in consent to participate, and be able to revoke consent at any time.
  – Revocation of consent arguably triggers the anti-discrimination provision referenced above.
Next steps
### Next Steps

<table>
<thead>
<tr>
<th>Action Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Legal Analysis**      | • Identify whether FI is subject to the CCPA.  
                          • Determine what FI should treat as “personal information” given breadth and what personal information falls under the scope of the GLBA/CFIPA exception.  
                          • Assess which non-traditional sharing arrangements may be subject to sales opt-outs (e.g., online data sharing).                                    |
| **Data Mapping**        | • Inventory data assets and processing activities that may include personal information of CA residents or households that does not fall under the GLBA/CFIPA exception (e.g., employee data).  
                          • Map data transfers, including to other affiliates, FIs, partners, and service providers.  
                          • Implement procedures to maintain accuracy of data maps.                                                                                      |
| **Third-party relationships** | • Review existing data sharing relationships and revise agreements, as needed, to minimize impact of opt-out rights.                                                                                       |
## Next Steps (cont’d)

<table>
<thead>
<tr>
<th>Action Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies and Procedures</td>
<td>• Design and implement policies to annually and accurately update privacy notices.</td>
</tr>
<tr>
<td></td>
<td>• Draft policies and procedures for responding to consumer rights requests.</td>
</tr>
<tr>
<td></td>
<td>• Update internal policies and procedures to account for CCPA, including regarding employee rights.</td>
</tr>
<tr>
<td></td>
<td>• Develop policies and procedures for ensuring compliance with anti-discrimination provisions.</td>
</tr>
<tr>
<td></td>
<td>• Create process and procedures to implement, maintain, track, and demonstrate reasonable security measures taken to protect personal information (especially the categories listed in the CCPA private right of action).</td>
</tr>
<tr>
<td></td>
<td>• Consider revising data retention policies in order to limit CCPA obligations.</td>
</tr>
<tr>
<td></td>
<td>• Develop materials to train relevant employees on CCPA obligations.</td>
</tr>
</tbody>
</table>
What are other states doing?
What Are Other States Doing?

- Other state developments on the privacy front
  - A comprehensive privacy bill may be on the way in Washington

- Topic-specific state laws continue to proliferate
  - NYDFS cybersecurity regulation: final implementation deadline in March 2019
  - Biometrics: e.g. Illinois’ Biometric Information Privacy Act which includes a private right of action for unlawful capture and storage of biometric data
    - Texas, Washington follow suit
  - Breach notification and substantive data security: Many states have been updating their laws; Colorado adopted Massachusetts-like law
  - Cyber safe harbor: Very interesting development in Ohio (S.B. 220, signed Aug. 2018)
“Hogan Lovells” or the “firm” is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word “partner” is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2018. All rights reserved