Freeborn

Your Future Is Our Purpose

U.S. Privacy Laws: ARE YOU COVERED?

by Rita W. Garry

A FREEBORN & PETERS LLP CLIENT ALERT

ABOUT THIS CLIENT ALERT

January 1, 2020 marks the beginning of a new decade and the date the California Consumer Protection Act (CCPA) becomes law, ushering in an era of expanding U.S. citizenry rights over the use and management of their personal information in commercial transactions. California will be joining the ranks of Maine, Nevada, and Vermont, which have already enacted consumer-based privacy protection laws. Eleven other states, including Hawaii, Illinois, Louisiana, Maryland, Massachusetts, Minnesota, New Jersey, New York, Pennsylvania, Rhode Island, and Washington also have consumer privacy, non-breach personal information protection laws in the works.

Who is Covered?

Generally, a "business" (and its controlled affiliates) that operates for profit is covered if it does business in California; collects personal information of California residents and/or households either alone or together with others that process covered data and can answer yes to at least one of the following:

- It has annual gross revenue in excess of $25 million;
- It acts on its own behalf or acts together with others to receive, sell, or share the personal information of at least 50,000 California consumers, households, or devices; or
- It derives at least 50 percent of its annual revenues from selling California consumers' personal information.

What is Covered?

The CCPA broadly defines "personal information" to include information that can identify, relate to, describe, be associated with, or be reasonably capable of being associated with a particular consumer or household. The exemplary list of such "personal information" categories includes:

- Identifiers including real name, alias, postal address, unique personal identifier, online identifier, internet protocol (IP) address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;

- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information; and
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (FERPA).

This list is not exhaustive and will include data that can be used to create a personal profile showing their preferences, characteristics, psychological trends, behavior, attitudes, intelligence, abilities, and aptitudes. It does not include personal information that is de-identified.

How is it Covered?

The CCPA grants to California residents a set of personal data rights and imposes on covered businesses corresponding obligations, which include:

CONSUMER RIGHTS	BUSINESS OBLIGATIONS
Notice	Collection of Personal Information must be disclosed and a list of the categories of types of personal information detailed. Privacy Notice must include an explanation of consumers' CCPA rights and be updated every 12 months.
Access & Information	CCPA-covered consumers have the right to ask for disclosures in a 12 month look back period of: • The categories of personal information businesses collect about them (*e.g.*, identifiers such as their names, Social Security numbers, IP addresses, email addresses, postal addresses; commercial information such as purchasing histories; geolocation data, biometric information, internet activity such as web browsing histories; and professional or employment-related information); • The sources from which that personal information was collected (*e.g.*, online order histories, online surveys, marketing companies, tracking pixels, cookies, web beacons, or recruiters); • The categories of personal information sold to third parties; • The categories of personal information disclosed for business purposes; • The categories of third parties to whom personal information was sold or disclosed (*e.g.*, tailored advertising partners, affiliates, social media websites, service providers); • The business or commercial purposes for which personal information was collected or sold (*e.g.*, fraud prevention, marketing, improving customer experience); and • The "specific pieces" of personal information collected
Deletion	CCPA-covered consumers have the right to ask that covered businesses to delete personal information collected on them, except if such personal information is: • Needed to complete a transaction for which it was collected; • Needed to comply with a legal obligation; • Protect against malicious, deceptive, fraudulent, or illegal activity; or • To identify and repair errors that impair existing intended functionality
Opt Out	CCPA allows California consumers to "opt out" of the "sale" of their personal information requiring covered businesses to install a verbatim link DO NOT SELL MY PERSONAL INFORMATION on their websites.
Nondiscrimination	CCPA prohibits a covered business from retaliating against consumers who exercise their CCPA rights by taking actions that discriminate against them, such as charging a different price, deny goods or services, or imposing penalties. [NOTE – It is not discrimination to charge consumers a different price or rate or provide a different level or quality of goods or services to the consumer if that difference is reasonably related to the value provided to the business by the consumers' data].

CCPA does exclude certain types of personal information that is regulated under federal laws, such as HIPAA and GLB, but offers only a temporary exclusion for employees' and B2B contact personal information until January 1, 2021.

What is Not Covered?

