ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

JULY 3, 2018

Landmark New Privacy Law in California to Challenge Businesses Nationwide

by David Keating and David Caplan

On June 28, 2018, Gov. Jerry Brown signed the landmark California Consumer Privacy Act of 2018 (CCPA).[1] The CCPA was swiftly devised and passed as part of a deal to avoid a similarly named ballot initiative from being added to the November 2018 ballot by an organization called Californians for Consumer Privacy.

The CCPA is a sweeping new law that establishes an array of new rights for California residents regarding the collection, use, and disclosure of personal information. Effective January 1, 2020[2], businesses in and outside of California that fall under the law will need to develop policies, procedures, and infrastructure to come into compliance. Because the CCPA was rushed through the legislature to meet the deadline imposed by the backers of the ballot initiative, we anticipate it will be subject to one or more amendments prior to 2020. The CCPA also authorizes the state attorney general to develop regulations "to further the purposes of" the statute.[3] Accordingly, businesses falling under the CCPA should also anticipate some changes to the law before it becomes effective.

The following provides an overview of the new law and concludes with key initial takeaways for business.

Covered Businesses

The CCPA defines "business" as a for-profit legal entity doing business in California that collects personal information of California residents, or on whose behalf the personal information is collected, and that determines the purpose and means of processing the personal information. A business must meet one of the following thresholds: (a) annual gross revenues in excess of $25 million; (b) annually buys, receives, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more California residents, households, or devices; (c) or derives 50 percent or more of its annual revenues from

---

1 CALIFORNIA CONSUMER PRIVACY ACT, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST).

2 § 1798.198(a). All citations to the CCPA are to Section 3, Title 1.81.5 of the CCPA, added to Part 4 of Division 3 of the California Civil Code.

3 § 1798.185(a)(1)-(2), (4), (7) .

selling residents' personal information. The term business also includes any entity that controls or is controlled by a business meeting one of the above thresholds and that shares common branding with the same.[4]

Certain businesses are out of scope by virtue of being covered by certain other state or federal privacy laws. For example, businesses in the healthcare industry are not subject to the CCPA to the extent the business collects protected health information under the California Confidentiality of Medical Information Act or the Health Insurance Portability and Accountability Act.[5] The CCPA does not apply to the sale of personal information to or from a consumer reporting agency in connection with a consumer report, to the extent the use of that information is limited by the federal Fair Credit Reporting Act.[6] The CCPA also does not apply to the extent it conflicts with the Gramm-Leach-Bliley Act and its implementing regulations.[7]

Personal Information under the CCPA

The CCPA is not limited to information about "consumers," despite the title of the statute. Instead, the law applies to personal information about all California residents, including employees, customers, vendors, and contractors.

The term "personal information" incorporates the usual data types but expands the scope beyond the meaning typically associated with that term in federal and state law. Under the CCPA, personal information includes a full buffet of data types, including probabilistic identifiers that can be used to identify a particular individual or device, characteristics of protected classifications under California or federal law, commercial information, such as records of personal property, products or services purchased, obtained, or *considered*, or other purchasing or consuming histories or tendencies, biometric information, internet or other electronic network activity information (e.g., browsing and search history, and information regarding an individual's interaction with a website, application, or advertisement), geolocation data, audio, electronic, visual, thermal, olfactory or similar information, professional or employment-related information, education information, and inferences drawn from any of the foregoing to create profiles reflecting, for example, the individual's preferences, characteristics, and psychological trends.[8]

Going beyond the individual resident, the term also includes information that could reasonably be linked, directly or indirectly, with a particular *household*.[9] Moreover, the definition of unique identifier includes a persistent identifier that can be used to recognize a *family*, or a device that is linked to a family.[10]

---

4 § 1798.140(c).

5 § 1798.145(c).

6 § 1798.145(d).

7 § 1798.145(e).

8 *See* § 1798.140(o)(1) for "personal information" generally; *see* § 1798.140(x) for "unique identifier" (referring to probabilistic identifiers).

9 § 1798.140(o)(1).

10 § 1798.140(x).

The CCPA Expands Californians' Personal Information Rights

The CCPA represents a significant expansion of privacy regulation in the United States. The CCPA sets forth a statutory framework that: 1) gives California residents the right to know what categories of personal information a business has collected about them; 2) gives California residents the right to know whether a business has sold or disclosed their personal information and to whom; 3) requires businesses to stop selling a Californian's personal information upon request; 4) gives California residents the right to access their personal information; 5) prevents businesses from denying equal service and price based on the exercise of the above rights; and 6) establishes a private right of action.

Right to Access

Moving significantly closer to imposing General Data Protection Regulation (GDPR)- style requirements on businesses that collect personal information of California residents, the statute establishes a new right of access, which requires businesses to disclose on request the categories and specific pieces of personal information the business has collected relating to a requesting resident.[11] If the response is in electronic format, then the information must be in a portable format, echoing the GDPR's new right to data portability.[12] Businesses must comply with these requests up to two times in a 12-month period.[13]

Right to Delete

The CCPA provides a right to request that a business delete any personal information about a California resident that the business has collected from the individual.[14] A business that receives a verifiable request from a California resident to delete their personal information must delete the individual's personal information from its records and direct any service providers to do the same.[15] This right is subject to a number of exceptions, including, for example, completing a transaction with the individual, detecting security incidents, complying with legal obligations, or use for other internal purposes that align with the expectations of the individual based on the applicable relationship with the business.[16] There is no clear exception for such common business practices as data held in back-up or disaster recovery storage, however, which will make compliance more complicated.

---

11 § 1798.100(d).

