CALIFORNIA USHERS IN THE NEXT GENERATION OF DATA PROTECTION

By Genevieve R. Walser-Jolly, Esq.

While businesses have been largely focused on the European Union's implementation of the General Data Protection Regulation ("GDPR") of late, California took its own first steps into the new frontier of consumer privacy and data protection as Governor Jerry Brown signed Assembly Bill 375, dubbed the "California Data Privacy Protection Act" on June 28, 2018.[1] The Act is scheduled to go into effect on January 1, 2020. This Article covers the Act's purpose, scope, proscriptions and remedies, and suggestions to business for compliance.

The Purpose of the Act

The Act is intended primarily to ensure the following rights for California residents:

- The right to know what personal information is collected about them;
- The right to know if their personal information is sold and to whom;
- The right to prohibit the sale of their personal information;
- The right to access their personal information; and
- The right to not be discriminated against for restricting use of their personal information.[2]

For purposes of the Act, personal information ("PI") includes but is not limited to: names; mailing addresses; telephone numbers; bank account numbers; credit card numbers; medical information; health insurance information; unique identifiers; IP address; email addresses; SSN; driver's license numbers; passport numbers; audio, visual, electronic, thermal, or olfactory information; employment information; education information that is not publicly available; geolocation data; internet activity; and any inferences drawn from these categories of information that reflect the consumer's preferences, behavior, attitudes, intelligence, etc.[3] The

[1] This compromise legislation was designed to avoid the pending California Consumer Personal Information Disclosure and Sale Initiative, which was withdrawn by its proponents once Governor Brown signed the Act. (https://ballotpedia.org/California_Consumer_Personal_Information_Disclosure_and_Sale_Initiative_(2018).)
[2] 2017 California Assembly Bill No. 375, California 2017-2018 Regular Session, Sec. 2(i).
[3] Cal. Civ. Code, § 1798.140(o)(1); Cal. Civ. Code, § 1798.80. The FIPA, by contrast, uses the term "personally identifiable financial information," which is defined as "information (1) that a consumer provides to a financial institution to obtain a product or service from the financial institution, (2) about a consumer resulting from any transaction involving a product or service between the financial institution and a consumer, or (3) that the financial institution otherwise obtains about a consumer in connection with providing a product or service to that consumer. Any personally identifiable information is financial if it was obtained by a financial institution in connection with

Act significantly expands the universe of PI, but still excludes information that is publicly available or will not allow individuals to be identified.[4] (Businesses may look to align their data collection with this exception where possible.)

What the Act Does

The Act requires covered companies to tell consumers what categories and specific pieces of PI were collected about them, and the purpose of the collection.[5] With a strong nod to the GDPR, companies must also advise consumers of their right to have their data deleted.[6] If requested by a consumer, the company must delete the specified data and require its service providers to do so as well.[7]

Companies are exempted from deleting data, however, if it is necessary: (i) to complete the transaction for which it was it was collected; (ii) to provide the goods or services requested by the consumer; (iii) to perform on a contract between the consumer and company; (iv) to detect and/or prosecute security incidents; (v) to exercise free speech, to ensure the consumer's right to free speech, or to protect any other right in law; (vi) to perform scientific, historical, or statistical research; (vii) to comply with legal obligations; or (viii) for internal use compatible with the context in which the consumer provided the data.[8]

Importantly, consumers also have the right to opt-out and to prohibit the sale of their data, i.e. personal information.[9] The rules regarding opt-out are explicit. The Act requires that affected businesses provide a clear and conspicuous homepage link titled "Do Not Sell My Personal Information" on its website that directs the customer to an opt-out form.[10] Businesses must also include a description of these privacy rights, along with a separate link, similarly titled, in their online privacy policies and/or other California-specific privacy notices.[11]

If a consumer opts-out of sharing their data, companies may not treat them differently in price, rates, service, or quality of goods unless the difference is reasonably related to the value of the

---

providing a financial product or service to a consumer," and may include some of the same information protected by AB 375, such as "[a]ccount balance information, payment history, overdraft history, and credit or debit card purchase information"; "personally identifiable financial information collected through an Internet cookie or an information collecting device from a Web server"; or even "[t]he fact that an individual is or has been a consumer of a financial institution or has obtained a financial product or service from a financial institution." (See Cal. Fin. Code, § 4052(b)(1)-(7).)

