SENATE JUDICIARY COMMITTEE
Senator Hannah-Beth Jackson, Chair
2019-2020 Regular Session

AB 25 (Chau)
Version: June 28, 2019
Hearing Date: July 9, 2019
Fiscal: Yes
Urgency: No
CK

SUBJECT

California Consumer Privacy Act of 2018

DIGEST

This bill authorizes a business to require authentication of consumers, as specified, in connection with requests made pursuant to the California Consumer Privacy Act (CCPA) and allows a business to require requests to be made through an existing account. The bill exempts certain personal information collected by business employers from the scope of the CCPA.

EXECUTIVE SUMMARY

The CCPA provides consumers a number of rights with regard to businesses' use of their personal information, as defined. Businesses that collect or sell a consumer's personal information, or disclose it for a business purpose, must provide notice and certain disclosures upon request by the consumer. This includes disclosing the categories of information the business has collected or sold, the categories of sources from which the information is collected, and the specific pieces of information collected about the consumer. The CCPA also allows consumers who are 16 years of age or older to opt out of the sale of their personal information with younger consumers needing to opt in before a business can sell their information. Consumers can also request that certain personal information be deleted.

This bill exempts from the protections of the CCPA personal information collected by businesses in their role as employers. It also provides flexibility for businesses in how they can require consumers to make requests pursuant to the CCPA and allows businesses to require authentication that is reasonable in light of the nature of the personal information requested.

This bill is author-sponsored and is supported by various business associations. It is opposed by an array of labor, consumer, and privacy groups.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the CCPA, which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

2) Provides consumers the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected. A business must provide the information upon receipt of a verifiable consumer request. (Civ. Code § 1798.100(a), (c).)

3) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice, as specified. (Civ. Code § 1798.100(b).)

4) Provides consumers the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (Civ. Code § 1798.105(a).)

5) Provides consumers the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

    a) the categories of personal information it has collected about that consumer;
    b) the categories of sources from which the personal information is collected;
    c) the business or commercial purpose for collecting or selling personal information;
    d) the categories of third parties with whom the business shares personal information; and
    e) the specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110(a).)

6) Provides consumers the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer the following:

a) the categories of personal information that the business collected about the consumer;
b) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and
c) the categories of personal information that the business disclosed about the consumer for a business purpose. (Civ. Code § 1798.115(a).)

7) Provides a consumer the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. (Civ. Code § 1798.120.) It further requires a business that sells consumers' personal information to third parties to provide notice to consumers, as specified, that this information may be sold and that consumers have the "right to opt-out" of the sale. (Civ. Code § 1798.120.)

8) Requires a business to, in a form that is reasonably accessible to consumers, 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 website, a website address. (Civ. Code § 1798.130(a)(1).)

9) Requires a business to, in a form that is reasonably accessible to consumers, disclose and deliver required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's duty to disclose and deliver the information within the time limit. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request. (Civ. Code § 1798.130(a)(2).)

10) Provides that the CCPA does not apply to medical information governed by other specified privacy laws; providers of health care, as specified; information

collected as part of clinical trials; personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, or the Driver's Privacy Protection Act. (Civ. Code § 1798.145.)

This bill:

1) Authorizes a business to require authentication of a consumer that is reasonable in light of the nature of the personal information requested.

2) Authorizes a business to require a consumer to submit the consumer's verifiable request through the consumer's account, where the consumer maintains an account with the business.

3) Provides that the CCPA does not apply to 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.

4) Defines the relevant terms used therein.

COMMENTS

1. Protecting the fundamental right to privacy

Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Privacy is therefore not just a policy goal; it is a constitutional right of every Californian. However, it has been under increasing assault.

