A DISCUSSION OF CALIFORNIA'S CONSUMER PRIVACY ACT (CCPA) AND DATA BREACH NOTIFICATION LAW

This client resource answers many of the most commonly asked questions about California's new privacy law set to take effect on January 1, 2020, the California Consumer Privacy Act ("CCPA"), and California's Data Breach Notification Law.

What is the CCPA?

The California Consumer Privacy Act (CCPA), signed into law on June 28, 2018, creates an array of new consumer privacy rights and business obligations with regard to the collection and sale of personal information.

What are some of the key highlights?

- CCPA is set to take effect on January 1, 2020.
- Gives California residents the right to prohibit sharing of personal information, right to request access and deletion, and right to statutory damages for security breaches without showing harm.
- Authorizes the California Attorney General to promulgate regulations after having solicited public comment (https://oag.ca.gov/privacy/ccpa).
- Prohibits enforcement until six months after publication of final regulations, or July 1, 2020, whichever is sooner.
- Requires businesses to deliver personal information collected, sold, shared or otherwise disclosed over the past 12 months.
- Will likely be amended by bills introduced in the 2019-2020 legislative session.

Who must comply?

A "business" must comply with the CCPA if it is a for-profit legal entity that collects consumers' personal information on its own or by others on its behalf, that alone or jointly with others determines the purposes and means of the processing, that does business in California, and satisfies at least one of the following thresholds:

- has annual gross revenues in excess of $25M;
- annually buys, receives, sells or shares the personal information of 50,000 or more consumers, households, or devices; or
- derives 50% or more of its annual revenues from selling consumers' personal information.

Based on this definition, it's worth noting that a physical presence in California is not required. The CCPA applies to any entity that controls or is controlled by a business, as defined above. The law applies to parent companies and subsidiaries sharing "common branding." There are exemptions for:

- Non-profits that do not operate "for profit or financial benefit;"

- Health care providers governed by California's Confidentiality of Medical Information Act (CMIA) or covered entities governed by the Health Insurance Portability and Accountability Act (HIPAA);

- Consumer reporting agencies to the extent that their use of personal information is limited by the Fair Credit Reporting Act (FCRA);

- Financial institutions to the extent that their use of personal information is governed by the Gramm-Leach-Bliley Act or California Financial Information Privacy Act.

What's considered "personal information" under the CCPA?

The CCPA defines "personal information" as 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."

To illustrate, but not limit, its broad definition of personal information, the CCPA lists the following specific categories:

- internet protocol address;

- records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

- biometric information;

- browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;

- geolocation data;

- audio, electronic, visual, thermal, olfactory, or similar information;

- professional or employment-related information;

- education information;

- inferences drawn from any of the above to create a profile about a consumer

The CCPA's definition of personal information excludes:

- "publicly available information" (information that is lawfully made available from federal, state, or local government records);

- "de-identified" or "aggregate" consumer information;

- information collected, used, sold or disclosed pursuant to the Gramm-Leach-Bliley Act or the Driver's Privacy Protection Act of 1995, but only if CCPA "is in conflict" with those laws information sold to or from a consumer reporting agency (as defined in the Fair Credit Reporting Act) when the personal information is "reported in, or used to generate," a consumer credit report.

It's worth noting that the CCPA defines "personal information" more broadly than that found in California's breach notification statute (Cal. Civ. Code §1798.82(h)), and even broader than the definition of personal data under the EU's General Data Protection Regulation (GDPR) since the CCPA's definition extends to "households" (which the CCPA does not define).

Who is protected by the CCPA?

The CCPA protects "consumers," defined as a California "resident." Residency is determined by the state's tax regulations. The tax regulation, at 18 CCR § 17014, defines a resident to include:

- every individual who is in California for other than a temporary or transitory purpose; and
- every individual domiciled in California who is outside the state for a temporary or transitory purpose.

When does the CCPA take effect?

Any business subject to the CCPA must comply by January 1, 2020. The law contains a 12-month look-back provision which requires businesses to respond to consumer requests for personal information collected or sold within the past 12 months. The law also provides that the California Attorney General may not bring an enforcement action until six months after publication of the final regulations, or July 1, 2020, whichever is sooner.

