CALIFORNIA PRIVACY RIGHTS ACT:

FROM A CREDIT UNION'S PERSPECTIVE

Presented by: Joseph Garibyan, Esq.
November 10, 2022

STYSKAL, WIESE & MELCHIONE, LLP
SW&M
FINANCIAL INSTITUTION ATTORNEYS

Disclaimer

These materials were prepared by the attorneys of Styskal, Wiese & Melchione, LLP. Although this presentation was prepared with care, it is not designed to be a complete or definitive analysis of the law in this area. Moreover, this presentation was prepared with the understanding that it reflects the authors' perception of the state of the law as of this date. Furthermore, the information contained in this presentation is not intended to constitute and should not be received as legal advice and does not in any way create an attorney-client relationship.

If you have any questions, or require further information on these materials, please do not hesitate to call our office at (818) 241-0103.

STYSKAL, WIESE & MELCHIONE, LLP
SW&M
FINANCIAL INSTITUTION ATTORNEYS

Overview

- CPRA significant modification of CCPA. Going forward, we're referring to it as CCPA
- Takes effect January 1, 2023. Regulations still pending!
- Exceptions to coverage applicable to credit unions, such as exceptions pertaining to financial sector privacy laws (i.e., Gramm-Leach-Bliley Act)
- Data inventory, mapping and classification with under CCPA
- CCPA rights and requirements
- Penalties for non-compliance and enforcement mechanisms

Exceptions to Coverage

- Not a covered “business”
  - $25 million gross revenue
  - Annual collection or processing of personal information of 100,000 or more consumers.
  - Half or more of revenue generated from selling personal information
- Nonprofits are exempt. But credit unions are not-for-profits, not nonprofits.
- GLBA / CalFIPA / FCRA
- California residency
- Deidentified & aggregated information
- Publicly available information
- Human resource data (expires Jan. 1, 2023)
- Business-to-business (B2B) (expires Jan. 1, 2023)

Data Inventory, Mapping and Classification

- **Data inventory** (also referred to as data mapping) generally refers to the practice of identifying all of the data elements a business collects, the sources of the data, where the data is stored, how the data is used, and what ultimately happens to the data.

- **Data classification** is the process of organizing the data into meaningful categories that help enable businesses to treat such categories differently for a variety of business purposes, and most certainly for regulatory compliance purposes.

Data Inventory, Mapping and Classification

Classification under CCPA

- Residency in California
- Whether data is “personal information”
  - Consider exceptions like publicly available, deidentified or aggregated information

- GLBA/CalFIPA/FCRA
  - members for consumer accounts vs. business accounts
  - prospects for membership, leads, customer lists
  - non-member website visitors

- Human resources data
  - job applicants
  - past or current employees
  - Independent contractors, dependents, etc.

- B2B data
  - business contacts

Consumer Rights

- Right to Know (information & access)
- Right of Data Portability
- Right to Deletion
- Right of Correction
- Right of Non-Discrimination
- Right to Opt-Out of Sale
- Right to Opt-Out of Sharing for Cross-Context Behavioral Advertising
- Right to Limit Use or Disclosure of Sensitive Personal Information
- Right to Access Information About and Opt-Out of Automated Decision-Making

Right to Know (RTK)

- 12-month lookback period for requests to know has been removed for information collected on or after January 1, 2022.

- Businesses must provide information beyond the 12-month period preceding the request unless it involves disproportionate effort.

Right of Data Portability

Right to Data Portability expanded to require transfer to another entity if technically feasible

Right to Deletion

Right to Delete requires deletion by service providers, contractors or third parties unless impossible or disproportionate effort

Right of Correction

- Request taken the same way as a right to know and right to delete
- Verification process is also very similar to right to know and right to delete
- Determination of whether to grant right is based on totality of circumstances, including:
  - The nature of the personal information at issue (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).
  - The nature of the documentation upon which the business considers the personal information to be accurate (e.g., whether the documentation is from a trusted source, whether the documentation is verifiable, etc.)
  - The purpose for which the business collects, maintains, or uses the personal information. For example, if the personal information is essential to the functioning of the business, the business may require more documentation.
  - The impact on the consumer. For example, if the personal information has a negative impact on the consumer, the business may require less documentation.

