SULLIVAN & CROMWELL LLP

July 2, 2018

California Consumer Privacy Act of 2018

New Statute Introduces Privacy Protections for California Consumers and Subjects Businesses to Potential Liability

SUMMARY

On June 28, 2018, California enacted the California Consumer Privacy Act (the "CCPA" or the "Act"), which will take effect on January 1, 2020.[1] The Act applies to any organization that conducts business in California and satisfies one of three conditions: (1) has annual gross revenue in excess of $25,000,000;[2] (2) annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices, alone or in combination; or (3) derives 50 percent or more of its annual revenue from selling consumers' personal information (each, a "Covered Business").[3] The Act also applies to any entity that "controls or is controlled by" any Covered Business.[4]

As detailed below, the CCPA establishes a new privacy framework for Covered Businesses by:

- Creating an expanded definition of personal information for purposes of the Act;
- Creating new data privacy rights for California consumers, including rights to know, access, have deleted and opt out of the sale of their personal information;
- Imposing special rules for the collection of consumer data from minors; and
- Creating a new and potentially severe statutory damages framework for violations of the Act and for businesses that fail to implement reasonable security procedures and practices to prevent data breaches.

The CCPA has significant implications for all Covered Businesses. The Act also allows potentially substantial penalties to be imposed on companies even in the absence of demonstrated consumer harm, and provides the California Attorney General with broad implementing authority.[5] For these reasons, and because compliance with the Act may require substantial lead-time and investment, businesses that are potentially subject to the Act should begin preparing and implementing a plan for compliance as soon as

possible. There may also be questions as to whether certain provisions of the CCPA are preempted by federal statutes such as the National Bank Act.

BACKGROUND

In September 2017, Alastair Mactaggart and Mary Ross proposed a statewide ballot initiative entitled the "California Consumer Privacy Act." Ballot initiatives are a process under California law in which private citizens can propose legislation directly to voters, and pursuant to which such legislation can be enacted through voter approval without any action by the state legislature or the governor.[6] While the proposed privacy initiative was initially met with significant opposition, particularly from large technology companies, some of that opposition faded in the wake of the Cambridge Analytica scandal and Mark Zuckerberg's April 2018 testimony before Congress.[7] By May 2018, the initiative appeared to have garnered sufficient support to appear on the November 2018 ballot.[8] On June 21, 2018, the sponsors of the ballot initiative and state legislators then struck a deal: in exchange for withdrawing the initiative, the state legislature would pass an agreed version of the California Consumer Privacy Act.[9] The initiative was withdrawn, and the state legislature passed (and the Governor signed) the CCPA on June 28, 2018.[10]

KEY PROVISIONS OF THE CCPA

Expanded Definition of Personal Information.

Under the Act, "personal information" ("PI") is broadly defined to mean "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 Act specifies that PI includes, but is not limited to: (i) identifiers, such as names, aliases, addresses, and IP addresses; (ii) characteristics of protected classifications under California or federal law; (iii) commercial information, including records of personal property, products or services purchased, or consuming histories or tendencies; (iv) biometric information; (v) Internet or other electronic network activity information, such as browsing history; (vi) geolocation data; (vii) audio, electronic, visual, thermal, olfactory, or similar information; (viii) professional or employment-related information; (ix) education information; and finally, (x) any inferences drawn from any of the information identified to create a profile about a consumer.[11]

The Act does, however, include a few limitations. First, the Act excludes "aggregate consumer information," which is defined as data that is "not linked or reasonably linkable to any consumer or household, including via a device."[12] Data kept in such a fashion does not fall within the definition of PI. Second, information that is publicly available from federal, state, or local government records is similarly excluded.[13]

The Act applies to *all* PI collected by Covered Businesses from consumers, who the Act defines as natural persons who are California residents, whether or not collected electronically.[14] Accordingly, the Act applies not only to Internet-based businesses, but also to businesses ranging from brick-and-mortar

stores to large financial institutions. Covered Businesses that collect consumer information should carefully evaluate what portions of the information they collect may constitute PI and therefore be subject to the provisions of the CCPA.