The CCPA has some clear, and some not-so-clear, exclusions from its coverage. These include:

- Protected Health Information – As it relates solely to the certain types of personal information that are protected under HIPAA, HITECH, or the Confidentiality of Medical Information Act (CMIA).
- Financial Institutions – Personal Information sharing practices engaged in by institutions governed by the Gramm-Leach-Bliley Act or the California Financial Information Privacy Act.
- Employee Information – This temporary exclusion covers personal information collected by a business about a natural person in the course of such person acting as a job applicant or an employee, owner, director, officer, medical staff member, or contractor of that business, and to the extent the person's personal information is collected and used by the business solely within the context of such person's role or former role as a job applicant, employee, owner, director, officer, medical staff member, or contractor of that business. This employee exclusion is only temporary until January 1, 2021.
- Limited B2B Exception – Businesses only doing business with other businesses (B2B) under amendment AB1355 may be excluded from some of the CCPA consumer rights' obligations as to the following personal information:

  Personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency. This business contact exclusion is only temporary until January 1, 2021.

Are Data Security Frameworks Covered?

Generally, the CCPA is designed to enhance privacy (not specifically security) of personal information. However, data security correlates to data privacy, and covered businesses must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Covered businesses should refer to the California Attorney General's February 2016 Data Breach Report for guidance on this topic. The CCPA's data security element speaks to a proportional framework so that information security requirements are "appropriate to the nature of the information."

How are the CCPA Rights Covered?

Under the CCPA, the California Attorney General can bring civil actions for injunctions or civil penalties of $2,500 per violation under the statute and up to $7,500 for any intentional violation. A business is in violation of the statute if it fails to cure an alleged violation within 30 days after being notified of alleged noncompliance.

The CCPA also includes a limited private right of action for consumers for violations of the statute's data security requirements. Specifically, a consumer can institute a civil action if nonencrypted or nonredacted personal information (as defined under California's data breach notification statute, California Civil Code, § 1798.81.5(d)(1)) is subject to unauthorized access and exfiltration, theft, or disclosure as a result of a business' failure to maintain reasonable security procedures.

How do Business' Cover CCPA Risk?

CCPA takes effect on January 1, 2020 and the California Attorney General is to enact regulations operationalizing the CCPA no later than July 1, 2020. On October 10, 2019, the first draft of these regulations was proposed, but will not be finalized until after several public hearings and a comment period that ends on December 6, 2019. As proposed, the CCPA Proposed Regulations ("Regulations") begin to bring some clarity (but also raise new questions) on how a business should design and implement its CCPA Compliance policies and procedures.

As the rule-making process continues, covered businesses must begin to take steps that should include:

- **Identify the sources and types, manner of usage, and storage of personal information of California residents.**
- **Update online Privacy Policy statements and analyze data collection points and the need for additional banner notices "at or before the point of collection" of such personal information and build "Do Not Sell My Info" opt-out mechanisms.**
- **If it offers financial incentives to California consumers in exchange for their personal information, it must create a financial incentive notice that explains an estimate of the value of such information and the method used to arrive at that estimate.**
- **Review all third-party vendor contracts to take advantage of the CCPA's "service provider" liability exclusions and data "sale" exceptions.**
- **Set up written policies and procedures to facilitate consumers' exercise of their data rights, to confirm receipt of consumer rights requests, along with accompanying consumer verification processes, to train personnel how to handle rights requests, to document the business' responsiveness to such requests, and to implement a 24 month records retention policy for CCPA rights requests compliance.**

If you have questions about these notable changes to California's consumer-based privacy protection laws or would like more information regarding the Freeborn & Peters LLP Emerging Industries Team, please contact Rita Garry at rgarry@freeborn.com or (312) 360-6581.

