September 18, 2019

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.com
An ALM Publication

Taking Stock of CCPA Amendments and Privacy Measures Passed by the California Legislature This Session That Now Await the Governor's Consideration

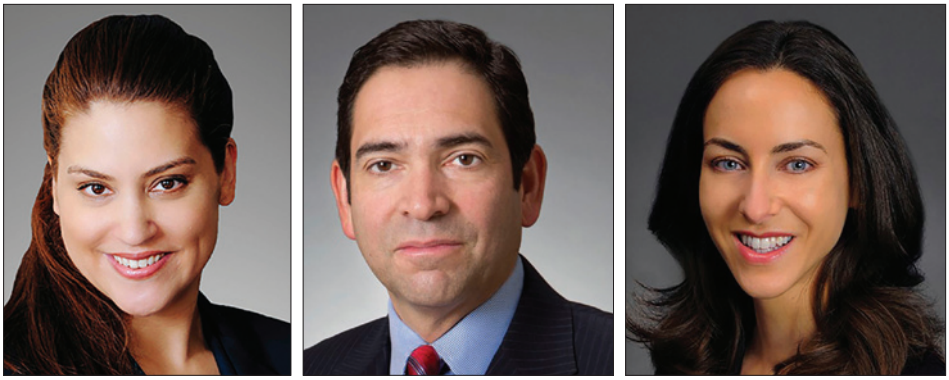
By Natasha G. Kohne, Dario J. Frommer and Diana E. Schaffner

Overview Points

- Sept. 13, 2019 was the deadline for the California Legislature to pass bills in order for the bills to be considered by the Governor this year.
- Several bills proposing amendments to the California Consumer Privacy Act (CCPA) and other key privacy and data protection issues passed and now await consideration by the Governor. Oct. 13, 2019 is the last day for the Governor to sign any bill sent to him this session.
- Below, we provide a practical summary of CCPA amendments and other privacy and data protection measures that passed this session. We also provide highlights of proposals that did not pass this session, but that garnered material support—e.g., proposals related to customer loyalty programs and the health and life sciences sectors.

Introduction

The California Legislature just finished the first year of its current two-year session. Privacy and data protection issues were front and center in Sacramento during the session, and the Legislature passed a number of measures including several proposed amendments to the California Consumer Privacy Act (CCPA). The Governor now has until Oct. 13, 2019 to sign the measures passed this session into law. The Legislature will reconvene on Jan. 6, 2020.



(l-r) Natasha G. Kohne, Dario J. Frommer, and Diana E. Schaffner, with Akin Gump Strauss Hauer & Feld.

As many are now aware, the California Legislature passed the CCPA in a little over a week in order to avoid a related ballot measure. Lawmakers, industry advocates and privacy activists all understood that certain sections of the law may need to be amended later to address issues they were not able to work out during the brief initial drafting period. The Legislature adopted the first amendments to the CCPA in September 2018, just months after the law passed. The initial amendments left many critical issues unresolved.

This session, industry advocates and privacy activists alike pushed for further amendments to fix issues they saw in the current CCPA (e.g., the need to exclude employee information). Lawmakers also introduced a flurry of additional privacy and data protection measures, some related in part to issues raised in the CCPA (e.g., expansion of the definition of "personal information" in California's data breach law). Given California's historic role as a trendsetter among the states when it comes to privacy and data protection issues, businesses should be prepared for the possibility that other states may take up similar measures in the coming years.

Key CCPA amendments were passed in AB25, AB874, AB1355 and AB1564**,** and other privacy and data protection measures were passed in AB1130 and AB1202. We discuss these measures in detail below. If the Governor signs the CCPA amendments and other privacy and data protection measures passed by the Legislature on or before October 13, the measures would take effect on Jan. 1, 2020 (unless otherwise noted).

Several important CCPA amendments and privacy and data protection proposals failed this session. Some of the proposals failed before they were included in a numbered bill. Many of these proposals are either already slated to be or will likely

be considered next session. Below, we also provide an overview of several of the proposals that garnered material support but did not pass.

Amendments to the CCPA That Passed This Session

The following section provides high-level descriptions of the key CCPA amendments that passed this session. We also provide the related statutory language where helpful. Language provided in blue was added to the CCPA, while language in red was struck from the law.

