CALIFORNIA BANKERS ASSOCIATION
A DIVISION OF THE WESTERN BANKERS ASSOCIATION

Regulatory Compliance Bulletin

October 3, 2018

The 2018 California Consumer Privacy Act (SB 375 and SB 1121)

This article was written by Purvi G. Patel, Nathan D. Taylor, and Nancy R. Thomas of Morrison & Foerster LLP[1]

With the enactment of the California Consumer Privacy Act of 2018, the United States now has its first truly sweeping privacy regime. The Act is the product of backroom wrangling between legislators, industry, and the primary sponsor of a ballot initiative by the same name. Intended as an alternative to the initiative, the Act went from introduction to being signed into law by the Governor in just one week.

The law will impose significant and often first-of-their-kind privacy obligations on financial institutions and other businesses handling data related to California residents. The Act is complex and contains drafting errors and ambiguities that are by-products of the speed with which the legislation made its way to the Governor's desk. To address some of these issues, the Legislature approved limited amendments to the Act, which the Governor signed into law on September 23, 2018.

The following provides a high-level overview of the scope and requirements of the Act as amended.

Covered Businesses and Personal Information

Covered Businesses

The Act applies to any entity doing business in California that determines the purpose and means of processing personal information (PI) relating to California residents and that meets one of the following thresholds: (i) has annual gross revenues in excess of $25 million; (ii) annually buys, receives for its commercial purposes, sells, or shares for commercial purposes PI relating to 50,000 or more consumers, households, or devices; or (iii) derives 50% or more of its annual revenue from selling consumer PI.[2]

[1] Ms. Patel can be reached at ppatel@mofo.com. Mr. Taylor can be reached at ndtaylor@mofo.com. Ms. Thomas can be reached at nthomas@mofo.com.

[2] § 1798.140(c)(1)(A)–(C). Unless otherwise specified, all citations are to Cal. Civ. Code Title 1.81.5 (§§ 1798.100–1798.199) (added by Stats. 2018, Ch. 55, Sec. 3).

The Act defines "consumer" broadly to include all California residents.[3] Unlike other privacy laws that may focus on information relating to specific individuals (*e.g.*, customers, children, or patients), the Act applies with respect to PI relating to any California resident, regardless of a business's relationship to the individual, including, for example, employees, customers, and vendors who are residents of California.

Covered Personal Information

The Act defines "personal information" broadly to include any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[4] In addition, while the Act defines PI in detail, the Act references information linked to a particular "household," a term which is undefined and could include any child, spouse, or even roommate, creating uncertainty regarding the scope of the Act.

The definition of PI includes, but is not limited to, 11 enumerated categories of information relating to consumers, including:

- Commercial information, including a consumer's purchasing or consuming histories or tendencies.
- Internet activity, such as a consumer's browsing patterns, search history, or interaction with a website, application, or advertisement.
- Inferences drawn about the consumer from any of the enumerated categories of PI in order to create a profile about the consumer reflecting, for example, her preferences or characteristics.[5]

Other Important Definitions

The Act includes a number of definitions that are important to defining its scope and the extent of its obligations and limitations. The number of terms defined is extensive and should be closely reviewed. We highlight three definitions because they are relevant to the various individual privacy rights—the definitions for the terms "collect," "sale," and "business purpose." The Act broadly defines these terms to encompass many ways in which a business may handle PI.

Collecting

The Act defines the term "collects" as "buying, renting, gathering, obtaining, receiving, or accessing any [PI] . . . from the consumer, either actively, or passively, or by observing the consumer's behavior."[6] For example, if a business accesses PI (such as photos or contacts) from a consumer device, it

[3] § 1798.140(g).

[4] § 1798.140(o)(1). The term "household," however, is not defined.

[5] *See* § 1798.140(o)(1)(D), (F), (K).

[6] § 1798.140(e).

has "collected" PI even if such information is not stored or retained by the business.

Selling

The term "sale" is defined as disclosing PI to "another business or a third party for monetary or other *valuable* consideration."[7] It is unclear how broadly courts will interpret "valuable consideration." Nonetheless, how the term is interpreted will be critical because the definition of "sale" defines, among other things, the scope of the consumer opt-out right provided in the Act.

