SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

AB 1711 (Seyarto)
Version: April 21, 2022
Hearing Date: June 14, 2022
Fiscal: Yes
Urgency: No
CK

SUBJECT

Privacy: breach

DIGEST

This bill requires agencies to report data breaches on their website when a person or business operating a system on behalf of an agency is required to disclose a breach of that system.

EXECUTIVE SUMMARY

Current law requires businesses that own, license, or maintain personal information to implement and maintain reasonable security procedures and practices to protect that information. In addition, California's data breach notification statutes require government agencies, persons, and businesses to provide residents with specified notices in the wake of breaches of residents' personal information.

This bill addresses the situation where a person or business is operating a system on behalf of a government agency. Where the person or business is currently required to disclose a breach of that system, this bill requires the agency to also disclose the breach by conspicuously posting the notice on its internet website.

The author argues this is necessary to make clear to affected consumers that the data breach notice is authentic and to inform them of where the data that was breached originated. Opposition argues that this confuses the roles of agency and vendor, and that the online posting requirement should be removed from the bill.

This bill is author sponsored. It is supported by Oakland Privacy. It is opposed by the Association of California School Administrators, the California Association of School Business Officials, and the California Special Districts Association.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, Sec. 1.)

2) Establishes the Information Practices Act of 1977, which 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:

    a) 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;
    b) 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
    c) 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 § 1798 et seq.)

3) Establishes the data breach notification law, which 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 §§ 1798.29(a), (c) and 1798.82(a), (c).)

4) Requires, pursuant to the data breach notification law, that 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 §§ 1798.29(b), 1798.82(b).)

5) Defines "personal information" for the purposes of the data breach notification law, to mean either of the following:

a) 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, credit card number, or unique biometric data generated from measurements or technical analysis of human body characteristics used to authenticate a specific individual, when either the name or the data elements are not encrypted or redacted; or
b) 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 §§ 1798.29(g) and (h); 1798.82(h) and (i).)

6) Provides that an agency, person, or business that is required to issue a security breach notification shall meet specified requirements. The notification must be written in plain language, meet certain type and format requirements, be titled "Notice of Data Breach," and include specified information. (Civ. Code §§ 1798.29(d), 1798.82(d).) Additionally, it authorizes them, in their discretion, to also include in the notification information about what the person or business has done to protect individuals whose information has been breached or advice on steps that the person may take to protect themselves. (Civ. Code §§ 1798.29(d), 1798.82(d).)

7) Establishes the California Customer Records Act, which provides requirements for the maintenance and disposal of customer records and the personal information contained therein. (Civ. Code § 1798.80 et seq.) It further 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. (Civ. Code § 1798.81.5(a).)

8) 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 § 1798.81.5(b), (c).)

This bill:

1) Provides that when a person or business operating a system on behalf of an agency is required to disclose a breach of that system, the agency shall also disclose the breach by conspicuously posting, for a minimum of 30 days, the notice provided by the person or business on the agency's internet website, if the agency maintains one.

2) Requires the disclosure to be posted in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

3) Defines "conspicuously posting on the agency's internet website" to mean providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

COMMENTS

1. The stunning incidence of data breaches

A vast majority of Californians engage in a wide range of activities online. Even before the pandemic forced many people to drastically shift their lives online, 70 percent of people in the state received financial services online, 39 percent telecommuted, 42 percent accessed sensitive health or insurance records online, and 39 percent communicated with doctors.[1] In addition, many companies have realized the financial benefits of collecting as much data on consumers as possible, tracking, storing, and selling the details of our everyday lives. Given the amount of activity online and the massive amount of data being collected and switching hands, concerns about data security have skyrocketed.

In 2020 alone, estimates suggest that there were over 1000 data breaches resulting in the exposure of over 155 million records.[2] According to the Federal Bureau of Investigation's (FBI) Internet Crime Report, the Internet Crime Complaint Center received "a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019."[3] A brief look at a few of the larger breaches illustrates the scope of the problem.

