SENATE JUDICIARY COMMITTEE
Senator Hannah-Beth Jackson, Chair
2017-2018 Regular Session

AB 375 (Chau)
Version: June 25, 2018
Hearing Date: June 26, 2018
Fiscal: Yes
Urgency: No
CK

SUBJECT

Internet service providers: customer privacy

DESCRIPTION

This bill provides consumers the right to access their personal information that is collected by a business, the right to delete it, the right to know what personal information is collected, the right to know whether and what personal information is being sold or disclosed, the right to stop a business from selling their information, and the right to equal service and price. Each right would contain certain exceptions. This bill would also provide a modified, private right of action, allowing for enforcement by the Attorney General, along with a right to cure for businesses in violation, as specified.

BACKGROUND

The world's most valuable resource is no longer oil, but data. Companies regularly collect, analyze, share, and sell the personal information of consumers. Increasingly, the control by the larger Internet companies of this data has given them enormous power. With this widespread collection of data comes serious concerns about consumers' privacy. The Cambridge Analytica scandal exposed the trove of data being collected by Facebook, the methods through which it was collected, and the potential for harm if that data is not properly protected. This is in addition to the collection of personal information by data brokers that collect it through various public and private sources, and package it for other businesses to buy. One example is Acxiom, a data broker that provides information on more than 700 million people culled from voter records, purchasing behavior, vehicle registration, and other sources. (Nitasha Tiku, *Europe's New Privacy Law will Change the Web, and More* (Mar. 19, 2018) Wired <https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/> [as of June 25, 2018].)

Currently, everything from toasters and baby dolls to televisions are connected to the Internet, gathering and using a wide range of information. This technology has limitless possibilities. Industry experts foresee a dramatic expansion in the years ahead with internet-connected household goods, including refrigerators, washing machines,

dishwashers, and thermostats. The CEO of Cisco has declared that IoT will generate $19 trillion in profits. (Kevin Maney, *Meet Kevin Ashton, Father of the Internet of Things* (Feb. 23, 2015) Newsweek <http://www.newsweek.com/2015/03/06/meet-kevin-ashton-father-internet-things-308763.html> [as of June 25, 2018].)

However, along with the promise IoT brings comes serious privacy and security concerns. Corporations are rapidly networking the physical world and gathering data from everything. Many of these devices collect a vast amount of personal and intimate information. If not properly secured, this immense amount of private information can be vulnerable to breaches. In addition, many of these devices can be directly hacked into, allowing strangers to conduct surreptitious surveillance on homes or to communicate through devices directly. Perhaps most disturbing, consumers may not even be aware of the full capabilities of these products or the information that is being collected. Recent research indicates that the number of devices will climb from 6.4 billion at the end of last year to 25 billion by 2020. (Tim Johnson, *Why your next Echo command should be: "Disconnect me from the internet"* (May 8, 2017) Sacramento Bee <http://www.sacbee.com/news/nation-world/national/article148879664.html> [as of June 25, 2018].)

These concerns have manifested on a more regular basis in recent years as there have been various revelations of companies covertly collecting personal data through various means and using that data for various purposes. In 2017, Bose Corporation was accused of secretly collecting and sharing personal information through its Bluetooth wireless headphones. (Jeff Roberts, These Popular Headphones Spy on Users, Lawsuit Says (Apr. 19, 2017) Fortune <http://fortune.com/2017/04/19/bose-headphones-privacy/> [as of June 25, 2018].) Vizio was recently forced to pay a $2 million settlement for collecting users' information without their knowledge, including tracking users' habits. (Hayley Tsukayama, *How to stop data collection on your Vizio (or other) television* (Feb. 9, 2017) Washington Post <https://www.washingtonpost.com/news/the-switch/wp/2017/02/09/ how-to-stop-data-collection-on-your-vizio-or-other-smart-television/?noredirect= on&utm_term=.73c048629c3b> [as of June 25, 2018].)

Consumers' Web browsing, online purchases, and involvement in loyalty programs also create a treasure trove of information on consumers. Advanced technologies and the use of sophisticated algorithms can create eerily effective profiling and targeted marketing. Therefore, it is of no surprise that a recent study by the Pew Research Center found that 68 percent of American Internet users believe existing law does not go far enough to protect individual online privacy.