12 *Id.*

13 *Id.*

14 § 1798.105(a). The California "Eraser" law already establishes a limited right to be forgotten for minors. Cal. Bus. & Prof. Code § 22581.

15 § 1798.105(c).

16 § 1798.105(d)(1)-(2), (7)-(8).

Right to Request Information

The CCPA provides the right for a California resident to request information about the categories and specific pieces of personal information that the business has collected.[17] The information businesses are required to disclose includes:

- The categories of personal information it has collected about that individual.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting or selling personal information.
- The categories of third parties with which the business shares personal information.
- The specific pieces of personal information it has collected about that individual.[18]

A California resident can also request information from a business that sells personal information or that discloses the information for a business purpose, including:

- The categories of personal information that the business sold about the individual.
- The categories of personal information that the business disclosed about the individual for a "business purpose,"[19] which are set out in an exclusive list of use cases focused on use for internal operational purposes related to the original purpose for which the business collected the information or other compatible purposes.[20]

Expanded Website and Privacy Notice Requirements

The new act requires businesses to expand existing disclosures in their website privacy notices or other California-specific descriptions of privacy rights to include a description of an individual's rights under the CCPA and the information required to be disclosed in response to individual requests for information, including the categories of personal information collected, sold or disclosed for a business purpose as defined in the statute.[21] This information must be updated at least every 12 months.[22]

"Do Not Sell My Personal Information"

The CCPA creates a right for a California resident to direct a business to stop selling his or her personal information to third parties[23] – which was the cornerstone of the original ballot initiative. Notably, the CCPA has an expansive definition of "sell," which includes releasing, disclosing, making available, and transferring

---

17 § 1798.110(a).

18 § 1798.110(a).

19 § 1798.115(a)(2)-(3).

20 § 1798.140(d).

21 § 1798.130(a)(5)(A)-(C).

22 § 1798.130(a)(5).

23 § 1798.120(a).

an individual's personal information to a third party for monetary or other valuable consideration.[24] As drafted, this captures many common practices such as sharing information with digital commerce fraud detection providers for use to improve those entities' threat databases.

The CCPA requires that businesses notify individuals that their information may be sold and that they have the right to opt out.[25] While this section generally follows an opt-out regime, it requires opt-in consent from minors between the ages of 13 and 16 or from parents in the case of children under 13.[26]

Websites of businesses that sell personal information are required to post a link on their homepage titled "Do Not Sell My Personal Information," which must link to a webpage that allows an individual to opt-out.[27]

Right to Equal Service

The CCPA prohibits a business from discriminating against a California resident because the individual exercised any of his or her rights under the CCPA.[28] A business cannot deny goods or services to the individual, charge different prices or rates for goods or services, impose penalties, provide a different level or quality of goods or services, or suggest any of the foregoing.[29] That said, a business may charge a different price or provide a different level or quality of goods or services if that difference is reasonably related to the value provided to the individual by the individual's data.[30]

If a business enters an individual into such a financial incentive program, it must obtain prior opt-in consent (revocable at any time) from the individual that clearly describes the material terms of program.[31]

Enforcement

The CCPA does not provide the same broad private right of action as the ballot measure it replaced, which had essentially deemed any violation of the act an injury in fact. Instead, the CCPA's private right of action focuses on holding businesses accountable directly to California residents for security breaches resulting from a business's failure to implement and maintain reasonable security measures.[32] An individual can recover damages from $100 to $750 per individual per incident or actual damages, whichever is greater.[33] There is some uncertainty regarding the scope of this right to sue in the final approved version of the statute,

---

24 § 1798.140(t)(1).

25 § 1798.120(b).

26 § 1798.120(d).

27 § 1798.135(a)(1).

28 § 1798.125(a)(1).

29 § 1798.125(a)(1)(A)-(D).

30 § 1798.125(a)(2).

31 § 1798.125(b)(1)-(3).

32 § 1798.150(a)(1).

33 § 1798.150(a)(1)(A).

however, as the threshold extends beyond the traditional definition of a security breach. In addition, the law in several places suggests individuals can bring a claim for violations of "this title." There is some risk, as a result, that individuals may have a right to bring a claim for violations of the statute more broadly.

A California resident wishing to file an action under the CCPA must first follow certain procedures. Prior to initiating any action against a business for statutory damages, the consumer must notify the business in question and allow 30 days to cure the noticed violation.[34] Individuals must also notify the state attorney general and follow certain procedures allowing the attorney general to prosecute the action.[35] The attorney general can pursue enforcement of any violations of the statutory provisions on its own, and businesses may be liable for up to $7,500 per violation in the case of intentional conduct.[36]

Key Initial Takeaways

We recommend businesses take time in the next several weeks to evaluate the new California law carefully and assess the potential impact to the business. As initial takeaways, businesses should consider the following:

- Review existing privacy disclosures to evaluate potential updates mandated by the CCPA.
- Commence planning to implement the "do not sell" requirement, including cataloguing data sales and reviewing vendor agreements for other types of data sharing that will amount to a sale under the expanded definition in the statute.
- Initial planning for an inventory of data concerning California employees, customers, contractors, mobile app users, website visitors, and other residents to start feasibility planning for fulfillment of access, deletion, and do not sell requests.
- Update vendor privacy language to implement flow-down terms for the new California privacy rights.
- Identify key vendor contracts and evaluate for compliance with California standards.

---

34 § 1798.150(b)(1).

35 § 1798.150(b)(2)-(3).

36 § 1798.155(b).

You can subscribe to future *Privacy & Data Security* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Helen Christakos
650.838.2091
helen.christakos@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Jan Dhont
+32 2 550 3709
jan.dhont@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM