Updated Alert: Governor Brown Signs Amendments to the California Consumer Privacy Act of 2018

by Joseph Lynyak

1. Introduction

On June 28, 2018, the California Legislature unanimously passed, and the Governor immediately signed, a sweeping expansion of data privacy protections for residents of California.[1] Assembly Bill No. 375, entitled the "California Consumer Privacy Act of 2018" (the "CCPA"), goes far beyond current U.S. privacy protections, and in many respects emulates elements contained in the European Union's General Data Protection Regulation (the "GDPR"), including the ability of a consumer to require that personal information be deleted by a covered business.[2]

Because of an unavoidable deadline to adopt the CCPA, discussed below, numerous drafting errors and patent ambiguities were contained in the legislation as finally adopted. In anticipation of this issue, a clean-up bill to address many of these problems was adopted on the last day of the California legislative session for 2018. That clean-up bill—Senate Bill 1121—was signed by Governor Brown on September 23, 2018.[3]

This updated alert incorporates many of the significant changes made to the original version of the CCPA, and also contains a separate discussion of many of the changes made by S.B. 1121, as well as compliance concerns businesses should consider as the effective date for the CCPA approaches.

2. Discussion

The numerous statutory provisions of the CCPA accomplish several stated goals, including: (a) the establishment of the rights of consumers in regard to their data; (b) providing a process whereby consumers can determine whether—and to what extent—a covered business is holding, selling and transferring their personal information; (c) requiring covered businesses to implement specific procedures to maintain consumer data and respond to consumer inquiries; (d) exempting (or partially exempting) certain business data collection and transfer practices from the coverage of the CCPA; (e) imposing liability for non-compliance by means of enforcement actions authorized to be

Related People

- Joseph Lynyak

Related Capabilities

- Financial Services Regulatory
- Privacy & Social Media
- Consumer Financial Services
- Securities & Financial Services Litigation & Enforcement
- California Consumer Privacy Act (CCPA)

brought by the California Attorney General and private parties; and (f) authorizing the California Attorney General to issue interpretations and regulations to implement the CCPA.[4]

A. Background

The genesis of the CCPA was the explosion of data breach incidents in the past few years, as well as a wave of continuing revelations that many social media sites (considered by many to be now functioning as utilities) were monetizing consumer information using methodologies not well understood by consumers despite privacy disclosures, or allegedly being gathered in violation of contractual agreements between parties.

In response to these concerns, in late 2017, privacy advocates commenced qualifying a ballot initiative to adopt consumer privacy protections that business interests believed would have created burdensome privacy requirements, while also making subsequent amendment of any privacy rules adopted via the ballot initiative process extremely difficult to achieve.[5]

Because a legislative alternative had to be adopted before the above-referenced privacy ballot initiative was certified, opponents of the ballot initiative hurriedly negotiated a legislative bill (*i.e.*, A.B. 375) that ultimately was agreed to by privacy stakeholders. After the CCPA was adopted by the California Legislature and signed by the Governor, the ballot initiative was withdrawn.

As noted above, because of the deadline to avoid placing a privacy initiative on the ballot for the November 2018 elections, S.B. 1121 was employed as a legislative vehicle to correct many of the drafting flaws in A.B. 375. Further, several industry groups undertook an intensive lobbying effort to: (a) clarify the scope of certain exemptions from coverage; (b) extend the date from which the California Attorney General would be required to issue implementing regulations; and (c) delay the date from which the Attorney General could commence enforcement actions.

The result of these two legislative enactments adds a new Title 1.18.5 to the California Civil Code, whose coverage provisions include not only internet-based companies such as social media sites but practically all businesses that operate in today's electronic environment using websites and other electronic means to capture consumer data obtained from California consumers.[6] Since its adoption in late July, U.S. and international businesses located outside of California—but regularly interacting with California residents—have begun to realize that the CCPA may likely impact their operations with California residents despite not maintaining a physical presence in California.