In response to these concerns, the proponents of the California Consumer Privacy Act, a statewide ballot initiative have been collecting signatures in order to qualify it for the November 2018, election. According to its Web site, the initiative "establishes new, groundbreaking consumer privacy rights. It empowers you to find out what information businesses are collecting about you and gives you the choice to tell businesses to stop selling your personal information." The site presents its case:

> The California Consumer Privacy Act will give you important new consumer privacy rights to take back control of your personal information.
>
> This November 2018 ballot measure says: You have the right to tell a business not to share or sell your personal information.
>
> . . .or at least you should. California law has not kept pace with changing business practices. Businesses not only know where you live and how many children you have, but also how fast you drive, your personality, sleep habits, health and financial information, current location, web browsing history, to name just a few things.
>
> You have the right to know where and to whom your data is being sold or disclosed. . . . but until you do, businesses will continue to use your personal information for their own purposes, including targeting you with ads, discriminating against you based on price or service level, and compiling your information into an extensive electronic file on you.
>
> You have the right to protections against businesses who do not uphold the value of your privacy.
>
> Passing the California Consumer Privacy Act will give you these rights. It's your personal information. Take back control!

(Californians for Consumer Privacy, *About the California Consumer Privacy Act* <https://www.caprivacy.org/about> [as of June 25, 2018].)

This bill would integrate many of the elements of the ballot initiative to provide consumers certain rights over their information, with certain exceptions. Consumers would be provided significantly more control over their information and given a modified enforcement mechanism to protect those rights. It would make its operation contingent on the withdrawal of the initiative measure above and would become operative on January 1, 2020.

CHANGES TO EXISTING LAW

Existing law, the California Constitution, provides that 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. (Cal. Const, art. I, Sec. 1.)

Existing case law states that legally recognized privacy interests are generally of two classes: interests in precluding the dissemination or misuse of sensitive and confidential information (informational privacy), and interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or

interference (autonomy privacy). (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 35.)

Existing federal and state law regulates the information practices of various industries. Examples of such laws include the federal Gramm-Leach-Bliley Act (which regulates financial institutions), Health Insurance Portability and Accountability Act (HIPAA) (which regulates the health care industry), the state Confidentiality in Medical Information Act (CMIA) (protects information maintained by the health care industry), the California Financial Information Privacy Act (protects information maintained by financial institutions), the Student Online Personal Information Protection Act (SOPIPA) (protects student information on K-12 Web sites or applications), and the Insurance Information Privacy Act (protects information maintained by the insurance industry).

Existing law establishes the Children's Online Privacy Protection Act (COPPA) to provide protections and regulations regarding the collection of personal information from children under the age of 13. (15 U.S.C. Sec. 6501 et seq.)

Existing law provides that every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier. A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts. (47 U.S.C. Sec. 222.)

Existing law, the Information Practices Act of 1977, declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. It further states the following legislative 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; and
- in order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code Sec. 1798 et seq.)

Existing law, the California Customer Records Act, provides requirements for the maintenance and disposal of customer records and the personal information contained therein. It provides the following definitions:

- "business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution, as specified. The term includes an entity that disposes of records;
- "records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted. "Records" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number;
- "customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business;
- "individual" means a natural person; and
- "personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code Sec. 1798.80 et seq.)

Existing law states it is the intent of the Legislature to ensure that personal information about California residents is protected and to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information. Existing law defines the terms "own" and "license" to include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term "maintain" includes personal information that a business maintains but does not own or license. (Civ. Code Sec. 1798.81.5(a).)

Existing law requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure and requires such businesses to contractually require nonaffiliated third parties to which it discloses such personal information to similarly protect that information. (Civ. Code Sec. 1798.81.5(b), (c).) Certain entities are excepted, including specified financial institutions and businesses regulated by law providing greater protections. (Civ. Code Sec. 1798.81.5(e).) "Personal information" for the purposes of these provisions, means either of the following:

- an individual's first name or first initial and the individual's last name in combination with one or more specified data elements, such as social security number, medical information, health insurance information, or credit card number, when either the name or the data elements are not encrypted or redacted; or
- a username or email address in combination with a password or security question and answer that would permit access to an online account. (Civ. Code Sec. 1798.81.5(d).)

Existing law requires a business to take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means. (Civ. Code Sec. 1798.81.)

Existing law, the data breach notification law, requires any agency, person, or business that owns or licenses computerized data that includes personal information to disclose a breach of the security of the system to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Secs. 1798.29(a), (c) and 1798.82(a), (c).)

Existing law requires any agency, person, or business that maintains computerized data that includes personal information that the agency, person, or business does not own to notify the owner or licensee of the information of any security breach immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code Secs. 1798.29(b), 1798.82(b).) "Personal information" for the purposes of these provisions, means either of the following:

- an individual's first name or first initial and the individual's last name in combination with one or more specified data elements, such as social security number, medical information, health insurance information, or credit card number, when either the name or the data elements are not encrypted or redacted; or
- a username or email address in combination with a password or security question and answer that would permit access to an online account. (Civ. Code Secs. 1798.29(g) and (h); 1798.82(h) and (i).)

Existing law requires businesses to either disclose to customers, upon request, what categories of personal information the business shares with third parties for marketing purposes, or provide customers with the ability to opt-out of having their information shared for marketing purposes. (Civ. Code Sec. 1798.83.)

Existing law declares any waiver of the provisions of the California Customer Records Act contrary to public policy and void and unenforceable. It provides any customer injured by a violation of these provisions a civil right of action to recover damages and

authorizes injunctive relief against such businesses. In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed $3,000 per violation; otherwise, the customer may recover a civil penalty of up to $500 per such violation. Businesses are granted a 90-day right to cure violations that are not willful, intentional, or reckless. A prevailing plaintiff is entitled to attorney's fees and costs for suits commenced under Section 1798.83. These rights and remedies are cumulative to any other rights and remedies available under law. (Civ. Code Sec. 1798.84.)

Existing law, the California Consumer Credit Reporting Agencies Act (Civ. Code Sec. 1785.1 et seq.) and the Federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.), require consumer credit reporting agencies to adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, hiring of a dwelling unit, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information. (Civ. Code Sec. 1785.1(d); 15 U.S.C. Sec. 1681(b).)

Existing law requires an operator of a commercial Internet Web site or online service (operator) that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit the commercial Internet Web site or online service to conspicuously post, or make available, its privacy policy, as specified. An operator violates this provision if the operator fails to post its policy within 30 days after being notified of noncompliance. (Bus. & Prof. Code Secs. 22575 & 22576.)

Existing law states that no satellite or cable television corporation may provide any person with any individually identifiable information regarding any of its subscribers, including, but not limited to, the subscriber's television viewing habits, shopping choices, interests, opinions, energy uses, medical information, banking data or information, or any other personal or private information, without the subscriber's express written consent. (Pen. Code Sec. 637.5(a)(2).)

Existing law specifies that individual subscriber viewing responses or other individually identifiable information derived from subscribers may be retained and used by a satellite or cable television corporation only to the extent reasonably necessary for billing purposes and internal business practices, and to monitor for unauthorized reception of services, as specified. (Pen. Code Sec. 637.5(b).)

Existing law requires, among other things, that the privacy policy identify the categories of personally identifiable information that the operator collects about individual consumers and the categories of third-party persons or entities with whom the operator may share that information. (Bus. & Prof. Code Secs. 22575 & 22576.)

This bill would establish the California Consumer Privacy Act of 2018 (the Act) to become operative on January 1, 2020, contingent on the privacy initiative being withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

This bill would provide that a consumer shall have 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. The obligation to provide such information is only triggered upon receipt of a verifiable consumer request and is limited to no more than twice per year. Such business would be required to 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 bill would provide that a consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. Upon such a request, the business would be required to delete the information from its records and direct any service providers to do the same. This right to delete would need to be disclosed by businesses collecting personal information

This bill would provide that businesses are not required to delete information upon request where it is necessary for the business to maintain the consumer's personal information for various purposes, including detecting security incidents; complying with a legal obligation; enabling solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; or otherwise using the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

This bill would provide that a consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer certain information, and the business shall disclose such information, including the following:

- the categories of personal information it has collected about that consumer;
- 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 whom the business shares personal information; and
- the specific pieces of personal information it has collected about that consumer.

This bill would provide consumers the right to request a business that sells or discloses their personal information disclose the following:

- the categories of personal information that the business collected about the consumer;

- 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
- the categories of personal information that the business disclosed about the consumer for a business purpose.

This bill would prohibit a third party from selling personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out.

This bill would provide consumers a right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell that information. It would place a requirement on 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 such sales. Such businesses would be required to provide a clear and conspicuous link on the business' Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information. For a consumer who has opted out of the sale of the consumer's personal information, a business would be required to respect the consumer's decision to opt out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

This bill would also provide that minor's must consent to the sale of their personal information before a business can sell it. It would further provide that a business shall not sell the personal information of a consumer if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale. A business that willfully disregards the consumer's age would be deemed to have had actual knowledge of the consumer's age.