The phrase "and privacy" was added to the California Constitution as a result of Proposition 11 in 1972; it was known as the "Privacy Initiative." The arguments in favor of the amendment were written by Assemblymember Kenneth Cory and Senator George Moscone. The ballot pamphlet stated, in relevant part:

> At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian. The right of privacy . . . prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. . . . The proliferation of government and business records over which we have no control limits our ability to control our personal lives. . . . Even more dangerous is the loss of control over the accuracy of government and business records on individuals. . . . Even if the existence of this information is known, few government agencies or private businesses permit individuals to review their files and correct errors. . . . Each time we apply for a credit card or a life insurance policy, file a tax return, interview for a job[,] or get a drivers' license, a dossier is opened and an informational profile is sketched.[1]

In 1977, the Legislature reaffirmed that the right of privacy is a "personal and fundamental right" and that "all individuals have a right of privacy in information pertaining to them." (Civ. Code § 1798.1.) The Legislature further stated the following findings:

- "The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies."
- "The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."

[1] *Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 17, quoting the official ballot pamphlet for the Privacy Initiative.

- "In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."

Although written almost 50 years ago, these concerns seem strikingly prescient.

Today, the world's most valuable resource is no longer oil, but data. Companies regularly and systematically collect, analyze, share, and sell the personal information of consumers. While this data collection provides consumers various benefits, public fears about the widespread, unregulated amassing of personal information have only grown since privacy was made a part of the California Constitution. Consumers' web browsing, online purchases, and involvement in loyalty programs create a treasure trove of information on consumers. Many applications on the smartphones that most consumers carry with them throughout the day can track consumers' every movement.

2. Responding to the systematic collection of consumers' personal information

In response to growing concerns about the privacy and safety of consumers' data, proponents of the CCPA, a statewide ballot initiative, began collecting signatures in order to qualify it for the November 2018 election. The goal was to empower consumers to find out what information businesses were collecting on them and give them the choice to tell businesses to stop selling their personal information. In response to the pending initiative, which was subsequently withdrawn, AB 375 (Chau, Ch. 55, Stats. 2018) was introduced, quickly shepherded through the legislative process, and signed into law. The outcome was the CCPA, Civil Code Section 1798.100 et seq.

The CCPA grants a set of rights to consumers with regard to their personal information, including enhanced notice and disclosure rights regarding information collection and use practices, access to the information collected, the right to delete certain information, the right to restrict the sale of information, and protection from discrimination for exercising these rights.

3. Personal information of employees

Since the passage of the CCPA, representatives of business, tech, and other industry groups have called for various changes, clarifications, and carve outs from the CCPA. As described by the author, "one issue that has been raised is the need to clarify that the definition of 'consumer' does not include an employee acting within their scope as an employee." The author argues that "the CCPA could be read to apply to Californians in their capacity as employees, both to capture their employee data and to potentially capture business data of another business in the context of business-to-business interactions."

To address these concerns, the bill adds an additional exemption to the CCPA, providing that its protections and controls do not apply to personal information that is:

- collected by a business about a person in the course of the 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 person's personal information is collected and used by the business solely within the context of the 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;
- 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; and
- 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.

The bill therefore excludes from the CCPA any information an employer business collects from an employee consumer in the employment context.

In support of this provision of the bill, the author and supporters of the bill assert the scenario that employees could exploit the rights of the CCPA to have their personnel files deleted, including, for example, complaints made against them. From a policy perspective, this would certainly be a troubling prospect. It should be noted that the CCPA currently provides broad exemptions from its application to ensure that nothing prevents businesses from complying with applicable laws; civil, criminal, or administrative inquiries or investigations; or exercising or defending legal claims. (Civ. Code § 1798.145(a).)

In addition, the specific section providing consumers the right to deletion, makes clear that a business does not have to comply with a deletion request for a series of reasons, including where retaining the information is necessary in order for the business to do the following:

- to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- comply with a legal obligation; or
- otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

(Civ. Code § 1798.105.) Arguably much of the information that an employer collects on an employee consumer that should be protected from deletion is protected by these broad exceptions. Therefore, arguably, the issue of an employee requesting deletion of the employee's personnel file and associated misconduct investigations is already addressed. But, certainly a narrowly crafted provision that ensures such data cannot be deleted could provide greater clarity.

