Davis Wright Tremaine LLP

THE CALIFORNIA CONSUMER PRIVACY ACT: WHAT FINTECH COMPANIES NEED TO KNOW

California enacted the nation's most extensive consumer privacy law last summer after only a week of legislative debate. The California Consumer Privacy Act of 2018 ("CCPA") was passed quickly to prevent a privacy ballot initiative and creates extensive notice, opt-out/opt-in, access, and erasure rights for consumers vis-à-vis businesses that collect their personal information, as well as a private right of action in the case of a data breach. Though dubbed by many as "California's GDPR," the CCPA is fundamentally different and will require businesses to invest billions of dollars into restructuring their operations.

The CCPA is likely to have a significant burden on the FinTech industry, where companies' reason for being is to collect, aggregate, and move the consumer data at the heart of the law. Specifically:

- New FinTechs could meet the threshold of data collection from 50,000 consumers, households, or devices almost instantly upon going live. Companies will need to devote a significant start-up budget to prepare for compliance.
- Where FinTechs are the conduit for transactions that involve other entities, they will have to conduct complex and detailed inquiries as to whether each party in the process is a third-party or a service provider, and how notice obligations, opt-out, access, and erasure rights will apply to that relationship.
- FinTechs will face increased risk of liability in the event of a data breach, as the new law creates a private right of action and sets statutory damages for a breach of certain sensitive consumer information, which can include financial data.

The following details the frequently asked questions regarding the CCPA and privacy legislation generally:

Q: What is covered?
A: All "Personal Information," whether collected Online or Offline.

The CCPA has been described in news reports as a regulation of "online privacy." In reality, it applies to all instances of collection of consumer personal information ("PI"), regardless of means, and across businesses regardless of industry. The definition of PI contained in the CCPA is broad—whereas most US laws only

consider information "personal" if it is a sensitive identifier or provides access to a financial account. By contrast, the CCPA extends to all 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," including name, email address, biometric information, and IP address. This is the first instance of non-individualized data belonging to a group of people being legally treated as PI, and to make it worse, the term "household" is not defined in the law.

Q: Who is subject to the new law?
A: Nearly all commercial entities are covered.

The CCPA applies to for-profit entities that do business in the State of California (including any same-branded controlled or controlling company) that meet any one of the following three criteria:

(1) gross revenue of more than $25 million;
(2) receives or shares PI for more than 50,000 "consumers, households, or devices"; or
(3) receives more than 50 percent of its annual revenue from the sale of PI.

Since visitors to a website contribute to the number of consumers, households, or devices for which data is collected, the 50,000 threshold is likely to be met easily, even for small businesses—particularly given that one consumer may have multiple devices. It is also likely that the CCPA will be interpreted to cover employee data, as the definition of consumer is not limited to individuals with whom a business engages in an arms-length transaction.

The CCPA tries to recognize pre-emption by the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA), but the exemptions remain limited, even after a series of technical amendments was passed in August. HIPAA-covered entities are fully exempt, as well as Business Associates for the protected health information they hold, but they may hold a much broader set of personal information which would not be exempt. GLBA-covered entities are exempt only with regard to the data they collect pursuant to GLBA; they will still face obligations with regard to other information, such as information regarding their California employees and data collected for marketing purposes. The CCPA also provides other exceptions allowing disclosure, such as to comply with law, respond to valid legal requests, "exercise" or defend legal claims, and the like.

Q: Is this an Opt-Out or Opt-In Law?
A: Both.

By and large, the CCPA is an opt-out law. Consumers can opt-out of the "sale" of their PI to a third party, and when they do, a business is prohibited from asking them to opt-back in for at least 12 months. "Sale" is defined broadly as the "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. No opt-out right applies to disclosures of personal information to service providers who process information for a covered business and who are prohibited by contract from using it for their own purposes.

Businesses will need to find a way to track compliance with the opt-out and time-out mandates across business departments and product or service lines—which may be technically impossible where the sale relates to information collected automatically via websites and consumers access a website from a different device.

For consumers under age 16, opt-in consent is required prior to any sale of information to a third party. Consumers between ages 13-16 can opt-in for themselves, and business must obtain a parent or guardian's affirmative authorization for consumers under 13. While the collection of information from children under the age of 13 is already covered under the Children's Online Privacy Protection Act, the CCPA applies to personal information collected both online and offline.

Businesses that currently offer free services in exchange for collecting information will face challenges parsing out the exact directive of the CCPA. The juxtaposition of the prohibition on denigrating the quality of service or charging consumer's higher prices simply because they opt-out of the sale of their PI and the permission to offer incentives to those consumers who affirmatively opt-in to the collection or sale of their PI, like the CCPA in general, is not the model of clarity.

Q: Will I have to change my privacy policy and or provide other consumer notices?
A: Yes.

Businesses must disclose—either on their websites if they have one or through other means—certain information regarding its practices regarding collection of consumer PI, and update the information at least once a year. Despite criticisms

that privacy policies are too long and rarely read, the CCPA requires these notices to include even more detail. Under the new law, the privacy policy must contain:

- A description of the consumer's rights under the CCPA
- How a consumer can submit access requests to the business
- The categories of PI the business collected about consumers in the preceding 12 months.
- Lists detailing the categories of PI about consumers that the business has sold or disclosed for business purposes in the preceding 12 months (or the fact that the business has not sold or disclosed PI)

If they engage in the "sale" of PI, a business must explicitly inform consumers that their information may be sold to third parties and that they have the right to opt-out of the sale of PI through a website link on the business' homepage titled "Do Not Sell My Personal Information" which offers an opt-out function. The CCPA does allow businesses to create separate California-only home pages that contain these links, so long as business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

Businesses must also notify consumers of any financial incentives they offer to influence the consumer's choice on this webpage.