This bill would prohibit discrimination against a consumer because the consumer exercised their rights under the bill. Such discrimination would include:
- denying goods or services to the consumer;
- charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title; and
- suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

This bill would provide that the above provision does not prohibit 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 by the consumer's data.

This bill would authorize businesses to offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business would be required to notify consumers of the financial incentives in such a case. A business would be permitted to enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent, which may be revoked by the consumer at any time. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data. A business would be prohibited from using financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature

This bill would set forth requirements for businesses to develop methods for consumers to exercise their rights under the Act, provide for procedures and timelines for complying with the Act's requirements, and detail the methods for identifying consumers and associating information provided by them with information collected by the business.

This bill would also require businesses to disclose specified information in its online privacy policy, including a description of consumers' rights, the methods for submitting requests, and lists of categories of information actually collected, sold, and disclosed by the business in the preceding year. Businesses would be required to inform the appropriate personnel of the requirements of the Act and how to facilitate consumers' exercise of those rights.

This bill would provide definitions for the key terms used in the Act, including the following:

- "business" would mean specified, for-profit entities that collect personal information and that meet one of the following criteria: (1) annual gross revenues of over $25 million; (2) annually buys, receives, sells, or shares the personal information of at least 50,000 consumers, households, or devices; or (3) derives 50 percent or more of its annual revenue from selling such information;
- "collects" and similar terms would mean buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.
- "consumer" would mean a natural person who is a California resident;
- "personal information" would mean information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:

    - specified identifiers, both online and off, such as a real name, alias, address, unique personal identifier, Internet Protocol address, email address, and other identifying numbers;
    - any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including signature, physical characteristics or description, education, employment, employment history, or any other financial information, medical information, or health insurance information;
    - characteristics of protected classifications under California or federal law;
    - commercial information, including 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, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement;
    - geolocation data;
    - audio, electronic, visual, thermal, olfactory, or similar information;
    - inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes;
- "research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business' service or device for other purposes must meet specified requirements;
- "sell," "selling," "sale," or "sold," would mean selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

This bill would make clear that the obligations imposed on businesses by the Act do not restrict a business's ability to comply with the law or lawful orders; cooperate with law enforcement agencies concerning unlawful conduct or activity; exercise or defend legal claims; collect information that is deidentified or in the aggregate; or to collect or sell such information if the conduct takes place wholly outside of California. The obligations of the bill would not apply if they would violate evidentiary privileges.

This bill would also make clear that it does not apply to certain information collected by a covered entity governed by the Confidentiality of Medical Information Act or the

Health Insurance Portability and Availability Act of 1996; information collected pursuant to the Gramm-Leach-Bliley Act or the Driver's Privacy Protection Act of 1994. It would also not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report.

This bill would provide certain timelines to respond to consumer requests with the ability to extend for specified reasons. If the business does not take action on the request of the consumer, the business would be required to inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business. The bill would also allow a business to charge a reasonable fee or refuse to act on a request if it is manifestly unfounded or excessive, in particular because of its repetitive character. A business would have to notify the consumer of the reason for refusing the request. The business would bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

This bill would immunize a business that discloses personal information to a service provider if the service provider receiving the personal information uses it in violation of the Act, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider would likewise not be liable for the obligations of a business for which it provides services.

This bill would provide that any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure, as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action to recover damages in an amount between $100 and $750 per consumer per incident or actual damages, whichever is greater; for injunctive or declaratory relief; or any other relief the court deems proper. The court would be required to consider specified circumstances in setting the amount of the statutory damages.

This bill would provide that a consumer is authorized to bring such actions only if all of the following requirements are met:

- prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer shall provide a business 30 days' written notice identifying the specific provisions the consumer alleges have been or are being violated. The business would have a 30-day right to cure, where possible. If cured and the business provides express written assurances that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business.

- a consumer bringing an action must notify the Attorney General within 30 days that the action has been filed; and
- the Attorney General, upon receiving such notice shall, within 30 days, do one of the following:
    - notify the consumer bringing the action of the Attorney General's intent to prosecute an action against the violation. If the Attorney General does not prosecute within six months, the consumer may proceed with the action;
    - refrain from acting within the 30 days, allowing the consumer bringing the action to proceed; or
    - notify the consumer bringing the action that the consumer shall not proceed with the action.