B. Consumer's Privacy Rights Under the CCPA

The CCPA establishes several privacy rights for California consumers (*i.e.*, California residents):

- The right to know what personal information is being collected;
- The right to know whether personal information is sold or disclosed and to whom;
- The right to say "no" to the sale of personal information;
- The right to access personal information; and
- The right to equal service and price, even if any privacy rights created by the CCPA are exercised.[7]

These privacy rights are implemented by the provisions of the CCPA, and are summarized as follows:

The Right to Know What Personal Information Is Being Collected—Section 1798.100 of the CCPA allows a "consumer" to require a covered "business" to disclose to the consumer the categories and specific pieces of "personal information" that the business collects, maintains, sells or transfers.

The Right to Know Whether Personal Information Is Being Sold or Disclosed and to Whom—Section 1798.110 of the CCPA requires that, when responding to a "verifiable consumer request,"[8] a covered business provide the following: (i) the categories of personal information it has collected; (ii) the categories of sources from which the personal information is collected; (iii) the business or commercial purpose for collecting or selling personal information; (iv) the categories of third parties with whom the business shares personal information; and (v) *specific items of personal information the covered business has collected about that consumer*.[9]

The Right to Prohibit the Sale of Personal Information and to Delete Information—Sections 1798.105 and 1798.120 of the CCPA create rights similar in kind to the EU's GDPR to direct a covered business to cease selling personal information (*i.e.*, the ability to "opt-out") and to delete personal information in the possession of the business and its service providers.[10] (The specific mandate to order a covered business holding personal information to delete the personal information is a radical departure from current U.S. privacy norms, and has been described in the EU as the "right to be forgotten.")[11] Certain exceptions to this right are included in the CCPA.

The Right to Non-Discrimination in Access, Equal Service and Price—Section 1798.125 of the CCPA contains antidiscrimination provisions that prevent a covered business from discriminating against a consumer who exercises his/her privacy rights under the CCPA. These provisions prohibit a covered business from: (a) refusing to conduct business with the consumer; (b) charging different prices or imposing penalties; or (c) providing a different level of products or services. However, a covered business may offer a different price, rate, level of service or quality of product of service if the differences are "related to the value provided to the consumer by the consumer's data."[12]

C. Coverage and Definitions

There are three principal defined terms that are used to establish possible coverage under the CCPA (subject to exceptions and clarifications contained throughout the CCPA): (a) the term "consumer"; (b) the term "business"; and (c) the term "personal

information." For purposes of an inquiry by a business whether the CCPA might apply, the following analysis must be undertaken: If a covered business collects personal information of a consumer, the business should determine whether it must comply with the CCPA or whether an exception or partial exception applies.

A consumer is a natural person who is a California *resident* however the individual is identified, including a unique identifier.[13] It includes household information pertaining to the consumer, and hence can relate to areas such as utility bills for a family.[14]

A business is a sole proprietorship or corporate entity of any type operating for a profit for its owners (including affiliated entities based upon a 50% ownership or control factor)[15] that: (i) collects consumers' personal information, whether alone or jointly with others; (ii) does business in the State of California,[16] and (iii) satisfies one or more of the following thresholds:

- The business has annual gross revenues in excess of $25,000,000;[17]
- Alone or in combination with others, the business annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices;[18] or
- The business derives 50 percent or more of its annual revenues from selling consumers' personal information.[19]

Finally, the concept of personal information is defined in an extraordinarily broad manner, and means "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."[20] For purposes of clarity, the CCPA includes a list of non-inclusive examples of what constitutes personal information.[21]

D. Compliance Procedures Required by Covered Businesses

To implement the new consumer privacy rights, the CCPA imposes several complex compliance and implementation requirements on covered businesses, and include:

Modification of Disclosures and Websites—Sections 1798.120(b) and 1798.135(a) of the CCPA require that informational disclosures be provided to consumers, including the functionality of websites to allow for the exercise of a consumer's privacy rights. Among other things, businesses will need to revise and regularly update online privacy policies and/or California-specific consumers' privacy rights to include the CCPA's consumer rights.[22]

Delivery of Information Requested by a Consumer—Within 45 days of the receipt of a verifiable consumer request from a consumer, a covered business will be required to disclose and deliver the requested information, free of charge to the consumer.[23] Businesses will be obliged to deliver the requested personal information twice a year (and impliedly may charge a fee if a request is made more than twice within that time frame).[24]

Training and Creation of a Response Team—In order to accomplish the foregoing, a covered business will have to train staff to receive verifiable consumer requests, including accessing compliance systems, retrieving information and complying with any directives made by a consumer.