Q: Am I obligated to respond to new consumer requests for information?
A: Yes, the CCPA establishes a "Right to Access."

The CCPA gives California residents the right to, up to two times in any 12-month period, request and access the "specific pieces" of personal information a business has collected regarding that individual, as well as the categories of PI collected, where it was collected from, the business purpose for the collection, and the categories of entities to whom personal information is sold or disclosed for a business purpose. If the information is provided in an electronic format, it must be portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.

The law notes in several places that a business will not be "required to reidentify or otherwise link information not maintained in a manner that would be considered PI;" however, the explicit listing of a number of data points that only indirectly point to a person (such as IP address and internet activity records) means that much information not obviously linked is stored in a manner that is considered PI. The

law also does not speak to whether businesses must disclose each and every instance in which personal data appears, or provide a general listing of specific information that excludes duplicative sources.

Q: Will consumers be able to request that I delete information?
A: Yes, in certain instances, the CCPA establishes a "Right to Erasure."

The CCPA gives consumers the right to request that a business and its service providers delete PI collected from the consumer. The business (or service provider) does not have to honor this request if it is "necessary" to retain the information due to any of nine exemptions applying, including for internal uses "reasonably aligned with the expectations of the consumer" or that are in a "lawful manner compatible with the context in which they were provided the information."

It is unclear, however, what constitutes a valid internal use, or whether a use is "internal" where data must be shared with service providers, consultants, or contractors to accomplish the use.

Q: Did the liability for breaches change?
A: Yes, the CCPA effectively supplements the Data Breach Notification Law with a private right of action.

The Act provides for statutory damages for consumers whose non-encrypted or non-redacted personal information—as such term is defined in California's data breach notification law—is "subject to unauthorized access and exfiltration, theft, of disclosure as a result of the business' violation of the duty to implement and maintain reasonable" security procedures. By providing statutory damages, the Act removes the standing requirement that has been a bar to most prior data breach litigations. The definition of personal information in the data breach law is more narrow than the definition in CCPA, and the change in the drafting process to create a private right only where there is "unauthorized access and exfiltration, theft, or disclosure" of personal information. The CCPA also creates liability for loss of paper data, which does not require notice under California's data breach notification law.

While the standard of reasonable security is not defined under California law, the AG has previously cited the 20 controls in the Center for Internet Security's Critical Security Controls as identifying a minimum level of information security that all organizations that collect or maintain personal information should meet. Credible

third-party assessments of an entity's compliance with these controls could become valuable in defense of a data breach lawsuit under the Law.

Q: What are the risks of non-compliance?
A: Enforcement by the Attorney General and individual consumers, with established statutory damages.

Consumers are afforded a limited private right of action and are able to recover "not less than" $100 and up to $750 per violation in private actions in the event of a breach of the more limited types of personal information covered by California's existing breach notification statute. They can only exercise this right, however, after a 30-day period in which an allegedly noncompliant entity can attempt to cure any deficiencies and subsequent notification to the Attorney General ("AG"), who can decide to prosecute the action itself (although it is unclear how an entity would cure an already reportable data breach). Although not entirely true, it appears as if the CCPA also attempts to prohibit a business' use of arbitration clauses in Section 1798.192. If this is the intent, the provision will likely be subject to legal challenges, given the Supreme Court's recent decisions upholding arbitration clauses.

The AG is tasked with enforcing all other provisions of the law, but also must give a business a 30-day period to cure a violation before bringing an action. Civil penalties in an AG action can be up to $2,500 for each violation ($7,500 if intentional), and any assessed penalties are divided between the jurisdiction on whose behalf the action was brought and a new Consumer Privacy Fund, which is created by the Act to offset the costs of enforcement.

Q: When do I have to be in compliance?
A: Jan. 1, 2020. The AG cannot bring an enforcement action until July 1, 2020, but consumers can start exercising their rights in January.

Given the rushed nature of the legislation and the identified drafting errors, it is likely that some amendments will be sought before that date. However, the core obligations of the law are unlikely to change.

Q: Is there likely to be federal legislation that preempts the CCPA?

A: Prospects for federal legislation look stronger than in the past, but don't delay compliance, as there is no guarantee that legislation will pass prior to Jan. 2020.

Since the CCPA was signed into law, executives from several large tech companies have issued public statements in support of federal privacy legislation, citing concerns about varying privacy laws in different states creating conflicting compliance obligations. Sen. John Thune, chair of the Senate Committee on Commerce, Science, and Transportation, has referred to federal legislation as "inevitable." However, the only bills proposed to date have come from Democrats. With control of Congress now divided, a bill would likely have to be bi-partisan to stand a chance of being passed by the Senate. There are no indications of what Republicans would even like to see in a federal privacy bill, and it remains uncertain as to whether compromise is possible in the current political environment. Even if a bill is passed, it may not be prior to Jan. 2020, and it may not fully preempt state law. As full compliance with the CCPA can take many months to achieve, companies that wait to see what happens in Congress create significant risk for themselves.