This bill would provide that any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the Act.

This bill would provide that a business is in violation of the Act if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be liable for a civil penalty as provided in Section 17206 of the Business and Professions Code in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section would be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. Intentional violations of the Act would be subject to a civil penalty of up to $7,500 for each violation.

This bill would provide guidelines for the disbursement of any penalties assessed or settlements secured, with 20 percent going to the Consumer Privacy Fund, newly created by this bill within the General Fund, with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

This bill would provide that wherever possible, laws relating to consumers' personal information should be construed to harmonize with the provisions of the Act, but in the event of a conflict between other laws and the Act, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control. It would supersede and preempt all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

This bill would also provide that on or before January 1, 2020, the Attorney General shall solicit broad public participation to adopt regulations to further the purposes of the Act.

This bill would provide that if a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to

a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

This bill would provide that any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt out of a business' sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

This bill would contain a severability clause.

COMMENT

1. Stated need for the bill

According to the author:

> AB 375, the California Consumer Privacy Act of 2018, ensures that consumers enjoy choice and transparency in the treatment of their personal information when accessing the Internet. Americans value their privacy, be it in the physical world or online. A PEW research study in 2016 found that "some 74% say it is 'very important' to them that they be in control of who can get information about them, and 65% say it is 'very important' to them to control what information is collected about them. The same study found that 64% of Americans believe that the government should do more to regulate what advertisers do with their personal information. Californians should have a right to choose how their personal information is collected and used. It is consistent with the right of privacy enshrined in our constitution, and we as Legislators have an obligation to ensure privacy rights for online consumers. AB 375 is a significant step in providing consumers more control over their data.

Common Sense Kids Action, the sponsor of this bill, writes in support:

> The California Consumer Privacy Act of 2018 will take the critical first step to protect the privacy of kids, families, and all consumers. This first-in-the-nation legislation would provide consumers with the following rights:
> - The right to know what personal information is being collected about them;
> - The right to know whether their personal information is sold or disclosed and to whom;
> - The right to say no to the sale of personal information;
> - The right to access their personal information; and
> - The right to equal service and price if they exercise their privacy rights.

2. The California Consumer Privacy Act of 2018

The California Consumer Privacy Act of 2018 (the Act), as established by this bill, would afford important rights to consumers to access and control their personal information. Each right would have certain exceptions that attempt to strike a balance between consumers' fundamental right to privacy and the legitimate interests of the businesses that collect such information. The Act would define "consumer" to include all California residents, ensuring widespread consumer protection.

In addition, the bill would provide a fairly expansive definition of "personal information." The definition would encompass the more obvious pieces of information such as name, address, and social security number. But also included within the non-exclusive list of what constitutes personal information is physical characteristics, biometric information, online identifiers, and Internet activity, including browsing and search histories and consumer interactions with Web sites, applications, and advertisements.

Even further, the bill would include the inferences that are drawn from the collection of these others pieces of data. Frequently, businesses draw their value from collected personal information by creating profiles of consumers reflecting their habits, patterns, preferences, political persuasions, and personalities and making inferences therefrom. The Attorney General would also be instilled with the regulatory authority to supplement the list as technologies advance. This thorough definition of what will constitute personal information makes the rights that would be provided by this bill, and that are discussed below, all the more significant.

Recently, a European privacy law went into effect that provides many of the rights afforded by the Act. It would provide that:

> companies must be clear and concise about their collection and use of personal data like full name, home address, location data, IP address, or the identifier that tracks web and app use on smartphones. Companies have to spell out why the data is being collected and whether it will be used to create profiles of people's actions and habits. Moreover, consumers will gain the right to access data companies store about them, the right to correct inaccurate information, and the right to limit the use of decisions made by algorithms, among others.

(Nitasha Tiku, *Europe's New Privacy Law will Change the Web, and More* (Mar. 19, 2018) Wired < https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/> [as of June 25, 2018].)

3. Right to access information

The first section of the Act provides consumers the right to access their information. Under this bill, consumers would have the right to seek disclosure of any of their

personal information a business has collected, up to twice per year. At or before the collection of the information, businesses would have to inform consumers as to the categories of information collected and the purposes for which it will be used. Upon request, businesses would have to deliver the ***specific pieces of personal information*** the business has collected promptly and free of charge, including the categories of personal information sold for each third party to whom the personal information was sold. This would empower consumers to discover exactly what businesses are collecting on them, regardless of whether there is a direct relationship.

This section of the bill has two adjoining paragraphs that read:

> (1) Retain any personal information collected for a single, one-time transaction, if the information is not sold or retained by the business.
>
> (2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

These paragraphs appear to be redundant, as similar provisions directly precede them.

4. Right to delete information

This bill would afford consumers the right to request deletion of any personal information a business collects. Businesses that collect personal information would need to disclose this right to delete to consumers. Again this would not be limited to businesses with which the consumer has a direct relationship.

Standing alone, this is a very broad right allowing persons to remove their sensitive data from any business' systems. However, there are numerous exceptions to this requirement to delete. For instance, businesses are not required to delete the information if it is necessary for the business or service provider to maintain the consumer's personal information in order to "[o]therwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information." The breadth, and vagueness, of this exception could arguably limit the scope of this right to delete significantly.

In addition, concerns about First Amendment rights are commonly raised around the issue of providing a right to delete, most notably when the Europe passed the law discussed above. This bill would contain an exception specifically addressing this issue, although it does not necessarily provide the most guidance to businesses who need to comply. This could be one area where regulations could more thoroughly outline the parameters of this exception.

5. Right to know what information is being collected, whether it is sold or disclosed, and to whom

This bill would provide consumers the right to request information about what types of information are being collected by a business, including the categories of information; the categories of third parties the information is shared with; and the specific pieces of information it has collected on that consumer. This would allow the consumer to be fully informed of what information is being kept by any business. The definition of "collect" would be fairly broad, as well. It would include information that a business receives passively, as well as actively, and even information that is obtained through simply observing the consumer's behavior. This all-encompassing definition ensures this right, as well as others discussed herein, are significantly robust.

It would also require businesses that sell or disclose the personal information of a consumer to disclose certain information to that consumer, upon request, including the categories of information being sold and disclosed and the third parties to whom it is being sold or disclosed.

6. Right to opt out of the sale of personal information

Consumers would be given the right, pursuant to this bill, to opt out of the sale of their personal information. A business would have to abide by such a request and respect the request to opt out for 12 months before being permitted to request that the consumer authorize the sale of the consumer's personal information.

It should be noted that the definition of "sell," "selling," "sale," or "sold," would include "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." This definition makes some important changes from that in the privacy initiative. The privacy initiative provides the following definition for "selling":

> (A) selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for valuable consideration; or
> (B) sharing orally, in writing, or by electronic or other means, a consumer's personal information with a third party, whether for valuable consideration or for no consideration, for the third party's commercial purposes.

"Sell" as used in this bill would essentially delete this second section of the definition, importantly the sharing of the information for no consideration to a third party for that party's commercial use. It is unclear why this change was made, but its effect would be

that a consumer could not opt out of the sharing of their personal information with third parties, so long as there is not valuable consideration received.

As a strong transparency and consumer protection measure, the bill would place a requirement on any business that sells personal information of consumers to third parties to notify those consumers of the possibility of such sales and inform them of their rights to opt out of such sales. This affirmative requirement on businesses that sell personal information would serve strong policy goals to make consumers fully aware of how their information is being used and their rights to stop such use.

An enhanced right would also be provided for minors. Businesses would be prohibited from selling the information of minors without their consent. This provides an "opt in" mechanism for minors, while all other consumers would have the ability to "opt out." However, there are two provisions governing the selling of minor's information. In Section 1798.120(c), it provides that a business that has not received consent to sell a minor's information shall be prohibited from selling it. This would presumably apply to any minor; thus, persons under 18 years of age. However, subdivision (d) of the same section provides an opt-in provision for consumers who are 16 years of age or younger, requiring them, or their parents for those under 13 years of age, to "affirmatively authorize" the sale. It is not clear what the difference between the consent that is required for all minors, and the affirmative authorization that is required for those minors 16 years of age or younger. However, it would likely be interpreted to mean that all minors would need to opt in before a business could sell their personal information.

7. Discrimination and pay-for-privacy

This bill would prohibit discrimination against a consumer based on the fact that the consumer exercised their rights under the bill. Such discrimination would include:

- denying goods or services to the consumer;
- charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title; and
- suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

These provisions standing alone would ensure that the rights that would be established by the Act are protected. However, the bill would also provide that these anti-discrimination provisions do not prohibit 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 by the consumer's data. The bill would further authorize businesses to offer financial incentives, including payments to consumers as compensation, for the

collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data.