What are the consequences for non-compliance?

The CCPA provides for the following options for imposing liability in the event of non- compliance:

- Civil Penalties. In actions by the California Attorney General, businesses can face penalties of up to $7,500 per intentional violation or $2,500 per unintentional violation (but there is an opportunity to cure any alleged violation within 30 days after receiving notice of the alleged violation).
- Damages. In actions brought by consumers for security breach violations, consumers may recover statutory damages not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater (regardless of whether actual damages are shown).
- Non-Monetary Relief - in actions brought by consumers for security breach violations, consumers may seek injunctive or declaratory relief, as well as any other relief the court deems proper.
- Businesses may also be subject to an injunction in actions brought by the Attorney General.

What are the CCPA's main requirements?

Businesses subject to the CCPA have a number of disclosure and other transparency obligations related to personal information:

- Provide notice about collection practices.
- Disclose and keep-up-date at least once every 12 months a description of consumers' rights.
- List separately the categories of personal information collected, sold, and disclosed for a business purpose in the preceding 12 months.
- Provide notice about onward transfers.
- Facilitate consumer requests by making available to consumers two or more designated methods for submitting requests for information.

- Implement and maintain reasonable security procedures and practices to deflect the private right of action created under Cal. Civ. Code §1798.150.

- If selling personal information, provide right to opt out via a clear and conspicuous link titled "Do Not Sell My Personal Information."

- If selling, seek opt-in from consumers between 13 and 16 years of age and from parents if consumer is under 13.

How should my business prepare for the CCPA?

Businesses who must comply with the CCPA will want to complete the key steps before the upcoming compliance date. Those steps include:

- Instituting teams and key contacts;

- Securing budget for CCPA compliance efforts;

- Conducting assessments to determine the components of the CCPA Compliance Program;

- Creating and updating privacy policies and procedures compliant with the CCPA;

- Documenting the CCPA Compliance Program;

- Raising awareness and delivering training on the CCPA Compliance Program;

- Creating and updating privacy notice and consent protocols, including the special rules for the collection and use of personal information of minors;

- Creating and updating protocols to address consumer privacy rights under the CCPA;

- Creating and updating data breach and incident response controls;

- Conducting a data mapping or inventory to identify the personal information and their flows;

- Creating and updating third-party management and sourcing controls;

- Implementing appropriate and reasonable security practices and procedures;

- Establishing monitoring and testing protocols to assess compliance with the CCPA Compliance Program requirements; and

- Maintaining the CCPA Compliance Program.

You may find it helpful to monitor information coming from the California Attorney General's Office for upcoming regulations and interpretive guidance to help address confusion about certain CCPA provisions. You can subscribe to the Attorney General's mailing list at https://oag.ca.gov/privacy/ccpa/subscribe.

What types of rights do individuals have under the CCPA?

The CCPA creates an array of new consumer privacy rights that include:

- The right to request a business to disclose the categories and specific pieces of personal information the business has collected on that consumer.

- The right of deletion, which applies only to data collected directly from and about consumers; has broad limitations.

- The right to opt out of the sale of personal information.

- The right to data portability — consumers may receive their personal information "in a readily useable" format that can then be transmitted to another entity "without hindrance."

- The right of access or disclosure — consumers have a right to request disclosure of their personal information, and to receive additional details regarding the personal information a business collects and its use purposes, including any third-parties with which it shares information.

- The right to sue for security breaches as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices.

- The right of antidiscrimination prohibits a business from discriminating against California consumers for exercising certain rights under the law.

Is the CCPA similar to the EU'S General Data Protection Regulation (GDPR)?

Yes and no. The CCPA shares some similarities to the GDPR, but there are differences as well, as summarized below:

Similarities

- Both laws broadly define personal information.

- Both laws expand obligations of protecting personal information to encompass formal compliance requirements.

- Both the CCPA and GDPR have potentially large regulatory fines.