Some in support are simply looking for a broad carve out of employees. A large coalition of groups, led by the California Chamber of Commerce, writes in support that the bill is necessary otherwise employees and job applicants will be covered by the CCPA, which it argues "was not an intended outcome of the CCPA, a law designed to address the privacy of consumers." The American Staffing Association writes in support:

> ASA members place workers in temporary and contract jobs and help businesses fulfill their workforce needs. A natural component of our members' work requires them to share individuals' personal information with businesses so they may be considered for job opportunities. The CCPA's broad applicability threatens our members' business model and the staffing industry as a whole. Although the CCPA was enacted to empower consumers, it fails to cabin its effects to individuals engaged in consumer transactions. As written, the CCPA's definition of "consumer" broadly includes any California resident, no matter the context in which the resident is acting. However, the interactions between job candidates, who are looking for employment to support themselves and their families, and staffing firms, whose purpose is to put people to work, are not consumer-business transactions. Individuals do not pay staffing firms for finding and placing them in jobs, so staffing firms utilize individuals' information in the employment, rather than the consumer, context.
>
> We therefore urge you to adopt AB 25 to clarify that job applicants and employees do not constitute "consumers" under the CCPA. Otherwise, the staffing industry will face a significant compliance burden that will impede the industry's ability to place people in jobs—hurting California's workers.

However, this wholesale carve out arguably undermines the privacy rights, currently provided by the CCPA, of consumers that apply through these agencies. Consumers may wish to exercise some of their rights under the CCPA specifically in connection with such businesses. For instance, a consumer may wish to know what types of information is being collected on them and is being sold to other businesses, given the potential impact on their livelihood. Certainly built into these relationships is the consent of the consumer to have the business share their information with potential employers, but arguably that sharing should end when the consumer wishes it to, as provided for by the CCPA.

A coalition of labor, privacy, consumer, and employee rights groups argue that the CCPA explicitly intended to apply to employee consumers as indicated by the inclusion of professional and employment-related information in the definition of personal information and further stated in the preamble to AB 375, where it states that it is "almost impossible to apply for a job . . . without sharing personal information."

The coalition in opposition expresses its concerns that the exemptions in the bill go too far in eroding the rights of employee consumers and make the case for why they should be preserved:

> Workers' interest in data privacy is closely related to consumers' interest, and many of the same technology is used to monitor both. Just as retailers may use personal data to create user profiles and direct targeted advertising, employers may aggregate data in the same way. For example, when Target mined a wide variety of data to build customer profiles to predict when a customer was expecting a baby, many found it troubling.[2] Employers can, and have, used the same data mining algorithms to infer/predict worker pregnancies and other health conditions.[3] This use of data by employers does not just threaten employee privacy, but can also be used to discriminate against workers on prohibited bases.[4] For example, Amazon experimented with an artificial intelligence hiring tool, but the company was forced to scrap the project when it downgraded graduates from all-women's colleges and penalized resumes that included the word "women's," as in "women's chess club captain."[5]
>
> Workplace monitoring, in its many forms, is an increasingly common business practice. According to a 2007 survey by the American Management Association of self-reported data, 66% of employers monitor internet traffic, 48% use video surveillance, 45% monitor keystrokes, and 8% track employees' location via

---

[2] Kashmir Hill, *How Target Figured out a Teen Girl was Pregnant before her Father Did* (Feb. 16, 2012) Forbes, https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2899d2ba6668 [as of Jul. 3, 2019]. All further internet citations are current as of July 3, 2019.

[3] Valentina Zarya, *Employers Are Quietly Using Big Data to Track Employee Pregnancies* (Feb. 17, 2016) Fortune, http://fortune.com/2016/02/17/castlight-pregnancy-data/; Rachel Emma Silverman, *Bosses Tap Outside Firms to Predict Which Workers Might Get Sick* (Feb. 17, 2016) Wall Street Journal, https://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940; Ellen Sheng, *Employee privacy in the US is at Stake as Corporate Surveillance Technology Monitors Workers' Every Move* (Apr. 15, 2019) CNBC, https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html.

[4] Kim, Pauline, *Data-Driven Discrimination at Work* (April 19, 2017). William & Mary Law Review, Vol. 48, pp. 857-936 (2017); Washington University in St. Louis Legal Studies Research Paper No. 16-12-01, https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=3680&context=wmlr.