Section 1798.125, where these anti-discrimination and incentive provisions reside, is internally inconsistent to a certain extent. It specifically prohibits "charging different prices or rates for goods or services." But, it also specifically authorizes in the following paragraph "charging a consumer a different price or rate." The same tension exists for "providing a different level or quality of goods or services." This is problematic in and of itself because it is vague as to exactly how a business can treat a consumer based solely on whether they have exercised their rights pursuant to the Act. Worse, these provisions could be read as an endorsement of pay-for-privacy type practices.

Privacy is of such import to California that it is enshrined in the California Constitution as an inalienable right. (Cal. Const, art. I, Sec. 1.) Allowing for businesses to treat consumers differently on the basis of whether they forego exercising that right is problematic. These provisions arguably can contribute to the transformation of a constitutional right into a luxury product that is affordable by a select few, creating unequal access to privacy and further enabling predatory and discriminatory behavior. This is a constitutional right that the Legislature should not commodify lightly.

8. Policies and procedures

The bill would outline requirements around how businesses should respond to requests and the timelines for doing so. It would also provide guidance on how to comply with the various provisions, namely the process of identifying consumers and associating the information that is supplied by the consumer in the relevant request with information the business has collected that is actually connected to that person. These provisions provide clear guidance on the basics for ensuring compliance. As the bill also calls upon the Attorney General to adopt regulations to carry out the various provisions of the Act, these procedures would likely be further flushed out through the regulatory process.

The bill would also outline specific pieces of information that would need to be included in the privacy policies of businesses that have such policies in place. This section of the bill would ensure consumers have a readily accessible way to find out what their rights are and how to exercise them. It would also require businesses to list out the various categories of information that they collect on consumers, including the specific categories of personal information that it has sold and the specific categories it has disclosed in the preceding 12-month period.

9. Other parameters on the rights provided by the Act

This bill would provide certain immunities and exemptions from compliance. First, a business would not be liable for violations of a service provider to which it discloses personal information as long as the business did not have actual knowledge or reason to believe the violation would occur. This is arguably a reasonable limitation on liability.
The bill would also allow a business to charge a reasonable fee or refuse to act on a request if it is "manifestly unfounded or excessive." A business would have to notify the consumer of the reason for refusing the request and would bear the burden of demonstrating the request is manifestly unfounded or excessive. It is unclear when a request by a consumer for, say, access to their information, would be determined to be manifestly unfounded. The bill already limits several of the business' obligations to no more than twice annually, thereby building in a protection for vexatious requests. One possible outcome of this provision is that it may open the door for fees to systematically be imposed on consumers.

10. Enforcement mechanisms

a. Private right of action

This bill would provide that any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure, as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action. In addition to injunctive and declaratory relief, the consumer would be able to seek recovery of actual damages or statutory damages in an amount between $100 and $750 per consumer per incident, whichever is greater. The court would be required to consider specified circumstances in setting the amount of the statutory damages, including the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth. For the purposes of this right of action, "personal information" would be as defined in Section 1798.81.5(d)(1)(A), which provides that personal information is either:

> (A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
> (i) Social security number.
> (ii) Driver's license number or California identification card number.
> (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
> (iv) Medical information.

(v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

This would create a private right of action for those whose personal information has been compromised through the failure of a business to properly maintain that information. By allowing any consumer to bring such actions, this bill would not require a direct contractual relationship between the consumer and the business. This would allow consumers to enforce their rights regarding personal information that is subject to unauthorized access, destruction, use, modification, or disclosure where the business is a data broker or other type of entity that collects personal information on consumers.

However, before a consumer could bring an action, the consumer would need to meet certain requirements. First, prior to initiating a civil action for statutory damages, a consumer would need to provide the offending business 30 days' notice of the alleged violations. If applicable, the business would have the right to cure during those 30 days. If cured and the business provides a written statement that the violations have been cured and that no further violations will occur, the consumer is prevented from seeking statutory damages.

