**CCPA**

It is obvious to even the most tech illiterate by now that regulations over data are becoming more onerous and intrusive against what was more of a wild west type scenario in the early days of data sharing.  The latest proof of this is in the newly enacted General Data Protection Regulation (GDPR) in the European Union effective on May 25, 2018 (it happens to be my birthday), and in the shadow of the pending U.S. Encrypt Act, and the most recent state’s effort to tighten the data screws for which the poster child currently is California’s new regulation, California Consumer Privacy Act (CCPA) that sets the bar higher than ever before for U.S. companies regarding data privacy regulation. If the bill comes into law in its present form, which this author believes it will not, then companies doing business in the U.S. will require almost the same data privacy controls and capabilities that multinationals need to do business in the European Union require today with some rather ideological exceptions. As always, “failure to protect the data” signals the same need GDPR has for end-to-end encryption, portability, conformity, and data residency.

**Background: The History and Ballot Initiative**

In early 2018 a California real estate developer spearheaded an effort to include a new privacy law — the Consumer Right to Privacy Act of 2018 — on the November 2018 California ballot. By June 2018, supporters of the initiative had gathered enough signatures to earn a place on the November ballot. In response, California legislators, working with representatives of affected California businesses and other interest groups, quickly negotiated and passed a substitute bill — The California Consumer Privacy Act of 2018 - the CCPA — in exchange for an agreement to drop the more restrictive text in the Consumer Right to Privacy Act from the November ballot.

The California legislator passed what is considered to be the absolute toughest data privacy law in the United States. The California Consumer Privacy Act of 2018 was approved by the California State Governor on June 28, 2018, and goes into effect on January 1, 2020. The law applies to any business that has more than $25 million in revenue, or buys or sells the personal information of 50,000 or more consumers, or derives 50 percent or more of its annual revenue from selling consumers’ personal information, and that does any amount of business in the State of California. The tone of the legislation is quite aggressive. The legislation specifically cites the March 2018 disclosure of the misuse of personal data by Cambridge Analytica. The legislation also references recent congressional hearings that followed which highlighted the fact that any personal information shared on the internet can be subject to considerable misuse and theft. This prompted the California legislature to move rapidly to protect Californians’ right to privacy by giving consumers much more control of their personal information.

**Details, details**

The CCPA generally offers California consumers new statutory rights to learn what personal information Covered Businesses have collected, sold and disclosed, opportunities to opt-out of the sale of their personal information, and (uniquely) protection from “discrimination” in the form of reduced service or functionality for exercising those rights. For Covered Businesses, the CCPA specifies disclosure obligations and compliance procedures that are designed to help California consumers exercise these new statutory rights. A snapshot of the key provisions includes:

Consumer Right to Know: Under the CCPA, similar to the new European regulations, California consumers have a right to request what personal information has been collected about them, as well as what personal information has been sold or otherwise disclosed about them. The CCPA requires Covered Businesses to comply with “verifiable requests” from consumers about the collection, sale, and disclosure of their personal information and outlines specific procedures and timelines that Covered Businesses must follow.

Consumer Right to Delete: Under the CCPA, similar to the new the European regulations, California consumers have a right to request that their personal information be deleted. Covered Businesses must honor “verifiable” requests to delete consumer personal information, subject to several notable exceptions, including that a Covered Business need not delete personal information if maintaining the information is required to complete a transaction or provide a good or service.

Consumer Opt-Out from Sale of Personal Information: Under the CCPA, California consumers are afforded the right to “opt-out” of the “sale” (which is broadly defined) of their personal information. Covered Businesses must provide notice of this right to consumers (including by providing a clear and conspicuous hyperlink entitled “Do Not Sell My Personal Information” on their websites) and must implement designated methods for consumers to opt-out (including a toll-free number and website address for opting-out). Covered Businesses must honor consumer opt-outs, and must wait 12 months before seeking re-authorization to sell their personal information.

Consumer Opt-In for the Sale of Personal Information of Minors: Under the CCPA, the personal information of minors under the age of 13 may only be sold if the consumer’s parent or guardian has affirmatively authorized (opted-in to) the sale. For minors aged 13-16, affirmative authorization is also required, but the consumer may provide the authorization.

Non-Discrimination for Exercise of Consumer Rights: Under the CCPA, Covered Businesses are prohibited from discriminating against consumers based on their having exercised rights (i.e., opting out of collection or monetization of data) pursuant to the CCPA. A Covered Business cannot refuse to sell goods or provide services, charge different prices for such goods or services, or provide lower quality goods and services because a consumer exercises his or her rights under the CCPA. However, this requirement does not prohibit a Covered Business from charging different prices or providing different quality goods or services if the difference is “reasonably related” to the value of the personal information at issue.

**CCPA Enforcement Provisions**

The CCPA is enforceable both by the Attorney General for the State of California and by private litigants. However, the Act contains technical terms regarding when and how a consumer can bring a private action under the statute. Notably, the terms provide Covered Businesses opportunities to cure certain instances of non-compliance. Key terms include:

Enforcement by Attorney General: Violations of the CCPA are enforceable by the California Attorney General, which is authorized to pursue civil penalties of up to US$7,500 per violation.

Limited Private Right of Action for Unauthorized Disclosure of Data: Consumers may bring a private right of action against Covered Businesses in connection with “certain unauthorized access and exfiltration, theft, or disclosure of a consumer’s nonencrypted or nonredacted personal information” if the Covered Business has failed to implement and maintain reasonable security measures to protect such information. However, prior to commencing an action for statutory damages (US$100-$750 per incident), the consumer must provide the Covered Business with 30 days to cure the alleged violation and to respond with a written statement that the violation has been cured

**SB 1121 – Clarifies the CCPA and acknowledges the Preemption**

Less than three months after California passed the CCPA, Governor Jerry Brown signed SB 1121, making a number of technical and substantive changes to the law.