Five Categories of Rights

The Act enumerates five categories of data privacy rights granted to consumers with respect to their PI: the "right to know," the "right to access," the "right to deletion," the "right to opt out," and the "right to equal service." These rights create a variety of obligations for Covered Businesses.

1. The Right to Know

The right to know requires Covered Businesses to make both affirmative disclosures to all consumers and respond to verifiable consumer requests with individualized disclosures about the business's collection, sale, or disclosure of the PI of the *particular* consumer making the information request. In their privacy policies or otherwise on their website if they do not have such policies, Covered Businesses must affirmatively disclose:

- At or before the time of collection, what PI the business will collect about its consumers and the purposes for which such data will be used;[15]
- The categories of consumers' PI that were actually collected in the preceding 12 months; and[16]
- The categories of consumers' PI that were sold[17] or disclosed for business purposes[18] in the preceding 12 months.[19]

In response to verifiable consumer requests, Covered Businesses must also disclose:

- What categories of the requesting consumer's PI were actually collected in the 12 months preceding the consumer's verifiable request.[20]
- What categories of the requesting consumer's PI were sold or disclosed for business purposes in the 12 months preceding the consumer's verifiable request.[21]

As part of their disclosures regarding data *collection*, businesses must include information about the categories of sources from which the PI was collected, the business or commercial purpose for "collecting or selling" that PI,[22] and the categories of third parties[23] with whom the business has shared the PI.[24] As part of their disclosures regarding data *sales or disclosures*, businesses must disclose, as applicable, the categories of PI sold and to whom it was sold, or the categories of PI disclosed for a business purpose and to whom it was disclosed.[25] If the request only pertains to sale, and not collection, the business need not disclose the sources of the PI.[26]

Businesses must provide at least two methods by which consumers can make verifiable consumer requests for disclosure, including, at a minimum, a toll-free number and an online form.[27] The deadline for providing requested disclosures is 45 days from receipt of the request.[28]

The Act also provides that the following circumstances do not constitute a sale of PI:[29]

- Consumer-directed disclosure or use that was intended by the consumer.
- Use of PI for the purposes of identifying a consumer who has opted out under the opt-out provision.
- Sharing PI with a service provider that is necessary for the performance of a business purpose, if the business has provided notice to its consumers, the service provider is acting on the business's behalf, and the service provider does not sell the PI.
- The business transfers PI to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction where the third party "assumes control of all or part of the business," subject to certain conditions.[30]

2. The Right to Access

The CCPA further guarantees consumers the right to access a copy of the "specific pieces of personal information that [a business] has collected about that consumer" to be delivered either by mail or electronically.[31] Whereas the right to know only provides consumers with information about what *categories* of PI have been collected, sold, or disclosed, the right to access provides consumers with a copy of the PI collected about them.

This right may also imply some duty to preserve. Unlike the right to know, this portion of the Act does not expressly specify whether businesses will have the obligation to preserve the PI collected about each consumer, only that the businesses need to provide the specific PI collected about the consumer. Considering that the Act provides that businesses that have collected PI for "single, one-time transaction[s]" have no obligation to retain any PI,[32] that may imply some duty to preserve may exist for data collected under other circumstances.

3. The Right to Deletion

The CCPA allows consumers to request the deletion of their PI from business servers and service providers.[33] Covered Businesses will be obligated to honor the deletion request unless it is necessary to maintain the PI in order to:

- Complete the transaction for which the PI was collected, provide a good or service requested by the consumer, or otherwise perform a contract between the business and the consumer.
- Detect and maintain data security.
- Debug to identify and repair errors.
- Exercise a right provided for by law.
- Comply with the California Electronic Communications Privacy Act.
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest when deletion would render it impossible or seriously impair the achievement of such research.
- Comply with legal obligations.
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

- Otherwise use the consumer's PI internally in a lawful manner that is compatible with the context in which the PI was provided.

The last two "internal use" exceptions require careful attention by Covered Businesses to ensure that, consistent with long-standing best practice for privacy policies, consumers are clearly advised at the time PI is collected of the potential internal uses of their data.

