INTELINK
Law Group, PC

THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA" OR "ACT"): WHAT IT IS, WHO IS AFFECTED, AND HOW TO COMPLY.

On January 1, California's new data privacy law, the CCPA, took effect, instituting a broad set of rights of an individual consumer to protect and control personally identifiable data a consumer discloses to a business subject to the Act. It imposes a corresponding set of obligations on a covered business to inform and provide access to data a business collects or processes with regard to that consumer, and to respond to that person's requests to delete, modify or stop using his or her data altogether.

While businesses have been subject to both federal and state laws aimed at preventing data security breaches, protecting minors from the use of their personal data, and safeguarding certain financial and health care data of individuals, businesses have been liable only for data security breaches and answerable primarily to the government agency in charge. In contrast, the Act now recognizes and enforces an ***individual's rights*** to know what personal data a business has about a specific consumer, what it is doing with it, and to control how a business uses, shares or processes that person's data. The assumption that once a consumer provides data to a business, the business is free to use it forever and without restriction is no longer valid. Rather, a business' collection and use of personal data is now subject to an ongoing exchange with the consumer as to what a business may collect, use or process of his or her personal data.

Pending further guidance from the State Attorney General's operating regulations, just issued and to become final before July 1, businesses subject to the Act should be in compliance or take steps to be in compliance with the Act's basic requirements:

Which businesses are covered?

The CCPA applies to businesses in California or doing business with California residents which have:

- ***Personally identifiable information ("PII") of 50,000 consumers, households or devies; or***
- ***$25 million or more annual net revenue; or***
- ***50% of the business' annual revenue is derived from the sale, purchase, or use of PII***

How is PII Defined?

Personally identifiable information is broadly defined as any information that can identify or be linked to a specific person. It includes basic details such as a person's name, mailing or email address, IP address, cell or other phone number, and driver's license or social security numbers. It also includes commercial information such as product purchases, biometric information, geolocation data, professional or employment information, and information that a business can derive from PII by processing the personal details received from a consumer to create a profile of preferences or characteristics.

How to Comply with the CCPA

Covered business or service providers need to take stock of what data they have, where it is located, the sources of the data, and the purposes for which it collects, stores or processes personal data. This basic analysis will in turn inform its design and implementation of a privacy plan, both with regard to its internal operations and its communications with individual consumers

The consumer's rights under the Act are to:

- *Know what PII a business has about the consumer;*
- *Upon proper verification, be provided access to that data within prescribed time limits;*
- *Request a business to delete or change all or some of the PII the business has about that person;*
- *Opt out of any "sale" by a business or service provider of that person's PII without verification and within shorter time limits than the request for information;*
- *Be equally treated by the business, even if a consumer opts out or requests deletion of PII from a business.*

A business's obligations under the Act to give effect to these consumer rights are to:

Inform consumers of the types and categories of information the business collects this data, the use (purposes) of the personal data, as collected, processing the data is subject to, the source(s) of the data, if not directly from the consumer, and if shared, with whom such data is shared.

Disclose to a verified consumer the specific PII or categories of PII or both the business has about that person, responding to a consumer within prescribed time limits and without charge.

This obligation entails setting up mechanisms for verifying that a consumer is the person to whom the personal data relates before disclosing the information to protect against fraud, and possibly breaching obligations imposed by other state or federal law. At least two means of enabling information requests and interacting with a consumer must be provided, for example, online and by phone.

Respond to verified requests by a consumer to delete or modify some or all PII a business holds, or to comply with a request not to make any further use of that consumer's data. A business must not only comply with consumer requests, but also but keep records of its responses to consumers for purposes of showing compliance with the Act and any state attorney general review or investigation.

Provide an "opt out" option with regard to the "sale" of a consumer's data: A "sale" of information includes any transaction in which there is an exchange of value for PII. If a business sells or shares the personal data of a consumer for any commercial purpose, it must disclose this fact to consumers and enable a consumer to "opt out" of further sales. This is best accomplished by providing a clear online ***link on the business' web home page for a consumer to click on a "button" labeled "opt out"***. The opt out request must be complied within 15 days of the receipt of the request and without verification of the consumer opting out. This obligation directly affects data brokers, marketing and ad tech companies, but also the businesses which outsource marketing tasks to them.

Not discriminate against consumers which request information, changes, deletions, or opt out of sale of that person's data, and those which do not. Some exceptions apply with regard to loyalty programs and certain incentives to encourage consumers to provide PII.

Further points to note:

The Act not only applies to data provided online, but to personal data collected, processed or used in any manner in offline transactions. This includes notices where security cameras are posted in retail shops or data provided to a business by phone.

The Act exempts employers from most obligations on a business regarding employee personal data, but does require an employer to disclose or provide notices to its employees of the types and categories of PII it collects and processes on employees.

This exemption does not apply to non-employment related data a business holds or to non-employees, and it may be subject to further amendments by January of 2021.

The Act gives consumers a private right of action for data breach claims. The precondition to filing is to allow a business a 30- day period to cure breach, and if there is failure to do so, the claimant can sue for by actual or statutory damages. The attorney general can also bring enforcement actions for any breach of the Act's obligations.actual or statutory damages. The attorney general can also bring enforcement actions for any breach of the Act's obligations.

Summary:

To date, the business community mindset has been to collect as much data as possible and to expect that collected data is then "owned" by the collector/processor. This premise is no longer viable; rather, businesses need to audit the universe of data they have and clearly communicate with consumers about the personal data they hold and the purpose or uses of that PII. If unnecessary to a business' operations, it may be best to permanently delete some of the data collected or held, and to minimize the scope of data collected for which it is now responsible to each consumer for use. Going forward, businesses will be responsible for ongoing dialogue with consumers on the collection and use of personal data, and to respond to requests for changes, deletions, and data sharing.

Currently, a number of other states are following California's lead and enacting privacy laws, with more state laws expected. A business which must comply with California's rules may plan to handle different state rules as they arise. However, it may be better to design a privacy policy and organization that is capable of complying with the highest or strictest standards of those state laws. This should enable a company doing business in more than one state to adjust to wider data privacy coverage throughout the country. The time is ripe for businesses to audit their data inventory, evaluate their need to hold certain data, assess the risk of retaining what isn't relevant to the business purpose, and create the means of responding to individual consumer requests for deletion, opt out, or other rights.

For specific advice on CCPA compliance, including privacy statements, opting out, verification approaches, internal procedures and employee training, handling of consumer requests, vendor or other partner contracts, and other state and federal privacy laws, please contact:

LESLIE WILLIAMS

at

lwilliams@intelinklaw.com