Collecting and Disclosing for a Business Purpose

The Act defines a "business purpose" as "the use of [PI] for the business' . . . operational purposes, or other notified purposes, provided that the use of [PI is] reasonably necessary and proportionate to achieve the operational purpose for which [the PI] was collected."[8] The Act divides "business purposes" into several categories of activities, including, for example, performing services, such as maintaining or servicing accounts, processing or fulfilling orders and transactions, processing payments, and providing analytic services. It is not clear if the definition's reference to the use of PI being "reasonably necessary and proportionate" to the purpose for which it was collected will be interpreted to function as a use limitation.

Scope – Exceptions and PI Exempted from the Act

Of particular importance to financial institutions, the Act, as amended, will not apply to information collected, processed, sold, or disclosed "pursuant to" the Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (SB1).[9] However, the GLBA/SB1 exception will not apply with respect to the Act's private right of action. That is, notwithstanding the exception, a consumer would still have a right under the Act to file suit relating to certain data security events, including those that involve information subject to the GLBA or SB1.

Moreover, the scope of the CCPA is broader than the scope of the GLBA and SB1. The GLBA and SB1 apply to information about consumers and customers who apply for or obtain financial products or services from a financial institution that "are to be used primarily for personal, family, or

[7] § 1798.140(t)(1) (emphasis added). Note that the Act includes a "service provider" exception to the definition of "sale." *See* § 1798.140(t)(2)(C). Because the Act defines sale as providing PI to either another *business* or a *third party*, sharing PI with entities meeting the "service provider" and/or "third party" exception brings that disclosure outside the scope of a "sale" for both the purpose of a business's disclosure obligations as well as consumers' opt-out right.

[8] § 1798.140(d).

[9] § 1798.145(e) (as amended by Stats. 2018, Ch. 735, Sec. 10).

household purposes."[10] As discussed above, the Act applies to information about California residents generally. Accordingly, financial institutions that are covered by the GLBA and SB1 will have to comply with the Act with respect to PI relating to California residents who are not consumers or customers under the GLBA, such as employees and individuals associated with business customers.

The Act includes several other exceptions, including: (i) where complying with the Act would interfere with compliance with legal processes;[11] (ii) for the collection of PI "wholly outside" California;[12] (iii) where compliance would violate an evidentiary privilege, such as the attorney-client privilege;[13] and (iv) for certain information covered by other state and federal privacy laws.[14]

Individual Privacy Rights

The Act creates four "core" individual privacy rights.

1. ***Right to Delete PI.*** First, the Act provides a consumer with the right to request that a business delete any PI that it has collected from the consumer.[15] The business must also direct service providers to delete a consumer's PI in response to a verified "deletion" request.[16]

   The Act, however, includes nine exceptions to the obligation to delete. Some of these exceptions are more clear cut, such as completing a transaction, detecting security incidents, or debugging to repair intended functionalities.[17] Others leave room for interpretation, such as where PI is used to "enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business,"[18] or where a business "[o]therwise use[s] the consumer's [PI], internally, in a lawful manner that is compatible with the context in which the consumer provided the information."[19]

[10] *See* 15 U.S.C. § 6809(9); 12 C.F.R. § 1016.3(e)(1); Cal. Fin. Code § 4052(f).

[11] § 1798.145(a)(1)–(4).

[12] § 1798.145(a)(6). Collecting PI "wholly outside of California" means (i) the business collected the PI while the consumer was outside California; (ii) no part of the sale of consumer's PI occurred in California; and (iii) no PI collected while the consumer was in California is sold. *Id*.

[13] *See* § 1798.145(b).

[14] *See* § 1798.145(c)–(f). These laws include the Confidentiality of Medical Information Act (CMIA), the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Driver's Privacy Protection Act (DPPA).

[15] § 1798.105(a).

[16] § 1798.105(c).

[17] § 1798.105(d)(1)–(3).

[18] § 1798.105(d)(7).