---

[1] Niu Gao & Joseph Hayes, *California's Digital Divide* (February 2021) Public Policy Institute of California, https://www.ppic.org/publication/californias-digital-divide/. All internet citations are current as of June 1, 2022.
[2] Joseph Johnson, *Cyber crime: number of breaches and records exposed 2005-2020* (March 3, 2021) Statista, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/#:~:text=In%202020%2C%20the%20number%20of,%2Dthan%2Dadequate%20information%20security.
[3] Internet Crime Complaint Center, *2020 Internet Crime Report* (March 17, 2021) FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

The infamous 2017 breach at Equifax lasted at least several months. "If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies."[4] The hackers involved were able to access people's names, Social Security numbers, birth dates, addresses, and driver's license numbers. Over 200,000 consumers also had their credit card numbers stolen. There is evidence that the massive hack of personal information has led to extensive identity theft with the thieves using the stolen information to apply for mortgages, credit cards, and student loans. The information is also being used to tap into bank accounts, to file insurance claims, and to incur massive debts on behalf of affected consumers.

Even before that, a much larger breach occurred in 2013, when hackers accessed Yahoo's email system, gathering data on more than 1 billion users.[5] Several years after the hack, a group began offering the entire database of information for sale on the so-called "dark web," with at least three confirmed buyers paying $300,000 each. The breach was not disclosed by Yahoo until 3 years after it occurred. It came after an earlier breach of 450,000 accounts in 2012 and before a hack in 2014 of 500 million user accounts.

More recently, in 2019, the personal information of over 530 million Facebook users was taken in a breach that exploited a vulnerability in a Facebook feature.[6] The company recently indicated it has decided not to notify the individual users affected, but the information remains publicly available after being posted to an online hacking forum. Major breaches have also occurred in the last year, with GEICO having driver's license data on 132,000 customers stolen and a hack of the ParkMobile application resulting in the personal information of 21 million users exposed.[7]

Unfortunately, because of the size of its economy and the sheer number of consumers, the data collected and held by California businesses is frequently targeted by cyber criminals, and California accounts for a sizeable share of the nation's data breaches.[8] In

---

[4] Seena Gressin, *The Equifax Data Breach: What to Do* (Sep. 9, 2017) Federal Trade Commission, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.
[5] Vindu Goel & Nicole Perlroth, *Hacked Yahoo Data Is for Sale on Dark Web* (December 15, 2016) The New York Times, https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html.
[6] Emma Bowman, *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users* (April 9, 2021) NPR, https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users.
[7] Zack Whittaker, *Geico admits fraudsters stole customers' driver's license numbers for months* (April 19, 2021) TechCrunch, https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/; Joe Marusak, *If you find parking spots with this popular app, your data may have been stolen* (April 16, 2021) Charlotte Observer, https://www.charlotteobserver.com/news/local/article250666434.html.
[8] California Department of Justice, *California Data Breach Report* (February 2016) https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

2015 alone, nearly three in five Californians were victims of a data breach. These data breaches are not harmless. The Attorney General reports that 67 percent of breach victims in the United States were also victims of fraud.

The frequency of data breaches in California and the threat that such breaches pose makes the enactment and enforcement of statutes protecting against and responding to these breaches vital to maintaining the right to privacy for California residents. California has addressed these issues over the years by requiring specific procedures for notifying individuals of data breaches; requiring certain security procedures and practices to prevent such breaches; and providing a right of action if such requirements are not implemented.

2. Laws to prevent and respond to data breaches

In 2003, California's first-in-the-nation security breach notification law went into effect. (*See* Civ. Code §§ 1798.29, 1798.82.) Since that time, nearly every state has enacted similar security breach notification laws, and governments around the world have or are considering enacting such laws. California's Data Breach Notification Law (DBNL) has two main provisions governing data breach notification requirements, Civil Code Sections 1798.29 and 1798.82. The two provisions are nearly identical, but the former applies to public agencies and the latter to persons or businesses.

California's DBNL 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. Such breach notifications must be titled "Notice of Data Breach," are required to meet certain formatting requirements, and must include specific information. This notification requirement ensures that residents are made aware of a breach, thus allowing them to take appropriate action to mitigate or prevent potential financial losses due to fraudulent activity.

3. Further clarity for breaches of systems operated on behalf of public agencies

According to the author:

> AB 1711 requires a state agency to conspicuously post a link on its website to the breach notification submitted by a business operating a system on behalf of the agency. This obligation is limited to systems that the business operates on behalf of the state agency. This will help provide clarification to the public who may view the business notification of the data breach suspiciously as a phishing scam.