Employee personal information, including related benefits plan and emergency contact information, is exempted from the CCPA (aside from two provisions) until Jan. 1, 2021. (AB 25)—Exempts from certain provisions of the CCPA personal information collected by a business about a consumer (i.e., a California resident) when that consumer is acting as an employee of, owner of, director of, medical staff member of or contractor of (collectively, "employee") that business. Only personal information collected and used solely within the context of the consumer's current or former role as an employee of that business is covered by the new exemption. Employee benefits plans and employee emergency contact information are also covered by the new exemption. The exemption does not apply to §§1798.100(b) (general notice provisions) or 1798.150 (private right of action (PRA)). Importantly, this exemption is temporary; it expires on Jan. 1, 2021.

Section 1798.145 is amended to add the following:

(g)(1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 150.

(4) This subdivision shall become inoperative on January 1, 2021.

Employee personal information collected in a business-to-business (B2B) context is exempted from certain CCPA provisions until Jan. 1, 2021. (AB 1355)—Exempts from certain sections of the CCPA personal information a business collects about a consumer through B2B communications (written or verbal) or transactions where the consumer is acting as an employee of, owner of, director of, medical staff member of or contractor (collectively, "employee") of a company, partnership, sole proprietorship, nonprofit or government agency. Specifically, B2B information is exempt from §§1798.100 (general obligations), 1798.105 (deletion obligations), 1798.110 (consumers' rights to request information from businesses that collect information), 1798.115 (consumers' rights to request information from businesses that sell or disclose information for a business purpose), 1798.130 (businesses' general compliance obligations, e.g., methods for submitting requests) and 1798.135 (businesses' obligations to comply with the opt-out requirement). Information must be collected and used solely within the context of the business conducting B2B due diligence, or providing or receiving a B2B product.

The exemption does not apply to §§1798.120 (opt-out rights), 1798.125 (nondiscrimination), and §§1798.140-1798.199 (definitions, enforcement, exemptions, etc.). This means that an employee of another company still has the right to, for example, opt-out of the sale of his or her personal information, to bring a PRA following a data breach, and to not be discriminated against for exercising any rights under the CCPA. Like the employee information exemption, the B2B exemption is temporary; it expires on Jan. 1, 2021.

Section 1798.145 is amended to add the following:

(l)(1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2021.

Changed the definition of "personal information" to mean information that is, among other things, "reasonably capable of being reidentified." (AB 874)—Revises the definition of "personal information" in the CCPA to add "reasonably," as follows: "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Industry advocates pushed for this change in an effort to bring the standard more in line with guidance from the Federal Trade Commission.

Deidentified information and aggregate information are excluded from the definition of "personal information." (AB 1355)—Clarifies that the definition of "personal information" in the CCPA does not include consumer information that is deidentified information or aggregate information.

Section 1798.140(o) is amended to revise the error in the original CCPA that provided that "[p]ublicly available" does not include consumer information that is deidentified or aggregate in §1798.140(o)(2) and to, instead, add the following:

~~(a) "Publicly available" does not include consumer information that is deidentified or aggregate consumer information."~~

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information."

Removed the restriction that information could only be "publicly available information" if it was a government record used in the same manner for which the record was originally maintained or made available. (AB 1355)—Revises the definition of "publicly available information" in the CCPA to mean any information lawfully made available from government records. Broadens the usefulness of the exception by eliminating the requirement to use the records only for the same purpose for which they were originally maintained or made available.

Section 1798.140(o) is amended to read:

~~(a)~~ (2) "Personal information" does not include publicly available information. For ~~these purposes,~~ purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government ~~records, if any conditions associated with such information.~~ records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. ~~Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer information that is deidentified or aggregate consumer information.~~

Expanded the existing exemption for information covered by the Fair Credit Reporting Act (FCRA) to cover information obtained in more ways than through sales alone. (AB 1355)—Expands the existing exemption in the CCPA for activity, collection, maintenance, disclosure, sale, communication or use of personal infor-

mation bearing on consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living, so long as certain restrictions related to the FCRA are met. Applies only to activity regulated by the FCRA, and only to information being used as permitted under the FCRA. Does not apply to Section 1798.150 (PRA).

Section 1798.145(d) is amended to read:

(1) This title shall not apply to ~~the sale of personal information to or from~~ an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting ~~agency if that information is to be reported in, or used to generate, a consumer report as defined by~~ agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and ~~use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).~~ by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting

(3) This subdivision shall not apply to Section 150.