[4] *Id.*; Cal. Civ. Code, § 1798.140(o)(2).

[5] Cal. Civ. Code, § 1798.100(a)-(b).

[6] Cal. Civ. Code, § 1798.105(a).

[7] Cal. Civ. Code, § 1798.105(c).

[8] Cal. Civ. Code, § 1798.105(d).

[9] Cal. Civ. Code, § 1798.120(a). The ability to opt-out from sharing of personal information is akin to the protection already in place in the California Financial Information Privacy Act ("FIPA"), which requires that customers have an opportunity to opt-out from sharing of nonpublic personal information with a company's affiliates. (See Cal. Fin. Code, § 4053(b)(1).) Section 4053(a)(1) of the Act goes further in mandating that sharing of private data with non-affiliated third parties requires prior affirmative consent (i.e., "opt-in"). AB 375, of course, is far broader in application and scope.

[10] Cal. Civ. Code, § 1798.135(a)(1).

[11] Cal. Civ. Code, § 1798.135(a)(2).

consumer's data.[12] However, companies *can* compensate consumers for the collection, sale, or deletion of PI.[13] This will undoubtedly be an area for creativity by businesses.

The Act includes additional consumer protections, depending on the age of the consumer to whom the PI is associated. Consumers over 16 years have the right to opt-out of having their PI sold to third parties.[14] Consumers between the ages of 13 and 16, however, must opt-in before a company can share their data.[15] Meanwhile, companies cannot sell data for consumers under the age of 13 without parental consent.[16] Any company that willfully disregards a consumer's age will be deemed to have had actual knowledge of the consumer's age.[17]

The Scope of the Act

The expected impact of the Act on tech companies like Google and Facebook has received most of the recent press, but financial services companies need to be keenly aware of the potential pitfalls of the Act, as well. California is the world's sixth largest economy, after all, giving the Act broad coverage.

The Act will affect any business that serves consumers[18] in California[19] and that does one or more of the following: (i) has gross revenue of at least $25 million annually; (ii) interacts with information related to 50,000 or more people, households, or devices (aggregate); or (iii) makes half of its annual revenue from selling personal information. It also applies to holding companies and subsidiaries that share common branding.

While consumer marketing is at the forefront of business practices that has shaped the Act and other similar regimes (like the California Financial Information Privacy Act referenced in the footnotes), the Act also potentially applies to less obvious, more seemingly routine activities that could be cause for concern for financial services companies, such as the use of aggregated data by financial services or FinTech companies in making credit decisions; the use of apps that gather PI or utilize location services; tracking of spending patterns for various purposes, whether they be marketing or fraud detection; and operation of customer loyalty program (e.g., by credit card companies).

[12] Cal. Civ. Code, § 1798.125(a).
[13] Cal. Civ. Code, § 1798.125(b)(3)-(4).
[14] Cal. Civ. Code, § 1798.120(a).
[15] Cal. Civ. Code, § 1798.120(d).
[16] *Id.*
[17] *Id*.
[18] The term "consumer" refers to any "natural person who is a California resident…." Cal. Civ. Code, § 1798.140(g).
[19] "The term "resident," as defined in the law, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents." Cal. Code Regs. tit. 18, § 17014. "Domicile has been defined as the place where an individual has his true, fixed, permanent home and principal establishment, and to which place he has, whenever he is absent, the intention of returning. It is the place in which a man has voluntarily fixed the habitation of himself and family, not for a mere special or limited purpose, but with the present intention of making a permanent home, until some unexpected event shall occur to induce him to adopt some other permanent home." *Id*.

Mortgage companies or small-dollar lenders that utilize leads generated by a third party also need to be aware of the practices of the companies from whom they purchase data. Third parties such as lead generators are prohibited from selling PI that they purchased from a business unless the consumer receives explicit notice and an opportunity to opt-out.[20] It is yet to be seen how a failure to provide opt-out notices can impact businesses down the chain.