Systems Design—While beyond the scope of this Alert, an implementation program might include the following components, many of which are essential elements of robust information governance policies and procedures: (a) mapping current data collection processes, data repositories and transfer protocols; (b) updating privacy policies; (c) developing and adopting policies, procedures and technologies to comply with the CCPA's covered business obligations; (d) testing and verification; (e) training and monitoring; and (f) modifying contractual arrangements with affiliates, vendors and third parties.

E. Effective Date of the CCPA and Delayed Enforcement

As a result of a strong objection from the California Attorney General to a provision in A.B. 375 that would have required the Attorney General to issue implementing and interpretive regulations by January 1, 2020—which the Attorney deemed to be practically impossible—a somewhat complicated set of compliance and effective dates were adopted by S.B. 1121.

Although the technical effective date of the CCPA remains January 1, 2020, because the Attorney General was given until July 1, 2020, to adopt regulations implementing the CCPA, no enforcement actions may be taken by the Attorney General until the earlier of six months after final regulations are adopted or July 1, 2020.[25]

F. Exemptions for Certain Business Data Collection and Data Transfer Activities

The CCPA contains numerous exemptions and partial exemptions of data use and functionality that will require close scrutiny by covered businesses. Each exemption is defined by the CCPA (and in many cases, was micro-managed in the legislative drafting process), and may assist (or hinder) a business in retaining the data or limiting its use on a go-forward basis if a consumer directs the business to cease using the data or to delete the same. Several of these categories include: (i) data used for purposes of a transaction with a consumer; (ii) sanitized data in a form not useable to identify a consumer; (iii) data used for public or peer-reviewed, historical or statistical research; (iv) publicly available personal information; (v) data used to comply with a consumer's data inquiry and instructions; (vi) data used for security purposes; and (vii) data used for free speech purposes.[26]

In addition, Section 1798.145 of the CCPA clarifies that the obligations imposed by the CCPA on a covered business do not restrict the ability of the business to: (1) comply with state or federal laws; (2) respond to civil, criminal and administrative actions, investigations and proceedings; (3) use "deidentified" consumer data (which can be collected, used and sold to third parties); and (4) collect data "if every aspect of the commercial conduct takes place wholly outside of California."[27]

For health care providers and banking institutions, S.B. 1121 clarified that the CCPA does not apply to health care information subject to HIPPA and personal information that is subject to Title V of the Gramm-Leach-Bliley Act ("GLBA"), as well as corresponding California statutes.[28] Further, the CCPA does not apply to the use of personal information obtained from or transferred to a credit reporting agency pursuant to the Fair Credit Reporting Act.[29]

G. Enforcement by the California Attorney General and Private Parties

For actions commenced by the Attorney General, Section 1798.155 of the CCPA allows imposition of penalties for intentional violations of any provision of the CCPA of up to $7,500 per violation, or $2,500 for unintentional violations if a business fails to cure unintentional violations within 30 days of notice of alleged non-compliance.[30]

For enforcement actions brought by private plaintiffs for data theft or data security breaches, Section 1798.150 of the CCPA allows statutory damages from $100 to $750 per incident (or actual damages, whichever is greater).[31] While a notice must be provided to a covered business providing a covered business the opportunity to cure the alleged violation, S.B. 1121 removed the authority of the Attorney General to intervene in a case brought by a private party.

H. Interpretative and Rule-Making Authority Given to the Attorney General

Perhaps in light of the complexity of the CCPA (and the haste in which it was drafted and adopted), Section 1798.155 of the CCPA specifically authorizes any business or third party to request guidance from the California Attorney General "on how to comply with" the CCPA. Further, Section 1789.185 directs the California Attorney General to issue regulations clarifying the requirements of the CCPA, as well as updating the nomenclature as technology advances beyond the scope of the technology in existence as of the date that the CCPA was adopted. As noted above, the Attorney General now has until July 1, 2020 to issue implementing regulations.[32]

I. Impact of S.B. 1121 on the CCPA

Although the adoption of S.B. 1121 was helpful in correcting obvious drafting errors, S.B. 1121 did not alter the expanded scope of privacy rights as originally envisioned by A.B. 375. Compliance will be burdensome and complicated—it is a virtual certainty that in the coming year industry groups will lobby the California Legislature for expanded flexibility and exemptions from coverage.