The bill also provides that a "consumer bringing an action as defined in paragraph (1) of subdivision (c) shall notify the Attorney General within 30 days that the action has been filed." First, there is no subdivision (c) within this section so it is unclear what this is in reference to. The reference should be clarified or removed. As to the substance, the Attorney General would, upon receiving this notice, have the authority to notify the consumer of its intent to prosecute an action for the violation. The Attorney General would then have six months to do so. After such period, if no action is prosecuted, the consumer would be authorized to proceed with the action. If the Attorney General does not act at all in response to the notice within 30 days, the consumer would be authorized to proceed.
However, the bill would also provide that, in response to the notice, the Attorney General could notify "the consumer bringing the action that the consumer shall not proceed with the action." This would essentially give the Attorney General the ability to unilaterally veto a consumer's right to bring an action under this section. While there is precedent for requiring a private plaintiff to provide the right of first refusal to the Attorney General to bring the action, there is no relevant precedent found that allows the Attorney General to simply tell the plaintiff no, without any explanation, without any criteria to apply, and without any other action required on the part of the Attorney General. (*See, e.g.*, Gov. Code Sec. 12652 [False Claims Actions]; Health & Saf. Code Sec. 25249.7 [Proposition 65].) Given that privacy is a constitutional right, allowing an official within the executive branch to deny a consumer the ability to vindicate that right pursuant to statute is problematic at best. This could allow the Attorney General to block an action even in the most egregious cases.

It is unclear what the justification is for such a provision, especially when there is no standard for the Attorney General to apply in determining whether to so restrict the plaintiff. Providing individual officials with the power to block Californians from the courts, even if limited to the enforcement of statutory claims, sets a troubling precedent.

In addition, a recent amendment to the bill would add the following subdivision to the section providing the private right of action: "Nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution." It appears that this provision would eliminate the ability of consumers to bring claims for violations of the Act under statutes such as the Unfair Competition Law, Business and Professions Code Section 17200 et seq. It also makes clear that the Act does not relieve any parties from having to follow the Constitution. This latter provision is likely unnecessary.

b. Attorney General enforcement and regulations

The Act would provide that a business in violation of the Act shall be given a 30-day right to cure. Businesses, service providers, or other persons failing to cure violations would be liable for civil penalties as provide in Section 17206 of the Business and Professions Code in an action brought by the Attorney General. In addition, for intentional violations of the Act, the liable party would be subject to civil penalties of up to $7,500 per violation.

The proceeds of such actions would be divided up as specified. Twenty percent would be placed into a newly created Consumer Privacy Fund, which would be placed within the General Fund. The purpose of the fund would be to offset the costs incurred by the judiciary and the Attorney General in enforcing the Act.

Furthermore, as referenced above, the Attorney General would be directed to adopt regulations to ensure the proper implementation of the Act and the realization of its purpose to protect consumers' personal information. This authority would allow the Attorney General to add to the definition of personal information, which is critically important as technology advances. The regulations could help to facilitate consumers' ability to opt out pursuant to the Act and otherwise exercise the rights newly created by the Act. It would also ensure that businesses are provided the necessary resources and direction to facilitate compliance.

In addition, the Attorney General would be given the power to establish "rules and guidelines regarding financial incentive offerings." This could serve the function of ensuring that the "anti-discrimination" provisions found in Section 1798.125(a)(1) are not undermined by the language in Section 1798.125(b). The former provision makes clear that discriminating against consumers for exercising their rights pursuant to the act is prohibited. The intent of this legislation is to afford consumers the maximum

amount of control over their data, and robust anti-discrimination provisions are critical to realizing that intent. Therefore, strong regulations carrying out this intent are vital.

Support: None Known

Opposition: Media Alliance

HISTORY

Source: Common Sense Kids Action

Related Pending Legislation:

SB 1121 (Dodd, 2018) would replace the term "customer" as used in Sections 1798.80 through 1798.84 of the Civil Code, the California Customer Records Act, with the term "consumer." It would also provide any consumer whose personal information has been breached or has not been properly notified of a breach with the right to institute a civil action for the recovery of statutory damages, injunctive or declaratory relief, and any other relief the court deems proper. This bill is currently in the Assembly Privacy and Consumer Protection Committee.

AB 1859 (Chau, 2018) would require a consumer credit reporting agency that knows of a vulnerability that could compromise the security of personal information for which there is an update to address, to apply that update or be held liable for any resulting damages. This bill is being heard in the Senate Judiciary Committee on the same day as this bill.

Prior Legislation: AB 375 (Chau, 2017), the previous version of this bill, would have enacted the California Broadband Internet Privacy Act to implement a modified version of the repealed Federal Communications Commission Rules regarding Internet Privacy.

Prior Vote:

Senate Judiciary Committee (Ayes 5, Noes 2)
Senate Energy, Utilities and Communications Committee (Ayes 9, Noes 1)
Assembly Floor (Ayes 77, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)

****