[19] § 1798.105(d)(9).

2. ***Right to Receive Information About, and Copies of, PI.*** The Act provides that, upon request, a business must disclose to a consumer the categories of PI that the business, within the year preceding the request, has: (i) collected; (ii) "sold" to a third party;[20] (iii) disclosed for a business purpose; and (iv) the categories of third parties to whom the business sold and/or disclosed PI for a business purpose.[21]

The Act requires that a business also disclose: (i) the business or commercial purpose for which PI was collected and/or sold; (ii) the categories of sources from which PI was collected; and (iii) the "specific pieces" of PI the business collected about an individual.[22] The Act's "portability" requirement greatly expands the scope and potential burden of responding to consumer requests. For example, a business must provide a consumer with the "specific pieces" of PI "in a readily useable format that allows the consumer to transmit [the] information from one entity to another entity without hindrance."[23]

To facilitate consumer requests for information, the Act requires businesses to make available two or more designated methods to request the information, including, at a minimum, a toll-free number and a website address (if the business has a website).[24] In addition, a business must disclose certain information about the Act online, including, if applicable, in its online privacy policy, and in any California-specific description of consumers' privacy rights.[25] This information, which must be updated at least once a year, includes: (i) a description of rights under the Act; and (ii) a list of categories of PI collected, sold to

[20] The Act defines "third party" in the negative to mean a person (which includes a corporate entity (*see* § 1798.140(n))) other than the business or a person receiving PI pursuant to a contract that prohibits it from: (i) selling the PI; (ii) retaining, using, or disclosing the PI for purposes other than those specified in the contract; and (iii) retaining, using, or disclosing the PI outside the direct relationship between the business and entity, and who signs a certification stating that the person understands these restrictions and will comply with them. § 1798.140(w)(1), (2). This definition creates what amounts to a service provider exception for entities subject to these contractual and certification requirements. This impacts businesses' disclosure obligations with respect to sales and disclosures for a business purpose, as well as consumers' opt-out rights. Moreover, the Act limits a business's liability for violations of the Act by persons covered by the third-party contractual/certification requirements. § 1798.140(w)(2).

[21] §§ 1798.110, 1798.115, 1798.130.

[22] §§ 1798.110(c), 1798.130(a)(5)(B).

[23] § 1798.130(a)(2).

[24] § 1798.130(a)(1).

[25] § 1798.130(a)(5).

a third party, or disclosed for a business purpose.[26]

3. *Right to Opt Out.* In general, the Act gives consumers the right to opt out of the "sale" of PI.[27] For consumers aged 16 or under, however, the Act requires that businesses obtain affirmative consent to sell PI either from the consumer (if the consumer is between ages 13 and 16), or from the consumer's parent or guardian (if the consumer is younger than age 13).[28]

   To enable consumer opt-out rights, the Act requires a "clear and conspicuous" link on the business's homepage, titled "Do Not Sell My Personal Information," as well as a link to the business's online privacy policy, if the business has one.[29]

4. *Right to Be Free from Discrimination.* The Act prohibits businesses from charging different prices or rates to consumers, providing different services, or denying goods or services to consumers who exercise their rights under the Act.[30] There are exceptions to this right, however, where, for example, the difference in prices or services is reasonably related to the value provided by the consumer's data.[31] The Act also allows businesses to offer financial incentives in connection with the collection, sale, or deletion of PI.[32] Consumers must opt in to such financial incentives programs, and may revoke their consent at any time.[33]

Private Right of Action and Attorney General Enforcement

The Act provides for enforcement both through private rights of action for consumers and through administrative enforcement.

The Act allows a consumer to sue if non-encrypted or non-redacted PI (as defined in the California safeguards law) "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of [a] violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."[34] As amended, the Act clarifies that the right to sue is limited to the described data security events and

[26] § 1798.130(a)(5)(A)–(C).

[27] § 1798.120(a).

[28] § 1798.120(d).

[29] § 1798.135(a)(1), (2). If a business has a separate page for California consumers and takes reasonable steps to direct Californians to that page, the business does not have to include the "Do Not Sell" link on its homepage. § 1798.135(b).