[5] Jeffrey Dastin, *Amazon scraps Secret AI Recruiting Tool that Showed Bias against Women* (October 9, 2018) Reuters, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

> GPS.[6] More recently, a 2018 survey of US/UK IT professionals found that 98 percent of U.S. and U.K. workplaces have some form of digital surveillance, such as tracking employees through sociometric badges or biometric scanners, scanning emails and social media posts, monitoring computer keystrokes, surveilling with a video camera or monitoring movement through GPS on phones.[7] That survey found that only 11 percent of workers were aware of the full extent of monitoring, and an equal percent were not aware that monitoring was taking place at all.

Indeed, the CCPA provides some transparency for employee consumers to understand the scope of this data collection, even if, as discussed above, they cannot delete it. Without these rights, the coalition argues, "workers have little opportunity to know what information is being collected about them, to correct erroneous information that might affect their opportunities at work, or to opt out of the sale of their personal data."

The coalition goes further to assert that not only should protections be rolled back for employees, but that they should be strengthened:

> While the CCPA's provisions are a necessary step in safeguarding workers' data privacy, more comprehensive steps will be necessary to fully address issues specific to the employment relationship. For example, the use of predictive hiring algorithms, which have raised significant questions about bias, must be addressed by additional legislation.[8] Further legislation should also address limits on monitoring workers to employ the least intrusive means that would achieve legitimate business goals, provide worker-specific discrimination and retaliation protections, and address the power imbalance that might compel workers to divulge private information in exchange for "financial incentives," as currently allowed by the law.
>
> We need to protect the data rights of workers and excluding them from this bill—with no plans to include them in an alternative system—would be a significant step in the wrong direction. We would be happy to work with you to discuss additional legislation to fully protect workers and strike the appropriate balance between businesses' legitimate needs for data and workers' rights to privacy and dignity in the workplace.

---

[6] The *rise of workplace spying* (July 5, 2015) The Week, https://perma.cc/NKP9-VSJZ.
[7] Chris Matyszczyk, *In a Startling New Study, Companies Admit to Spying on Employees Far More Than Employees Realize* (June 21, 2018) Inc., https://www.inc.com/chris-matyszczyk/study-shows-how-much-companies-spy-on-employees.html.
[8] Miranda Bogen and Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias* (December 2018) Upturn, https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

In response to these concerns, the author has agreed to the following amendments:

> Amendment
>
> In Section 2 of the bill, make the following amendments:
>
> Amend (g)(3) to read: "(3) This subdivision shall not apply to *subdivision (b) of Section 1798.100 or* 1798.150."
>
> Add (g)(4) to read: *"(4) This subdivision shall be inoperative on or after January 1, 2021."*

While not eliminating all of the concerns raised above regarding protections for employee consumers, these amendments ensure there are both some safeguards in place and that a more narrowly tailored response is necessary within the next year otherwise the law reverts back to its current form. The former amendment refers to Section 1798.100(b) which provides:

> A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

This language mitigates some of the concerns about employers secretly surveilling their employees. Although it would not allow employee consumers access to the specific pieces of information collected or the right to limit the sale of such information, the provision would now require employers to inform employees what types of information they are collecting on the employees and the reasons for so collecting it. This will create a layer of transparency not provided by the language of the bill in print.

These amendments will move some of the groups in opposition to the bill to a neutral position.

4. Streamlining and clarifying the request and authentication process

Currently the CCPA provides consumers with the right to request certain information from businesses that collect or sell their personal information, this includes the categories of sources from which the data was collected, the categories of personal information it has collected and sold, and the specific pieces of personal information it has collected about that consumer. (Civ. Code §§ 1798.110, 1798.115.) Consumers may also request that a business delete personal information about the consumer, which the business has collected from the consumer. (Civ. Code § 1798.105.)

In order to comply with these obligations, businesses must disclose and deliver the required information within 45 days of receiving a "verifiable consumer request," which means a request that is made by a consumer, and that the business can reasonably verify, pursuant to regulations to be adopted by the Attorney General, to be the consumer about whom the business has collected personal information. (Civ. Code § 1798.140(y).) The CCPA makes clear that a business cannot require the consumer to create an account with the business in order to make a verifiable consumer request.