4. The Right to Opt Out

Under the Act, consumers may opt out of the sale of their PI to third parties.[34] If an individual consumer does not affirmatively opt out, and such consumer is not a minor (as discussed below), their data may be sold without further action (provided that sale is disclosed in the business's privacy policy). Covered Businesses, however, must post a "clear and conspicuous link" entitled "Do Not Sell My Personal Information" on their national website or California-specific webpage,[35] describe the right and include a link to the opt-out page in their privacy policy,[36] and ensure that "all individuals responsible for handling consumer inquiries" about privacy practices and CCPA compliance are informed of the opt-out requirements and "how to direct consumers to exercise their [opt-out] rights."[37]

In order to implement this system, Covered Businesses will need to separate consumer PI that they wish to sell into at least two categories: (1) PI of consumers who have opted out, and (2) PI of consumers who have not opted out.[38] Covered Businesses that do not nationally conform to California's system may also need a third category of PI for non-California residents. Further, minors have distinct rights, discussed below. Consumers can opt in or out at any time, and businesses must "respect the consumer's decision . . . for at least 12 months before requesting that the consumer authorize the sale of [their PI]."[39]

5. The Right to Equal Service

The CCPA grants a right to equal service, prohibiting discrimination against consumers who exercise their rights under the Act.[40] Covered Businesses are generally prohibited from denying goods or services to those consumers, charging them different prices or rates (including through use of discounts or other benefits), or providing them with a different level or quality of service.[41] Businesses may be permitted, however, to charge these consumers different rates or to provide different levels of service provided there is some relationship to the "value provided to the consumer by the consumer's data."[42] Businesses may also offer financial incentives, including payments to consumers as compensation, for the collection or deletion of PI.[43] It is uncertain at this point how these permitted pricing differentials will work in practice, and it appears likely that Covered Businesses will ask for further guidance.

Special Rules for Minors

The CCPA generally prohibits the sale of PI if the business has actual knowledge that the consumer is less than 16 years of age or willfully disregards the consumer's age.[44] If the business wishes to sell such information, it must obtain affirmative consent from the consumer if they are between the ages of 13 and 16, or their parents' consent if they are under 13—creating a special opt-in system for minors.[45]

Public Enforcement Framework

Except in the data breach context, there is no private cause of action available under the Act. Rather, the only enforcement mechanism for violations of the Act is by the California Attorney General. For violations of the Act, a Covered Business is subject to statutory damages as follows:

- Damages for a violation of the Act that the business did not cure within 30 days of notice: up to $2,500 per violation.[46]
- Damages for intentional violations: up to $7,500 per violation,[47] in addition to the $2,500.[48]

The Act creates a 30-day window for businesses to cure violations.[49] Proceeds of any settlement or award will be allocated to a new fund called the "Consumer Privacy Fund," intended to offset any costs incurred by the state courts or California Attorney General in connection with the Act.[50] The Act provides that any business or third party may seek the opinion of the Attorney General for *ex ante* guidance on "how to comply with the provisions" of the Act.[51]

Private Action: Liability for Data Breach

Under the Act, Covered Businesses are liable for the unauthorized access and exfiltration, theft, or disclosure of certain categories of "nonencrypted or nonredacted"[52] PI due to the business's failure to implement reasonable security procedures and practices appropriate for the particular type of PI.[53] Significantly, liability does not appear to require a showing of consumer harm, and statutory damages may be significant. The Act provides for statutory damages, in action brought by a consumer, of between $100–$700 per violation per consumer or actual damages, whichever is higher.[54] In addition to this limited private cause of action,[55] the Act authorizes the California Attorney General to bring a public enforcement action, as described above.[56]

Notably, for the purpose of data-breach liability only, PI is defined pursuant to California Civil Code § 1798.81.5(d)(1)(A).[57] This definition is much narrower than the general definition of PI included in the Act. For purposes of data-breach liability, PI means an individual's first name or first initial and last name in combination with one of the following:

- Social Security number.
- Driver's license number or California ID number.
- Account number, credit or debit card number, in combination with the requisite security code.
- Medical information.
- Health insurance information.

As a result, the Act expands potential data-breach liability because it not only permits suit in the absence of a showing of both particularized and concrete harm but also creates a private right of action with an associated statutory damages framework.