Right to Opt-Out of Sale and Opt-Out of Sharing for Cross-Context Behavioral Advertisements

- "Sale" and "Sharing" for cross-context behavioral advertisements considered treated nearly the same
- Opt-Out Methods
  - "Do Not Sell or Share My Personal Information" Link
  - Alternative Opt-Out Link:
    - Must be titled "Your Privacy Choices" or "Your California Privacy Choices" and must include the following icon: 
    - Available as an option if business also must provide "Right to Limit Use of Sensitive Personal Information"
  - Opt-Out Preference Signals

Right to Limit Use or Disclosure of Sensitive Personal Information

What is sensitive personal information?

- Personal information that reveals a consumer's:
  - social security, driver's license, state identification card, or passport number;
  - account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
  - precise geolocation;
  - racial or ethnic origin;
  - religious or philosophical beliefs;
  - union membership; or
  - genetic data.
  - The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.
- The processing of biometric information for the purpose of uniquely identifying a consumer.
- Personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation

Right to Limit Use or Disclosure of Sensitive Personal Information

- Must get prior express consent of consumer before collecting or processing sensitive personal information for purposes other than the following (provide use is reasonably necessary and proportionate):
  - To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.
  - To prevent, detect, and investigate security incidents.
  - To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
  - To ensure the physical safety of natural persons.
  - For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business.
  - To perform services on behalf of the business.
  - To verify or maintain the quality or safety of a product, service or device that is owned, manufactured, manufactured for, or controlled by the business.
  - For purposes that do not infer characteristics about the consumer. For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer
- If a business does not use sensitive personal information for these limited purposes, it must provide an opt-out as well.
- Opt-out is via a ""Limit the Use of My Sensitive Personal Information" Link or Alternative Opt-Out Link discussed previously.

Right to Access Information About and Opt-Out of Automated Decision-Making

- Proposed regulations don't address this issue at all
- From GDPR and other consumer privacy statutes, it may be inferred that regulations will require some disclosure about the logic behind the automated decision-making process, risk-assessments, and right for consumers to object to fully automated processes that include profiling of consumer in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

HR Data and B2B Data Exemptions Expire

- Exceptions set to expire January 1, 2023
- For HR Data, must reconcile with Labor Code requirements with personnel records and wage records requests
  - Different timelines and substantive response requirements between Labor Code and CCPA

Dark Patterns

- “Dark pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation.
- CPRA draft regulations have additional requirements for ease of use, symmetry of choice, avoidance of dark patterns
- Can no longer make it difficult for consumers to exercise

Data Minimization, Purpose Limitation and Retention

- Data minimization, purpose limitation and retention limitation
  - Collection of information must be reasonably necessary and proportionate to achieve purpose for which PI collected or processed
  - Compatible with consumer's reasonable expectation
  - Must obtain opt-in consent if using, retaining and/or sharing PI for any purpose that is unrelated or incompatible with purpose for which PI collected.
- Notice at collection must disclose the retention period for each category of personal information or the retention criteria for each category

Contracts with Service Providers, Contractors, and Third-Parties

- Ensure that vendors process PI under applicable financial sector CCPA exceptions (GLBA, SB-1, FCRA)

- Otherwise, must ensure contracts follow express requirements of CPRA regulations.
  - Service providers & contractor under similar contractual requirements
  - Third-parties have different requirements

Contracts with Service Providers, Contractors, and Third-Parties

In their contracts, service providers and contractors must be prohibited from:

- Selling or sharing PI
- Retaining, using or disclosing PI for any purpose other than business purpose specified in contract. Business purpose must specifically be identified.
- Retaining, using, or disclosing PI outside of direct relationship between service provider/contractor and the business
- Require adherence same level of privacy and data security as required of business
- Combining PI received from the business with PI received from other sources
- Notification to business for inability to comply with CCPA requirements
- Grants testing and audit rights to business for compliance with CCPA

Penalties for Non-Compliance and Enforcement Mechanisms

CCPA

- Private right of action for breach ($100 - $750 per violation + actual damages + other remedies)

- California Privacy Protection Agency enforcement & California Attorney General

Contact Us:

Styskal, Wiese & Melchione, LLP
550 N. Brand Blvd Suite 550, Glendale CA 91203

(818) 241-0103

Joe.Garibyan@swmllp.com

www.swmllp.com

www.tinyurl.com/swm-linkedin

STYSKAL, WIESE & MELCHIONE, LLP

SW&M

FINANCIAL INSTITUTION ATTORNEYS