Besides extending the effective date of the CCPA, S.B. 1121 modified the health care exemption as set forth in Section 1798.145(c), as well as the exemption for financial institutions as set forth in Section 1798.145(e).

However, it is important to note that the exemptions do not technically exempt health care in regard to companies or financial institutions, but rather, personal information that is subject to existing federal and California laws and regulations. This means, for

example, that a financial intermediary would be subject to the obligations under Title V of the Gramm-Leach-Bliley Act and the California Financial Information Privacy Act in regards to the capture, sale or transfer of consumer data. However, if data is transferred, it is not clear whether the business receiving the personal information is entitled to rely upon these partial exemptions.

Importantly, the exemption for financial institutions does not exempt a financial institution from a private party lawsuit or class action for a data breach that is authorized by Section 1798.150.[33]

3. Observations and Recommendations

We note the following:

First, while the California Legislature will convene between now and the effective date of the legislation—and is expected to provide additional clarification on several confusing and sometimes internally contradictory provisions—few industry participants anticipate significant substantive changes to the increased privacy protections contained in the CCPA, due to the fact that there may remain an overhanging threat by privacy adherents to restart the ballot referendum that was abandoned as a result the compromise that has become the CCPA.

Second, the scope of the CCPA potentially encompasses all retail and commercial activity that includes the collection of data relating to a resident of California and retained, sold or transferred by a covered business. At the earliest possible date, businesses, including non-California businesses, must immediately commence the process of evaluating coverage under the CCPA, as well as designing and implementing an effective compliance program.

Third, because of the compromise nature of the provisions of the CCPA, data breaches may immediately result in the filing of private party litigation demanding statutory damages from the business whose data was the subject of the breach. Because the only defense to statutory damages is a showing that the business maintained adequate security measures, security policies and procedures will have to be constantly updated and verified.

Finally, the adoption of the CCPA has created a call for a national policy on privacy that would preempt state laws such as the CCPA. Considering that the GDPR required several years to negotiate (and several additional years to implement), adopting a national privacy standard may at best be a long term strategy. (Whether a national privacy policy ultimately resembles the new EU privacy protections of the GDPR, which are already experiencing significant growing pains, remains to be seen.) In any event, while a national privacy law is now under active consideration, preemption of state laws favored by businesses may be difficult due to the extremely narrow GOP majority. This might mean, for example, the adoption of a national privacy standard that reflects some or all of the provisions of the CCPA or the EU's GDPR.

* * *

This Alert is intended to be a high-level summary of several significant provisions of the CCPA, and is not intended to be a comprehensive recitation of all of the CCPA's requirements applicable to individual industries and businesses. Our Cybersecurity, Privacy, and Social Media Practice Group will be closely following developments in the following months, and we would welcome discussion of questions and comments from clients and friends of the firm.

[1] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.
[2] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.
[3] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB1121.

[4] The CCPA is an extension (or elaboration) on a Californian's constitutional right to privacy, as set forth at Article 1, Section 1 of the California Constitution.
[5] See https://oag.ca.gov/system/files/initiatives/pdfs/17-0027%20%28Consumer%20Privacy%29_1.pdf.
[6] The CCPA is set forth at Sections 1798.100 through 1798.198 of the California Civil Code.
[7] Section 2 of A.B 375.
[8] Section 1798.140(y) of the CCPA.
[9] Section 1798.110 of the CCPA. It appears that a business collecting personal information that is sold or transferred to a third party, in the absence of a contractual right, may not be able to restrict the use of any data transferred to the receiving party.
[10] While adult consumers must opt-out of the sale of their personal information, a covered business must obtain the affirmative authorization for the sale of personal information for minors under the age of sixteen. Section 1798.120(d) of the CCPA.
[11] Section 1798.120 of the CCPA, which references the definition set forth at Section 17014 of Title 18 of the California Code of Regulations.
[12] Section 1798.125(b)(1) of the CCPA also authorizes a covered business to provide financial incentives, including payments to a consumer, for the collection, sale or deletion of personal information.
[13] Section 1798.140(g) of the CCPA.
[14] Importantly, unlike virtually all "consumer" protection statutes, the use of the term "consumer" should be viewed as data information pertaining to a resident of California that may also include non-consumer purposes such as a resident's business operations that can be associated to an individual. (Whether this definitional approach includes individuals operating as a sole proprietorship or in a broader context as an employee of a corporate entity is unclear.)