[30] § 1798.125(a)(1).

[31] § 1798.125(a)(2).

[32] § 1798.125(b)(1).

[33] § 1798.125(b)(3).

[34] § 1798.150(a).

does not apply to violations of the Act's privacy obligations.[35]

The Act provides the California Attorney General (AG) with exclusive jurisdiction to sue for violations of the Act, and provides that a business "shall be in violation of" the Act if the business fails to cure an alleged violation within 30 days after being notified of the violation.[36] The AG can seek an injunction and civil penalties of either $2,500 per non-intentional violation or $7,500 per intentional violation.[37]

Operative Date and Regulations

The Act's operative date is January 1, 2020.[38]

Critical to the Act's scope and requirements, the Act requires the AG to adopt implementing regulations on certain issues, including, for example, establishing exceptions, rules, and procedures for compliance.[39] The AG also can adopt additional regulations as necessary to further the Act's purposes.[40]

The AG has until July 1, 2020 to adopt these regulations and is required to solicit "broad public participation" for its rule writing.[41] The AG may bring enforcement actions starting July 1, 2020, or six months after the AG issues final regulations, whichever is sooner.[42] This creates uncertainty on the timing of potential AG enforcement actions. If the AG publishes the final regulations:

- Before June 30, 2019, enforcement actions could start on January 1, 2020.
- Between July 1, 2019 and December 31, 2019, enforcement actions could start sometime between January 1, 2020 and July 1, 2020, depending on the exact publication date.
- Between January 1, 2020 and July 1, 2020, enforcement actions could start on July 1, 2020, potentially leaving businesses with little or no time to comply with the published regulations.

Next Steps and Takeaways

The California Consumer Privacy Act is a first, not only because of its expansive scope, but also because of the legislative process by which it was enacted. Never

[35] § 1798.150(c) (as amended by Stats. 2018, Ch. 735, Sec. 11). This amendment largely puts to rest the debate as to the scope of the private right of action, but the provision, even as amended, continues to include drafting issues with repeated references to "violations of this title" in § 1798.150(b).

[36] § 1798.155(a).

[37] § 1798.155(b) (as amended by Stats. 2018, Ch. 735, Sec. 12).

[38] § 1798.198.

[39] § 1798.185(a) (as amended by Stats. 2018, Ch. 735, Sec. 13). The Governor signed legislation giving the AG $700,000 and five new staff members to write these regulations (Stats. 2018, Ch. 449).

[40] § 1798.185(b).

[41] § 1798.185(a); *see* § 1798.185(a)(3), (6), (7).

[42] § 1798.185(c) (as added by Stats. 2018, Ch. 735, Sec. 13).

before has such sweeping privacy legislation been enacted in the span of a single week, with limited input from key stakeholders. This fast track averted the ballot initiative and the challenges presented by the initiative, but even after amendment, it left a complex—and messy—privacy regime whose exact scope and requirements are not clear.

Businesses undoubtedly will continue their efforts to identify and advocate for amendments, such as narrowing the definition of "consumer," specifying the extent to which the Act applies in the context of vendor relationships, and clarifying whether the Act requires pre-collection notice to consumers. Separately, financial institutions and other businesses should also monitor for any regulatory proposals by the California AG to implement the Act and be prepared to advocate accordingly.

Over the long term, financial institutions and other businesses will need to assess the Act's many obligations, mindful of the AG's implementing regulations and any potential legislative "fixes" that may be enacted. The compliance process for many businesses will be a complex one that will require a significant investment of time and resources even for those institutions for which the Act will not apply to many, if not most, of their customers. In some areas, business may find efficiencies in the steps required to develop a compliance plan. Identifying the various places where PI is stored will be relevant not only to the right to deletion but also to the right to receive a disclosure of the "specific pieces" of PI collected. Nonetheless, it is clear that the burden associated with compliance with the Act will far outweigh what many U.S. companies will have previously experienced.

Kevin Gould was CBA's lead lobbyist on SB 375 and SB 1121.