The bill amends this section of the law to authorize a business to require the consumer to submit the above requests through an account with the business where the consumer already maintains such an account. This allows ease of process and provides a layer of authentication built into the request. The bill further authorizes businesses to require authentication of the consumer that is reasonable in light of the nature of the personal information requested. This provides flexibility to businesses to ensure the consumer making the request is actually the subject of the requested information. The requirement that the authentication be reasonable is crucial in order to prevent barriers to consumers exercising their rights pursuant to the CCPA. It is not the intent of this change to interfere with the requirement that businesses offer at least two methods to consumers for making their requests.

SUPPORT

Advanced Medical Technology Association
Alliance of Automobile Manufacturers
American Council of Life Insurers
American Property Casualty Insurance Association
American Staffing Association
Association of California Life & Health Insurance Companies
Association of National Advertisers
Azusa Chamber of Commerce
Brawley Chamber of Commerce
California Asian Pacific Chamber of Commerce
California Association of Realtors
California Attraction and Parks Association
California Bankers Association
California Cable & Telecommunications Association
California Grocers Association
California Hospital Association
California Land Title Association
California League of Food Producers
California Life Sciences Association
California Mortgage Bankers Association
California Restaurant Association
California Retailers Association

California Staffing Professionals
Camarillo Chamber of Commerce
Card Coalition
Carlitos Way Fresh Mexican Food
Carniceria Mi Mercadito LLC
Civil Justice Association of California
Consumer Data Industry Association
Consumer Technology Association
CTIA
El Amigazo Western Wear
El Rancho Mexican Restaurant
Email Sender & Provider Coalition
Entertainment Software Association
Greater Conejo Valley Chamber of Commerce
Insights Association
Interactive Advertising Bureau
International Franchise Association
Internet Association
Investment Company Institute
La Rosa Meat Market
Long Beach Area Chamber of Commerce
Los Angeles Area Chamber of Commerce
Murrieta/Wildomar Chamber of Commerce
National Payroll Reporting Consortium
North Orange County Chamber
Orange County Business Council
Oxnard Chamber of Commerce
Panaderia Los Arcos
Pleasanton Chamber of Commerce
Rancho Cordova Chamber of Commerce
San Gabriel Valley Economic Partnership
Santa Clarita Valley Chamber of Commerce
Santa Maria Valley Chamber
Securities Industry and Financial Markets Association
Silicon Valley Leadership Group
Simi Valley Chamber
Society for Human Resource Management
Software & Information Industry Association
Southwest California Legislative Council
TechNet
The Silicon Valley Organization
Tulare Chamber
UPS

OPPOSITION

American Civil Liberties Union of California
AI Now Institute
Access Humboldt
Annette Bernhardt, UC Berkeley Labor Center
Matthew Bodie, Callis Family Professor, Saint Louis University School of Law
California Employment Lawyers' Association
California Federation of Labor
Center for Digital Democracy
Common Sense Kids Action
Consumer Federation of America
Digital Privacy Alliance
Electronic Frontier Foundation
Equal Rights Advocates
Jobs with Justice San Francisco
Pauline Kim, Daniel Noyes Kirby Professor of Law, Washington University School of Law
Media Alliance
National Employment Law Project
North Bay Jobs with Justice
Oakland Privacy
Partnership for Working Families
Privacy Rights Clearinghouse
Purism
Restaurant Opportunities Center United
Brishen Rogers, Associate Professor of Law, Temple University
Jason Schultz, Professor, NYU School of Law
SEIU California
United for Respect
Warehouse Workers Resource Center
Working Partnerships USA

RELATED LEGISLATION

Pending Legislation:

SB 561 (Jackson, 2019) amends the private and consumer enforcement mechanisms in the CCPA. The bill also authorizes the Attorney General to provide general guidance on compliance with the CCPA. This bill is currently pending consideration in the Senate Appropriations Committee.