Enforcement and Remedies

There are two prescribed avenues for enforcement of the Act. First, consumers can file a private right of action.[21] The right is limited, however, to actions regarding the unauthorized access or exfiltration, theft or disclosure of a consumer's "nonencrypted or nonredacted personal information" resulting from a company's failure to maintain and implement security procedures to protect personal information.[22] Furthermore, PI in this context is defined more narrowly pursuant to California Civil Code section 1798.81.5(d)(1)[23] and includes simply an individual's first name or initial and last name in combination with any one or more of the following, when either the name or the data elements are not encrypted or redacted: (i) Social Security number; (ii) driver's license or California ID number; (iii) account number, credit or debit card number, *in combination with the requisite security code*; (iv) medical information; *or* (v) health insurance information.

Consumers can sue for $100 to $750 or actual damages, whichever is more.[24] Consumers can also sue for injunctive relief or any other relief the court deems proper.[25] Courts will take the relevant circumstances into consideration, including the number of violations, the willfulness of the defendant, and, similar to considerations regarding punitive damage awards, the defendant's assets, liabilities and net worth.[26]

Before a consumer can file suit, they must provide the offending business with notice and 30 days to cure the alleged breach.[27] The consumer must also notify the State Attorney General within 30 days of filing suit.[28] Once the AG has notice, they can decide whether or not to step into a consumer's private case.[29]

Alternatively, the AG can bring a civil action in the name of the people of the State to recover a civil penalty of $2,500 *per violation* under section 17206 of the California Business and Professions Code, which such violation is not cured within 30 days of notice.[30] This is the primary enforcement mechanism, given the limitations on private rights of action. The AG can also sue to recover $7,500 for *each intentional* violation.[31]

---

[20] Cal. Civ. Code, § 1798.115(d).
[21] Cal. Civ. Code, § 1798.150(a)(1).
[22] *Id.*
[23] *Id.*
[24] Cal. Civ. Code, § 1798.150(a)(1)(A).
[25] Cal. Civ. Code, § 1798.150(a)(1)(B)-(C).
[26] Cal. Civ. Code, § 1798.150(a)(2).
[27] Cal. Civ. Code, § 1798.150(b)(1).
[28] Cal. Civ. Code, § 1798.150(b)(2).
[29] Cal. Civ. Code, § 1798.150(b)(3)(A).
[30] Cal. Civ. Code, § 1798.155(a).
[31] Cal. Civ. Code, § 1798.155(b).

The remedies provided are significant, but the more restrictive ballot measure would have allowed consumers to sue for up to *five times* as much per violation. As such, it is easy to see why industry giants did not strongly oppose passage of the Act.

Compliance with the Act

Still, with a year and a half before implementation, there is plenty of time for the financial services industry to lobby for revisions to what will be the country's toughest data privacy protection scheme. But those businesses operating in California need to make ready to comply with the Act now. This will include ramping up privacy compliance procedures to implement such measures as:

- Detailing the consumers' rights under the Act in the company's online and written privacy policy.
- Amending privacy policies and procedures to include the following: steps for promptly verifying requests from consumers; procedures for verifying opt-out or deletion requests from an authorized third parties on a consumer's behalf; specifying that the company has a policy of honoring consumer requests for PI to be deleted and opt-outs; and detailing when a consumer request is so unreasonable that a response is not required and specify the language to be used in a written response to the consumer.
- Providing resources to customers to request disclosure and deletion of collected data and a to opt-out of data selling, such as including a link on the company's homepage; establishing an 800 or fax number; and/or specifying a mailing address.
- Responding to consumer requests within 45 days and free of charge unless an extension of time is warranted due to complexity of the request. Responses to consumer requests need to cover the most recent 12 month period of time.[32]
- Establishing a process for consumers to appeal written responses.
- Identifying applicable service providers and establish steps for requesting service providers to honor a consumer's opt-out or request for deletion.
- Developing and implementing thorough training for a specified team. Training should include the Act's intent, the consumers' rights, and the business' obligations to respond to consumer requests.

Information technology, risk management, marketing, regulatory compliance and leadership divisions of affected businesses alike are all implicated by the new rules and should work in concert to ensure a smooth transition in this new regulatory age.

Severson & Werson will continue to monitor and report on upcoming changes to the Act and related, breaking developments in consumer privacy. For questions, please contact Genevieve Walser-Jolly at grw@severson.com*, or any member of Severson & Werson's Data Privacy Group.*

[32] It may be instructive to consider the CFPB's guidelines on when a mortgage servicer is not required to respond to a Qualified Written Request. (12 CFR 1024.36.)