SB 1121 clarifies that identifiers specified in the CCPA are no longer automatically considered to fall under the definition of “personal information” — only if they can be connected with an individual or household.

The bill also includes clarifications to avoid conflict with several other regulations, including HIPAA, the Gramm-Leach-Bliley Act (covering information maintained by financial institutions), the Driver’s Privacy Protection Act (covering motor vehicle and driver’s license information), and the California Financial Information Privacy Act.

Additional revisions include the following:

* Consumers’ right to litigation under CCPA only applies to data breaches, not to violations under any other section.
* The CCPA will preempt local laws, but only after the bill goes into effect on January 1, 2020.
* The California Attorney General’s general enforcement of the law will begin “six months after the publication of final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.” Attorney General Xavier Becerra has reportedly told Governor Brown that he expects to issue final rules under the law by June 2019 in anticipation of the January 1, 2020 enforcement date

In particular: SB 1121 modifies the financial institution carve-out language in CCPA section 1798.145(e). While the change is a welcome development for entities subject to regulation under the Gramm-Leach-Bliley Act (GLBA), it does not grant full exemption from the CCPA. Therefore, GLBA-regulated entities that collect information online will need to analyze the CCPA’s requirements and how they apply to a specific business.

The original carve-out language provided that:

“This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, if it is in conflict with that law.”

That language raised a number of issues, such as what would constitute a “conflict” between the GLBA and the CCPA, and whether the language was consistent with the GLBA in that personal information is not collected, processed, sold, or disclosed pursuant to the GLBA. The provision also failed to address the relationship between the CCPA and California’s Financial Information Privacy Act.

The new language tries to resolve some of those issues, stating:

“This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act … . This subdivision shall not apply to Section 1798.150.”

The new language removes the phrase “if it is in conflict with that law,” incorporates the California Financial Information Privacy Act, and adds a sentence providing that financial institutions are still subject to Section 1798.150. The preamble explains those changes as follows:

“The bill would also prohibit application of the act to personal information collected, processed, sold, or disclosed pursuant to a specified federal law relating to banks, brokerages, insurance companies, and credit reporting agencies, among others, and would also except application of the act to that information pursuant to the California Financial Information Privacy Act.”

While the revised language is likely well received by GLBA-regulated entities, it should not be interpreted as a full exemption. Rather, GLBA entities will remain subject to the provisions and requirements of the CCPA if they engage in activities falling outside of the GLBA—which they almost certainly do.

By way of explanation, the GLBA regulates financial institutions’ management of nonpublic personal information, which is defined in 15 U.S.C. § 6809 as personally identifiable financial information: 1) provided by a consumer to a financial institution; 2) resulting from any transaction with the consumer or any service performed for the consumer; or 3) otherwise obtained by the financial institution.

The CCPA defines “personal information” much more broadly to include “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.” The CCPA identifies numerous examples such as online identifiers, Internet Protocol addresses, email addresses, browsing history, search history, geolocation data, and information regarding a consumer’s interaction with a website or online application or advertisement. Notably, the CCPA’s definition also includes any “inferences drawn” from any personal information that is used “to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.”

Therefore, to the extent that GLBA-regulated entities are using targeted online advertising, tracking web page visitors, and/or collecting geolocation data—to name a few examples—either through their web pages or apps, they will need to analyze the CCPA’s requirements.

As for the new statutory language providing that “[t]his subdivision shall not apply to Section 1798.150,” the impact of that sentence cannot be overstated.

Section 1798.150 sets forth a private right of action for consumers to seek statutory damages of not less than $100 and not greater than $750 “per consumer per incident or actual damages, whichever is greater” if the consumer’s information “is subject to an unauthorized access, exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices.” In other words, GLBA-regulated entities will still be subject to millions of dollars of potential damages if they experience a data breach.

**Compare to GDPR**

The California Consumer Privacy Act of 2018 is similar in many ways to the European Union General Data Privacy Regulation (GDPR). GDPR fines can reach as much as four percent of the company’s prior year global revenue. The California Consumer Privacy Act has a damage limit of $750 per person for each violation, but, in some cases, the violation penalty can be much higher. GDPR also has an inviolate 72-hour window for breach notification, and the California Consumer Privacy Act of 2018 doesn’t. In most other areas, the legislation is quite similar and suggests the need for broadscale changes to corporate operating procedures within governance and compliance as well as changes to software systems and security infrastructure.

**How Will it Change- Prediction of Final Law being Watered Down**

**Key Context for Businesses**

California lawmakers drafted and passed the CCPA in a matter of days. For many observers, the headlines about the enactment of the law were the first news of the sweeping privacy changes now on the books. Understanding the sudden and significant impact the law will have upon businesses, lawmakers built in a delayed effective date, of January 1, 2020, with a now enforcement date of July 1, 2020. This delay is a similar time period to the 24-month delay between the effective date for Europe’s General Data Protection Regulation and its enforcement date of May 25, 2018. The delayed effective date also sets the stage for intervening laws amending or modifying key definitions or provisions of the CCPA. But for now, in light of the difficulty of complying with new data access and opt-in or opt-out rights, covered businesses should begin immediately assessing how the law as passed will apply to their information collection, retention, marketing, and other pertinent business plans or practices. Pre-emptive federal universal privacy legislation is another potential consequence of the first-of-its-kind California law.

While it is very likely that there will be changes prior to the January 2020 effective date, and in light of the very long lead time required to adapt business plans and practices to this new rights regime, companies should immediately begin a preliminary assessment of how CCPA may impact them, even as the ink begins to dry on this newly-enacted legislation.

By John Stephens