SB 753 (Stern, 2019) provides that a business does not sell personal information if the business, pursuant to a written contract, shares, discloses, or otherwise communicates

to another business or third party a unique identifier only to the extent necessary to serve or audit a specific advertisement to the consumer. The bill requires the contract to prohibit the other business or third party from sharing, selling, or otherwise communicating the information except as necessary to serve or audit advertisement from the business. This bill is currently pending consideration in the Senate Judiciary Committee.

AB 288 (Cunningham, 2019) provides that when a user of a social networking service deactivates or deletes the user's account, the service shall provide the user the option of having the user's personally identifiable information permanently removed from any database controlled by the service, from the service's records, and to prohibit the service from selling that information to, or exchanging that information with, a third party in the future. Consumers are authorized to bring civil actions for damages that occur as a result of violations of the bill, including attorney's fees, pain and suffering, and punitive damages, as specified. This bill is currently pending consideration in the Assembly Privacy and Consumer Protection Committee.

AB 846 (Burke, 2019) authorizes a business to offer a different price, rate, level, or quality of goods or services to a consumer, including offering its goods or services for no fee, if either the offering is in connection with a loyalty or rewards program or the offering is for a specific good or service whose functionality is directly related to the collection, use, or sale of the consumer's data. This bill is currently pending consideration in the Senate Judiciary Committee.

AB 873 (Irwin, 2019) loosens the definition of "deidentified" and narrows the definition of "personal information" in the CCPA. The bill thereby limits the personal information subject to the protections of the CCPA. This bill is currently pending consideration in the Senate Judiciary Committee.

AB 874 (Irwin, 2019) amends the definitions of "personal information" and "publicly available" in the CCPA. It removes the application of the CCPA to publicly available information that is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in government records or for which it is publicly maintained. This bill is currently pending consideration in the Senate Judiciary Committee.

AB 981 (Daly, 2019) eliminates a consumer's right to request a business delete or not sell the consumer's personal information under the CCPA if it is necessary to retain or share the consumer's personal information to complete an insurance transaction requested by the consumer. It also strengthens privacy protections for the information of insureds. This bill is currently pending consideration in the Senate Insurance Committee.

AB 1146 (Berman, 2019) exempts from the opt-out and deletion protections and provisions of the CCPA vehicle information, including ownership information, shared

between a new motor vehicle dealer and the vehicle's manufacturer, if the vehicle information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall and is not sold, shared, or used for any other purpose. This bill is currently pending consideration in the Senate Judiciary Committee.

AB 1355 (Chau, 2019) makes a series of technical changes to the CCPA and amends the definitions of "publicly available" and "personal information." This bill is currently pending consideration in the Senate Judiciary Committee.

AB 1416 (Cooley, 2019) establishes exceptions to the CCPA for a business that provides a consumer's personal information to a government agency solely for the purposes of carrying out a government program or sells the personal information of a consumer who has opted out of the sale of the consumer's personal information to another person for the sole purpose of detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity. This bill is currently pending consideration in the Senate Judiciary Committee.

AB 1564 (Berman, 2019) reduces the methods a business must make available to consumers for submitting requests for information required to be disclosed pursuant to the CCPA. It removes the requirement that a business provide a toll-free telephone number for such purposes. This bill is currently pending consideration in the Senate Judiciary Committee.

AB 1760 (Wicks, 2019) strengthens various protections for consumers, including a change from opt-out consent for the sale of information to opt-in consent for the sharing of information. The bill also includes data minimization requirements and modifies various definitions. It also explicitly allows district attorneys, city attorneys, and county counsel to bring actions on behalf of the people for violations of the CCPA in addition to the Attorney General. It also removes the provision regarding the legal opinions of the Attorney General. This bill is currently pending consideration in the Assembly Privacy and Consumer Protection Committee.

Prior Legislation:

AB 375 (Chau, Ch. 55, Stats. 2018) *See* Comment #2.

SB 1121 (Dodd, Ch. 735, Stats. 2018) amended the CCPA to make technical fixes and to address various stakeholder concerns.

PRIOR VOTES:

Assembly Floor (Ayes 77, Noes 0)
Assembly Appropriations Committee (Ayes 18, Noes 0)

Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)
****