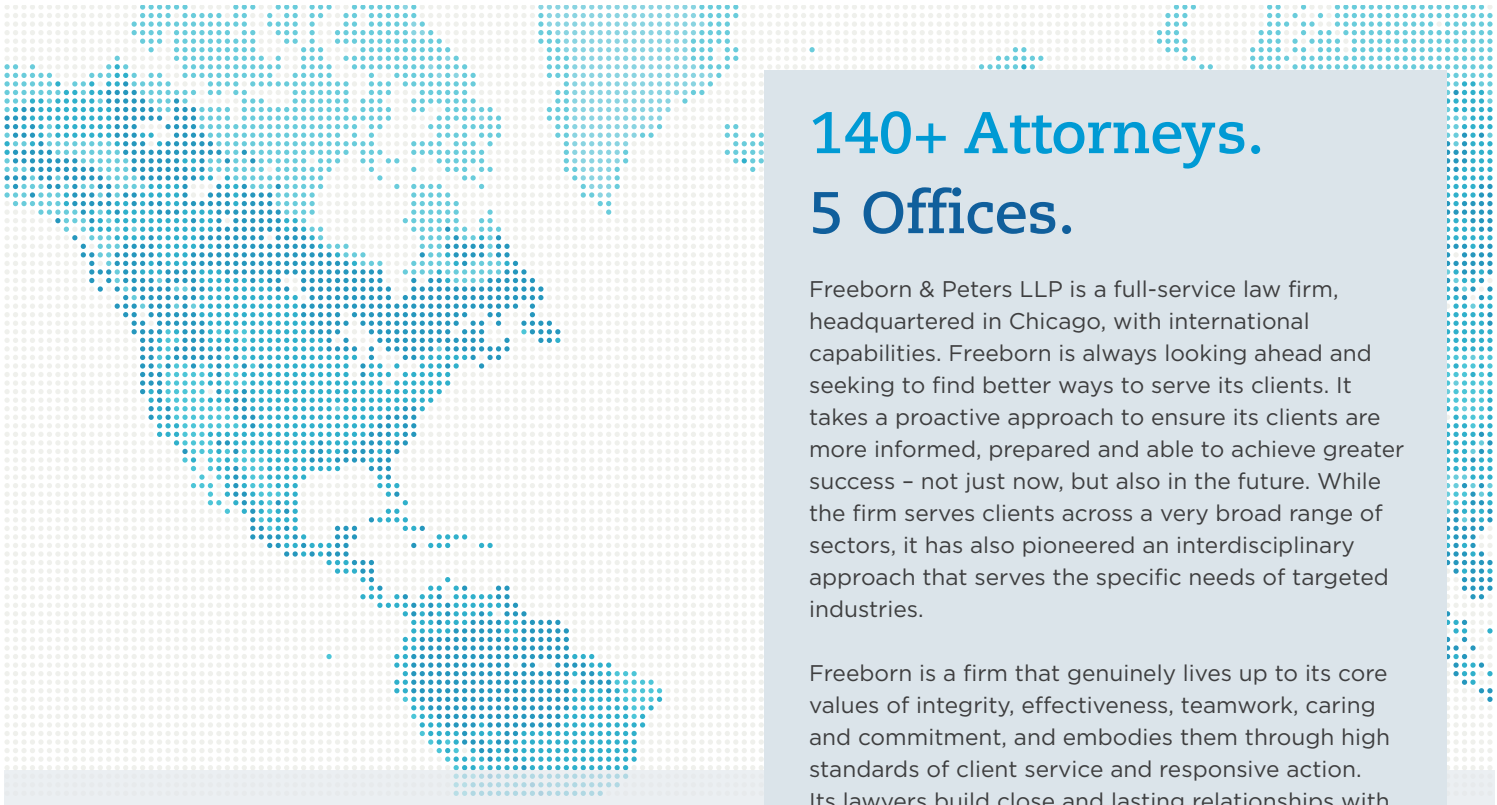
ABOUT THE AUTHOR

Rita Garry
Senior Counsel
Chicago Office
(312) 360-6581
rgarry@freeborn.com

Rita Garry serves as Senior Counsel and is a member of the Corporate Practice Group and a member of the Emerging Industries Team. Rita's practice focuses on corporate and business enterprise law, including M&A, business sales, joint venture, corporate governance and succession planning, securities, finance, private placements and crowd funding.

Freeborn

Your Future Is Our Purpose



140+ Attorneys. 5 Offices.

Freeborn & Peters LLP is a full-service law firm, headquartered in Chicago, with international capabilities. Freeborn is always looking ahead and seeking to find better ways to serve its clients. It takes a proactive approach to ensure its clients are more informed, prepared and able to achieve greater success – not just now, but also in the future. While the firm serves clients across a very broad range of sectors, it has also pioneered an interdisciplinary approach that serves the specific needs of targeted industries.

Freeborn is a firm that genuinely lives up to its core values of integrity, effectiveness, teamwork, caring and commitment, and embodies them through high standards of client service and responsive action. Its lawyers build close and lasting relationships with clients and are driven to help them achieve their legal and business objectives.

For more information visit: www.freeborn.com

CHICAGO
311 South Wacker Drive
Suite 3000
Chicago, IL 60606
(312) 360-6000
(312) 360-6520 fax

NEW YORK
230 Park Avenue
Suite 630
New York, NY 10169
(212) 218-8760
(212) 218-8761 fax

SPRINGFIELD
217 East Monroe Street
Suite 202
Springfield, IL 62701
(217) 535-1060
(217) 535-1069 fax

RICHMOND
901 East Byrd Street
Suite 950
Richmond, VA 23219
(804) 644-1300
(804) 644-1354 fax

TAMPA
1 Tampa City Center
201 North Franklin Street
Suite 3550
Tampa, FL 33602
(813) 488-2920