Charged the California Attorney General's Office with establishing regulations regarding how to process and verify consumer requests involving "households." (AB 1355)—Adds a provision to the section of the CCPA instructing the Attorney General (AG) to adopt regulations to "establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household in order to address obstacles to implementation and privacy concerns." Industry advocates pushed for the removal of "household" from the definition of "personal information" throughout the session and raised concerns over the potential for misuse and potential abuse of consumer requests for "household" data; for example, in the domestic violence context.

Enabled businesses to require a consumer making a request for information to provide authentication that is reasonable in light of the information sought by the consumer. (AB 1564)—Permits businesses to require consumers seeking to exercise their rights under the CCPA to request certain information to provide authentication that is reasonable in light of the personal information being sought. This seems to permit businesses to require additional authentication for more sensitive information.

Section 1798.130(a)(2) is amended to read: "The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request."

Enabled businesses to require a consumer making a request for information to receive information in response to that request through an existing account. (AB 1564)—Permits businesses to require consumers that already have accounts with the business to receive information provided in response to their requests through those accounts. Businesses are still prohibited from requiring consumers to create accounts to submit consumer requests.

Section 1798.130(a)(2) is amended to read: "If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account."

Fixed wording issue in the PRA provision to clarify that a consumer may only bring a PRA if their nonencrypted and nonredacted personal information is affected by a data breach. (AB 1355)—Revises language in the PRA provision as follows: "(a) (1) Any consumer whose nonencrypted ~~or~~ and nonredacted personal information, … is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures …" Industry advocates suggested the change was needed to make clear that personal information has to be both nonencrypted and nonredacted to provide a basis for a PRA.

Provided that businesses that operate online only and have a direct relationship with consumers may require consumer request submissions via email. (AB 1564)—Permits businesses that operate solely online and that have a direct relationship with the consumer to provide an email address only as a means for consumers to submit requests. Businesses that have more than an online-only presence must still provide consumers at least two methods to submit requests, including a toll-free telephone number.

Section 1798.130(a) is amended to read:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone ~~number, and if the business maintains an Internet Web~~

~~site, a Web site address.~~ number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

Clarified that businesses are not required to collect more information or retain information for longer than they would in the ordinary course. (AB 1355)—Expands the existing provision clarifying that businesses are not required to reidentify or relink information to say that businesses do not have to collect personal information they would not otherwise collect in the ordinary course, or retain personal information for longer than they would otherwise retain the information in the ordinary course.

Section 1798.145(i) is amended to read:

(i) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

Made various technical fixes to the nondiscrimination provision, including that what matters is the value of data to the business, not the consumer. (AB 1355)—Revises the CCPA's nondiscrimination provision to clarify that what matters is the value of the data to the business, not to the consumer—for example: "(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the ~~consumer~~ business by the consumer's data." Revises the provision further to change references to Section 1798.135 to Section 1798.130 with regard to notice required and other issues."

Exempted certain information shared between a vehicle dealer and others for the purposes of effectuating, or in anticipation of effectuating, certain repairs. (AB 1355)—Exempts certain information where that information is shared for purposes of effectuating, or in anticipation of effectuating, vehicle repair covered by vehicle warranty or recall.

Additional Non-CCPA Privacy and Data Protection Measures That Passed This Session

Multiple other privacy and data protection measures, aside from amendments to the CCPA, were also considered in Sacramento this session. Two important measures that passed this session are highlighted below. Businesses should consider the possibility that other states may take up similar measures.

Expanded the definition of "personal information" under the California data breach notification law, which, in turn, expanded the definition of "personal information" subject to the CCPA's PRA to include biometric and other data. (AB 1130)—At the urging of the California Attorney General, the Legislature expanded the definition of "personal information" under the California data breach notification law to include unique biometric data and tax identification numbers, passport numbers, military identification numbers and unique identification numbers issued on government documents. Expansion of this definition is particularly important as the CCPA's PRA provision adopts the definition of "personal information" in the California data breach notification law.

Required "data brokers" to register with the Attorney General's Office, pay certain fees, and make certain information available to the public through their registration. (AB 1202)—This measure requires entities that fall into the broad definition of "data broker" to register with the Attorney General's Office and pay certain fees. "Data broker" means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. "Data broker" does not include any of the following: (1) a consumer reporting agency, to the extent that it is covered by the FCRA; (2) a financial institution, to the extent that it is covered by the Gramm-Leach-Bliley Act and implementing regulations; and (3) an entity to the extent that it is covered by the California Insurance Information and Privacy Protection Act (IIPPA), which provides certain protections for personally identifiable information provided to an agent, broker or insurance company in order to apply for insurance or submit a claim. Companies are required to comply with the law on or before January 31 following each year in which they meet the definition of data brokers. Laws passed this session generally go into effect on Jan. 1, 2020.