To bring a private claim or class action, consumers must provide businesses with 30-days' written notice.[58] In the event that cure is possible within 30 days, the business may be able to avoid statutory damages, but not actual pecuniary damages (if they exist).[59] After 30 days, if the breach has not been cured, consumers may bring an action but must also notify the Attorney General, who has 30 days from notification to either bring an enforcement action, notify the consumer of the intent to bring an enforcement action, refrain from acting, or notify the consumer bringing the action "that the consumer shall not proceed with the action."[60] If the Attorney General refrains from acting or notifies the consumer of the intent to bring an action but fails to do so within six months, the consumer may bring an action against the company for statutory damages due to data breach.[61]

EXCEPTIONS

The Act also creates several exceptions. By its terms, it will not restrict a business's ability to:

- Comply with federal, state, or local laws.
- Comply with civil, criminal, or regulatory inquiries or investigations.
- Cooperate with law enforcement agencies.
- Exercise or defend legal claims.
- Collect, use, retain, sell or disclose consumer information that is de-identified or aggregate consumer information. "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed and is not reasonably likable to a consumer or device. "Deidentified" information is information that "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer."[62] To fall within this exception, businesses must implement technical safeguards that prohibit reidentification, business processes that specifically prohibit reidentification, business processes to prevent inadvertent release of deidentified information. Finally, they must make no attempt to reidentify information.[63]
- Collect or sell consumer information so long as every aspect of the commercial conduct takes place outside of California—meaning that the data was collected while the consumer was outside the state and no part of the sale occurred within the state.[64]

The Act creates several exemptions as well. The Act shall not apply where:

- Compliance would interfere with or violate evidentiary privileges.
- The information is protected or health information governed by the Confidentiality of Medical Information Act or governed by HIPAA.
- The sale of information is to or from a consumer reporting agency that is to be reported in or used to generate a consumer report.
- The information is collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act (Public Law 106–102) *if it is in conflict with the Act*.
- The information is collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 *et seq.*) *if it conflicts with the Act*.

Finally, the Act creates several limits on secondary liability:

- A limit on liability for businesses that have disclosed PI to third parties that subsequently violate the Act. To qualify for this limit, a business must only disclose PI pursuant to a contract including specific provisions.[65] The contract must include a certification that the third party understands the requirements of the Act and provisions prohibiting the third party from reselling the data, retaining or using the data for any purpose other than what was enumerated in the contract, and retaining or using the data outside of the direct business relationship between the third party and the disclosing business.[66] A business that abides by these requirements is immune from liability for violations of the Act by such third-party recipients.[67]
- A limit on liability for businesses that disclose PI to service providers that subsequently violate the Act. To qualify for this limit, a business must establish that at the time of disclosing the PI, it did "not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation.[68]
- A limit on liability for service providers when the business for which it provides services violates the Act.[69]

BRIEF COMPARISON WITH THE EUROPEAN UNION'S ("EU") GENERAL DATA PROTECTION REGULATION ("GDPR")[70]

At a high level, the CCPA bears certain similarities to GDPR, the comprehensive regulation governing the "processing of personal data" of EU residents.[71] But the CCPA and GDPR provide for differing rights, obligations, and exceptions, and compliance with one will not necessarily ensure compliance with the other. For example, unlike GDPR, the CCPA does not generally (other than with respect to minors) require businesses to implement an "opt-in" system to obtain consumers' consent prior to processing their information.[72] Instead, the CCPA requires businesses to allow consumers to "opt-out" of having their information sold.[73] Thus, businesses will need to develop a CCPA compliance strategy in light of these and other differences with GDPR. Businesses may choose to adopt differentiated policies for consumers in different jurisdictions, or may seek to create a unified global policy that adopts the most consumer-favorable protections from the CCPA and GDPR (and, of course, other applicable regulations).

IMPLICATIONS

The CCPA will require businesses to take several steps to come into compliance on or before the effective date of January 1, 2020.

- As of the effective date, privacy policies will need to be updated with information about opting out with a link to the opt-out page and information required by the right to know (*i.e.*, information about which categories of PI the business is collecting and will collect in the future, a list of categories of PI that the business has collected in the preceding 12 months, a list of categories of PI that the business has sold in the preceding 12 months, and a list of categories of PI that the business has disclosed for a business purpose in the preceding 12 months).
- Because of the right to know and right to deletion, businesses will need to implement a framework to track and respond to potentially large numbers of consumer requests, identify data that relates to consumers across diverse systems and platforms, and aggregate (and ideally encrypt) the data

so that it can be communicated to consumers. Businesses will need to understand and map their data so they can act on consumer requests efficiently.

- As of the effective date, businesses will need to be able to identify and segregate all consumer data they may sell. All consumer data, whether online or offline, will need to be separated into different categories to ensure no data of a California resident who has opted out is sold. For many businesses, this will require a substantial investment.
- Businesses planning on mergers, acquisitions, or transactions involving consumer data should seek legal advice to determine if and how the Act would impact the transaction. Although such business processes are excepted from the rules governing the right to know about the sale of PI, the Act requires "sufficiently prominent and robust" notice if a third party "materially alters" how a consumer's data is used, and because consumers have consumer-specific rights guaranteeing access to certain information, this is particularly troublesome information for mergers, acquisitions, and transactions that are not otherwise publicly disclosed.[74]
- Businesses need to consider how to apply the requirements of the CCPA with their information technology systems that handle PI and address potential challenges in applying the new rules to important areas like big data analytics and artificial intelligence algorithms that leverage PI.
- As of the effective date, training programs will need to be developed and implemented for employees responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the Act.
- Businesses should verify and update, if necessary, any security procedures and practices so that they are appropriate to the nature of the information being protected.
- Businesses disclosing information to third parties should only do so pursuant to a written agreement that complies with the restrictions on using, retaining, disclosing, and selling any PI that is provided to these third parties.[75]
- As of the effective date, businesses will need to offer a toll-free number and a website allowing consumers to opt out.

Among the implications for many other industries, financial institutions may need to take special care with respect to certain provisions of the Act:

- Banks will need to consider the impact that the "right to opt-out" would have on a bank's ability to transfer to third parties the information accompanying loans and other instruments, including for securitization and pooling transactions.
- Financial institutions will be able to collect and keep consumer data for information like bank and brokerage accounts, though there may be heightened notice requirements.
- Financial institutions will be permitted to acquire customer account information through merger and acquisition, but may be subject to heightened notice requirements.
- Financial institutions should be able to sell or transfer information to service providers, but there may be additional notification requirements. Banks will not be liable if the service provider uses the PI in violation of the Act so long as the Bank does not have actual knowledge or reason to believe that the service provider intends to commit such a violation.

* * *

ENDNOTES

1 California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.198(a) (2018).

2 Pursuant to § 1798.185(a)(5), this number will be adjusted every odd-numbered year to reflect any increase in the Consumer Price Index.

3 *Id.* § 1798.140(c)(1).

4 *Id.* § 1798.140(c)(2).

5 *Id.* § 1798.155.

6 *How to Qualify an Initiative*, CAL. SECRETARY OF STATE, http://www.sos.ca.gov/elections/ballot-measures/ (last accessed June 29, 2018).

7 *See Committee to Protect California Jobs*, CAL. SECRETARY OF STATE, http://cal-access.sos.ca.gov/Campaign/Committees/Detail.aspx?id=1401518&session=2017&view=received (last accessed July 1, 2018); *see also* Sasha Ingber, *Facebook Will Stop Funding Opposition To A User Privacy Initiative in California*, NPR (Apr. 12, 2018), https://www.npr.org/sections/thetwo-way/2018/04/12/602002272/facebook-will-stop-opposing-a-user-privacy-initiative-in-california; Christopher Crosby, *Verizon Exits Fight Against Proposed Calif. Privacy Law*, LAW360 (May 9, 2018, 3:37 PM), https://www.law360.com/articles/1041676/verizon-exits-fight-against-proposed-calif-privacy-law.

8 To appear on the November 2018 ballot, an initiative needed to submit 365,800 verified signatures by June 28; Mactaggart and Ross submitted 629,000. *California Consumer Privacy Act Clears Major Hurdle: Submits 629,000 Signatures Statewide*, CALIFORNIANS FOR CONSUMER PRIVACY (May 3, 2018), https://www.caprivacy.org/post/california-consumer-privacy-act-clears-major-hurdle-submits-625-000-signatures-statewide. The proposed initiative was withdrawn before verification could be completed.

9 John Myers & Jazmine Ulloa, *California lawmakers agree to new consumer privacy rules that would avert showdown on the November ballot*, L.A. TIMES (June 21, 2018, 8:40 PM), http://www.latimes.com/politics/la-pol-ca-privacy-initiative-legislature-agreement-20180621-story.html.

10 *See* CAL. CIV. CODE § 1798.198(b) (making the Act contingent upon withdrawal of ballot initiative 17-0039); *see also Initiatives and Referenda Withdrawn or Failed to Qualify*, CAL. SECRETARY OF STATE, http://www.sos.ca.gov/elections/ballot-measures/initiative-and-referendum-status/failed-qualify/ (last accessed June 29, 2018) (listing the status of ballot initiative 17-0039 as having been withdrawn on June 28, 2018).

11 *Id.* § 1798.140(o)(1). It is important to note that the provisions of the CCPA are "not limited to information collected electronically or over the Internet," but apply to brick-and-mortar businesses as well. *Id.* § 1798.175.

12 *Id.* § 1798.140(a).

13 *Id.* § 1798.140(o)(2).

14 *Id.* § 1798.175.

15 *Id.* § 1798.100(b).

16 *Id.* § 1798.110(c).

17 The Act specifically prohibits third parties from further sale of PI unless the consumer has received explicit notice and is provided with an opportunity to opt out. *Id.* § 1798.115(d).

18 "Business purpose" is defined as "the use of personal information for the business' or a service provider's *operational purposes*, or other notified purposes, provided that the use of [PI] shall be reasonably necessary and proportionate to achieving the operation purpose for which the [PI]

was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected." *Id.* § 1798.140(d). Among the several enumerated purposes, the Act provides that "Business purposes are . . . Performing services on behalf of the business or service provider, including . . . providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider." This could somewhat undercut the restrictions on "sale." Additionally, it is possible that disclosure may occur for non-business purposes. It is unclear whether such disclosures will require notice to consumers.

19 *Id.* §§ 1798.110(c); 1798.115(c).

20 *Id.* § 1798.110(a).

21 *Id.* § 1798.115(b).

22 The Act require businesses that collect PI to make disclosures that go beyond merely what PI was collected. As part of the disclosure, the Act requires information about "[t]he business or commercial purpose for *collecting or selling* personal information." *Id.* § 1798.110(a)(3).

23 The Act defines "third party" to exclude persons to whom data is disclosed pursuant to a written contract prohibiting the party from (i) selling the information, (ii) retaining, using, or disclosing the information for any purpose other than performing the services enumerated in the contract, and (iii) retaining, using, or disclosing the information outside of direct business relationships between the person and the business. *Id.* § 1798.140(w). If a person, under such a contract, violates any of the restrictions set forth in the Act, the disclosing business will not be liable, only the person will. *Id*. § 1798.140(w)(2)(B).

24 *Id.* § 1798.110(a).

25 *Id.* § 1798.130(a)(4).

26 *Compare id.* § 1798.110(a), *with* § 1798.115(b), *and* § 1798.130(a)(4).

27 *Id.* § 1798.130(a)(1).

28 *Id.* § 1798.130(2). Extensions are sometimes available, but the Act is not clear as to whether the extension is an additional 45 days, *see id.* § 1798.130(2), or an additional 90 days, *see id.* § 1798.145(g)(1).

29 *Id.* § 1798.140(t)(2).

30 *Id.* § 1798.140(t)(2)(D).

31 *Id.* § 1798.110(a)(5). If disclosure is made electronically, in a portable—and to the extent technically feasible—readily useable format, consumers will have the capability of transmitting this information to other entities without hindrance.

32 *Id.* § 1798.100(e).

33 *See id.* § 1798.105.

34 *Id.* § 1798.120(a).

35 *Id.* § 1798.135(a)(1).

36 *Id.* § 1798.135(2).

37 *Id.* § 1798.135(a)(3).

38 The Act does not describe the process in which consumers opt in. *See id.* § 1798.120(d). Presumably, this will be clarified by regulations passed under § 1798.185(b) (giving the Attorney General broad authority to pass necessary regulations outlining different processes) or through legislative amendment.