Differences

- Unlike the GDPR (which repealed the EU Data Protection Directive), the CCPA does not repeal and replace existing data protection laws in California (like the breach notification law).

- Unlike the GDPR, the CCPA's protections are based on an individual's residence.

- The CCPA does not prohibit the processing of personal information by default.

- The CCPA contains no data minimization requirements.

- The CCPA imposes no recordkeeping obligations on businesses.

- The CCPA does not require the designation of a Data Protection Officer.

- The CCPA does not create a right to rectification.

- The CCPA creates no specific restrictions on international transfers.

Does California have a law on breach notice, and if so, is it different from the CCPA?

Yes and yes. California does have a breach notice law – the California Data Breach Notification Law (Cal. Civ. Code §1798.82) – and it is different from the CCPA.

Under California's breach notice law, a business must provide notice of a data breach if:

- it is doing business in California;
- it owns or licenses computerized data;
- the data includes personal information of California residents;
- there was an unauthorized acquisition of electronic personal information belonging to these California residents; and
- the personal information is not encrypted, or it is encrypted but there is reason to believe the encryption key was also compromised.

What's considered "personal information" under California's Data Breach Notification Law?

California law defines "personal information" as an individual's first name or first initial and last name in combination with any one or more of the following:

- Social security number;
- Driver's license/ID card number;
- Account or card numbers if combined with a security/access code;
- Medical information;
- Health insurance information; or
- Data collected from an automated license plate recognition system.

Personal information is also defined as a username or email address, in combination with a password or security question and answer that would permit access to an online account.

Who must be notified under the law?

Businesses must notify any California resident whose personal information was compromised as a result of a data breach. Any business that is required to notify more than 500 California residents as a result of a single breach must also submit a single sample copy of that notification to California's Attorney General. Businesses that maintain, but do not own or license, personal information must inform the entity that owns or licenses the information of any security breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

What must be included in the notice?

The notice must include the following minimum information:

- Name and contact information of the one issuing the notice;
- List of the types of personal information involved in the breach;
- Key dates involving the breach;
- Whether a delay in providing the notice is attributable to an investigation by law enforcement;
- A general description of the breach;
- The contact information of major credit reporting agencies if the breach exposed a social security number or a driver's license or CA identification card number; and
- An offer to provide appropriate identity theft prevention and mitigation services if the one providing the notice was the source of the breach.

The following information may be included in a breach notice, but it's optional, not required:

- Information about what has been done to protect breach victims; and
- Advice on steps that victims may take to protect themselves.

Must the breach notice information be presented in a certain way?

Yes. The information in the notice must follow these guidelines:

- Written in plain language;
- Titled "Notice of Data Breach;"
- Organized under the following headings –
    - What Happened?
    - What Information Was Involved?
    - What We Are Doing?
    - What You Can Do
    - For More Information
- Title and headings must be "clearly and conspicuously displayed;" and
- Font size no smaller than 10-point type.

When must the notice be sent?

- A business that owns or licenses computerized data containing personal information of CA Residents must notify affected residents "in the most expedient time possible and without unreasonable delay.
- A business that maintains computerized data owned or licensed by another must notify the owner or licensee "immediately following discovery" of the breach.
- Timely notifications must take into account legitimate needs to cooperate with law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

- Notice may be delayed if law enforcement determines that notification will impede a criminal investigation.

- If notice must be sent to more than 500 California residents, a copy of the notice must also be sent to the California Attorney General (but no timeframe is mentioned).

How may notice be sent?

Notification may be sent:

- in writing;

- electronically, provided it satisfies the provisions regarding electronic records and signatures set for in the federal E-Sign Act, 15 U.S.C. § 7001 *et seq.*;

- via substitute notice if the cost of providing notice is greater than $250,000, the number of persons to be notified is exceeds 500,000, or the business does not have sufficient contact information. The substitute notice must include all of the following:

    - an email notice (when the business has an email address for the affected individuals);
    - conspicuous posting of the notice on the business's website (if the business has one) for at least 30 days; and
    - notification to major statewide media.