Proposals That Did Not Pass/Now Two-Year Bills

A number of privacy and data protection proposals failed to pass or were held in committee. Some of these proposals may be heard again when the Legislature reconvenes in January 2020. Many of these proposals were not standalone bills; but, rather, were proposed amendments to others bills.

Proposal to revise certain provisions relevant to the health and life sciences sectors. Privacy activists and industry advocates came to an agreement regarding a number of fixes to different provisions in the CCPA impacting the health and life sciences sectors. Many of these fixes sought to harmonize the CCPA with the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 (as amended and together

with their implementing regulations, HIPAA) and other existing and long-accepted standards. The compromise included language addressing concerns relating to the lack of alignment between the CCPA deidentification standard and the longstanding HIPAA deidentification requirements, narrowness of the exception for use of personal information in clinical research, and lack of a sufficient carve-out for vendors and other HIPAA business associates already handling health information in compliance with HIPAA's extensive requirements applicable to protected health information. Despite the fact that privacy advocates and health industry stakeholders achieved extraordinary agreement on critical details, the amendments were not enacted in the final days of the Legislative session.

Proposal to exempt customer loyalty and rewards programs from the CCPA's antidiscrimination provision. (AB 846)—The bill would have added a new subsection to the CCPA exempting customer loyalty and reward programs from certain restrictions under the nondiscrimination provision. It is now a two-year bill. Privacy activists worked on revisions along the way that made the proposed amendment more difficult for businesses to use.

Proposal to revise the definition of "deidentified" to make it more practical. There were efforts to amend the definition of "deidentified" information to make the definition more workable.

Proposal to require businesses to post notices regarding their use of facial recognition technology. (AB 1281)—This is now a two year bill. This bill would have required any company to post a notice informing consumers that it used facial recognition technology at or before time of use. Author, Assemblyman Chau, has already scheduled a hearing for the fall regarding concerns with facial recognition technology.

Proposal to remove "household" from the definition of "personal information." There were efforts to remove "household" from the definition of "personal information" in light of safety concerns and practical considerations. Privacy activists opposed. The Attorney General's Office has been tasked with coming up with regulations related to the issue.

Proposal to revise certain provisions in the CCPA to address advertising issues. There were efforts to get a workable amendment related to advertising issues in light of the strict service provider/third party dichotomy set up by the CCPA.

Proposal to add exemption to the CCPA permitting businesses to share information for the limited purpose of combatting fraud and similar misconduct. There were efforts to add an exemption that would permit businesses to share information with other parties that are not service providers in order to help fight fraud and similar misconduct.

Proposal to expand the definition of "publicly available information" to information lawfully made available to the public, including materials outside of government records.—There were efforts to expand the definition of "publicly available" information beyond government records to include any information lawfully available in the public domain, including social media posts, etc.

Conclusion

We anticipate that privacy and data protection issues will remain a significant policy issue in California in the second year of the two-year Legislative session. Efforts to amend the CCPA will likely continue and we may see movement on other privacy issues. What issues will be paramount may depend on the content of the Attorney General's CCPA regulations, expected this fall, and whether those regulations clarify certain issues. We will continue to monitor these developments closely.

Natasha G. Kohne *is a partner in Akin Gump's San Francisco office and co-leader of the firm's cybersecurity, privacy and data protection practice where she advises companies on privacy- and cybersecurity-related compliance, investigations and enforcement actions. She also represents companies in U.S. and international and cross-border litigation, arbitration and investigations.*

Dario J. Frommer *is a partner in Los Angeles and a member of the firm's Public Law and Policy Practice. He provides strategic legal and political advice to many of California's most prominent companies and government agencies. He represents clients in high-stakes matters—including legislation, rulemaking, enforcement actions, procurements and investigations—before state and local government entities.*

Diana E. Schaffner *is counsel in the firm's San Francisco office, where she advises clients on privacy- and cybersecurity-related litigation, investigations and compliance matters, including with regard to the California Consumer Privacy Act and other state, federal and international statutes and regulations. In addition, Diana handles high-stakes, complex commercial litigation and business disputes involving companies in emerging technologies, financial services and retail.*