[15] Section 1798.140(c)(2) of the CPPA.

[16] California takes a very expansive view of the concept of what constitutes "doing business" in California, and merely engaging in an internet transaction with a California resident is clearly intended to include non-California businesses within coverage of the

CCPA.

[17] Section 1798.140(c)(1)(A) of the CCPA. It is unclear whether this threshold is to be computed on a global basis or solely in regard to business associated with California residents.

[18] Section 1798.140(c)(1)(B) of the CCPA. It should be noted that even modestly successful websites may exceed this threshold. (Further, if a business is hosted on another website through connectivity or a hosting arrangement the transmission of data through a sharing arrangement may implicate coverage under the CCPA.)

[19] Section 1798.140(c)(1)(C) of the CCPA.
[20] Section 1798.140(o)(1) of the CCPA.
[21] Sections 1798.140(o)(1)(A) through (o)(1)(K) of the CCPA. The non-inclusive list includes data items as: (a) name, address, unique personal identifiers, social security number, driver's license, passport number, biometric information, etc.; (b) categories of personal information specifically identified under California law, including protected classifications; (c) commercial or consumer consuming histories or tendencies; (d) internet usage and browsing history; (e) employment and educational history; and (f) inferences drawn from any of the personal information collected to create a profile about a consumer. Importantly, S.B. 1121 amended the definition of "personal information" to make clear that identifiers such as IP addresses, geolocation data, or purchasing history are "personal information" *only if* they can be "reasonably linked, directly or indirectly, with a particular consumer or household." [22] The CCPA imposes heightened obligations on businesses that sell consumers' personal information. For example, covered businesses will be required to provide a conspicuous link, titled "Do Not Sell My Personal Information," on their Internet homepages and in their online privacy policy, which consumers can use to opt-out of the sale of their information. Many companies that specialize in big data, however, do not actually sell consumers' personal information, meaning they arguably would not be subject to these heightened requirements. (Google, for example, has advertisers describe their target market to Google, at which point Google uses its data to "place" advertisements accordingly. The same is true of Facebook.)
[23] Section 1798.130(a)(2) of the CCPA.
[24] Businesses may extend the deadline to comply with a consumer's request by 90 days for complex or voluminous requests.
[25] Because regulations issued by the Attorney General will likely impact violations of the CCPA that would give rise to a private cause of action, private party civil damage actions would appear to be subject to this enforcement delay as well.
[26] Sections 1798.105(d) and 1798.140(o)(2) of the CCPA.
[27] Section 1798.145(a) of the CCPA.
[28] These two significant exemptions apply to personal information that is subject to these alternative privacy requirements, but not the entities themselves. This may mean, for example, that industry groups such as health care companies and financial intermediaries may be required to separate data bases that are subject to HIPPA or Title V of GLBA from data bases that are subject to the CCPA.

[29] These exemptions were clarified by S.B. 1121 and are discussed below.
[30] The CCPA creates a new "Consumer Privacy Fund" to fund enforcement, with the proceeds from settlement and the collection of penalties being required to be deposited into that fund.
[31] While beyond the scope of this Alert, it should be noted that it is unclear whether measurement of damages would be based upon a single data breach or the number of data breaches measured (and multiplied by) each affected consumer. (If the latter interpretation is correct, this multiplier effect significantly increases the liability for the failure to maintain adequate security for a consumer's personal information.)
[32] Due to the highly technical nature of data capture, use and transfer, the California Attorney General may face a rule-making process that will strain governmental expertise.
[33] For purposes of liability for a data security breach brought by a private party, Section 1798.150(a)(1) adopts a narrower definition of "personal information," which is set forth at Section 1798.81.5 of the California Civil Code.