ENDNOTES (CONTINUED)

39 *Id.* § 1798.135(a)(5).

40 *Id.* § 1798.125(a)(1).

41 *Id.* § 1798.125(a)(1).

42 *Id.* § 1798.125(a)(2).

43 *Id.* § 1798.125(b).

44 *Id.* § 1798.120(d).

45 *Id.*

46 *Id.*

47 The Act is not clear as to whether "per violation" in this context means per incident per consumer or merely per incident—a distinction that could mean the difference between $2,500 in damages and $250,000,000 for an incident affecting 100,000 consumers. In the June 28, 2018 Senate Floor Analysis (one of the last pieces of legislative history prior to passage), the report discusses statutory damages in the data breach context as "per consumer per incident." *See California Legislative Information: Senate Floor Analysis* (June 28, 2018), *available at* https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375. This is suggestive that "per violation" really means "per incident per consumer."

48 *Id.* § 1798.155(b).

49 *Id.* § 1798.155(a).

50 *Id.* §§ 1798.155(c); 1798.160.

51 *Id.* § 1798.155(a).

52 The Act does not specify the level of encryption required or define "nonredacted" PI. *See id.* § 1798.150(a)(1). These terms can be subject to numerous interpretations.

53 *Id.* § 1798.150.

54 *Id.* § 1798.150(a)(1)(A).

55 The provision that provides for the private cause of action uses ambiguous language to outline its limitations. The private cause of action is limited to actions pursuant to the data breach section, but uses language requiring purported plaintiffs to provide 30-days' written notice "identifying the specific provisions of this title the consumer alleges to have been or are being violated." *Id.* § 1798.150(b)(1). Despite this ambiguity, a report issued by the Assembly Committee on Privacy and Consumer Protection stated that the statute only created a "limited private right of action" for data breaches. *Informational Hearing Report*, ASSEMBLY COMM. ON PRIVACY AND CONSUMER PROT., (June 27, 2018) https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375.

56 CAL. CIV. CODE § 1798.155(a)–(b); *see also* CAL. BUS. & PROF. CODE § 17206.

57 *Id.* § 1798.150(a)(1).

58 *Id.* § 1798.150(b)(1).

59 *Id.*

60 *Id.* § 1798.150(b)(3).

61 *Id.* It seems intended by the Act that if the Attorney General brings an action during the 30-day period or notifies the consumer during that period that the Attorney General intends to bring an action within six months, the consumer cannot proceed with their private right of action. *See id.*

62 *Id.* § 1798.140(h).

ENDNOTES (CONTINUED)

63 *Id.* § 1798.140(h)(1)–(3).

64 *Id.* § 1798.145(a)(6). Businesses are also prohibited from storing PI about a consumer while the consumer is in California and then collecting that PI when the consumer and stored personal information is outside of California. *Id.*

65 *Id.* § 1798.140(w)(2).

66 *Id.* § 1798.140(w)(2).

67 *Id.* § 1798.140(w)(2)(B).

68 *Id.* § 1798.145(h).

69 *Id.*

70 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

71 *Id*.

72 CAL. CIV. CODE § 1798.120; General Data Protection Regulation Art. 7.

73 CAL. CIV. CODE § 1798.120. The CCPA only requires businesses to allow consumers to "opt-out" of having their information sold to third parties. Unlike GDPR, the CCPA does not require businesses to allow consumers to "opt-out" of having their data processed in other ways.

74 *Id.* § 1798.140(t)(2)(D).

75 *Id.* § 1798.140(w)(2)(A).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Los Angeles		
Patrick S. Brown	+1-310-712-6603	brownp@sullcrom.com
Eric M. Krautheimer	+1-310-712-6678	krautheimere@sullcrom.com
Rita-Anne O'Neill	+1-310-712-6698	oneillr@sullcrom.com
Alison S. Ressler	+1-310-712-6630	resslera@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5600	mousavin@sullcrom.com
Sarah P. Payne	+1-650-461-5669	paynesa@sullcrom.com
John L. Savva	+1-650-461-5610	savvaj@sullcrom.com