As stated, this bill amends the DBNL to cover specific breaches, those compromising a system being operated by a person or business *on behalf of* an agency. The concern is that consumers may receive data breach notifications from the person or business operating the system and not make the connection to the agency to whom they have given their information. This can result in either consumers not trusting the notification or simply not being as informed about what data has been breached. The bill requires the agency itself to also post the notification for a limited period of time to better get the word out to affected Californians. The goal is greater transparency leading to better data protection when consumers are able to begin to mitigate the risks more quickly and efficiently.

Writing in support, Oakland Privacy makes the case for the bill:

> Assembly Bill 1711 adds new language for the second scenario (an entity maintaining computerized data on behalf of an agency that the agency does not own) mandating that the government agency's disclosure of the breach takes the form of a conspicuous website notice.
>
> While certainly representing an increased administrative burden, we are confident that notices solely from third party contractors can be confusing to consumers trying to figure out what data this contractor possessed and why they had it. If people don't know a data breach has occurred and what data of theirs is affected and how, they are unable to take actions to protect themselves, if such actions are needed.
>
> Actions people impacted by data breaches can take includes changing passwords, initiating two-step authentication, requesting a credit freeze, signing up for a monitoring service, or replacing financial cards. Certain actions may or may not be necessary for a particular data breach scenario, but impacted persons should always have the choice to be fully informed and to make the best decisions for themselves.

A coalition of associations write in opposition, including the Association of California School Administrators and the California Association of School Business Officials, writes in an oppose-unless-amended position:

> AB 1711 confuses the roles and responsibilities of a public agency and vendor.
>
> Under AB 1711, the public agency would be required to post a notice on their agency's website (if they have one) even when the vendor maintaining their data was the source of the data breach. We believe the proposed online posting requirements could create further confusion and alarm rather than provide helpful information, at the expense of staff time

and resources. Parties' whose data was not affected could flood the agency with inquiries to determine if their data was exposed.

Public agencies already place a significant amount of information on their homepages, which is critical to their operations and allows services to be provided in a timely and efficient manner. Adding further required website content, particularly on homepages or first significant webpages, may distract from the core service functions of public agencies. AB 1711's prescriptive language and lack of flexibility as to what constitutes conspicuously posting a link to a notice may also raise potential website accessibility concerns now or in the future.

SUPPORT

Oakland Privacy

OPPOSITION

Association of California School Administrators
California Association of School Business Officials
California Special Districts Association

RELATED LEGISLATION

Pending Legislation:

AB 2135 (Irwin, 2022) requires state agencies that do not fall under the direct authority of the Governor to adopt and implement certain information security and privacy policies, standards, and procedures meeting specified federally-established criteria, and requires those agencies to perform a comprehensive independent security assessment every two years for which they may contract with the Military Department or a qualified responsible vendor. This bill is currently in this Committee.

AB 2190 (Irwin, 2022) requires that the chief of the Office of Information Security submit an annual statewide information security status report including specified information to the Assembly Committee on Privacy and Consumer Protection beginning no later than January 2023. This bill is currently in this Committee.

AB 2355 (Salas, 2022) requires any local education agency to report any cyberattack impacting more than 500 pupils or personnel to the California Cyber Security Integration Center, and requires it to establish a database that tracks reports of such cyberattacks and to report annually to the Governor and relevant policy committees of the Legislature. This bill is currently in the Senate Education Committee.

Prior Legislation:

AB 346 (Seyarto, 2021) would have expanded the DBNL for public agencies to apply to circumstances in which the personal information of a California resident was, or is believed to have been, accessed or acquired, rather than just acquired, by an unauthorized person. This bill died in the Assembly Privacy and Consumer Protection Committee.

AB 825 (Levine, Ch. 527, Stats. 2021) added "genetic information" to the definition of personal information for purposes of the laws requiring certain businesses to implement and maintain reasonable security procedures and practices to protect personal information they own, license, or maintain. It required businesses and agencies that maintain personal information to disclose a breach of genetic information.

AB 1130 (Levine, Ch. 750, Stats. 2019) updated the definition of "personal information" in various consumer protection statutes, including the DBNL, to include certain government identification numbers and biometric data.

AB 2678 (Irwin, 2018) would have provided that a person or business that is required to provide a security breach notification pursuant to California's data breach notification statutes must include therein a notice instructing the affected person that information related to security freezes and fraud alerts is available from the major credit reporting agencies and include the mailing address and internet website address of the major credit reporting agencies, as specified. This bill died on the Senate Inactive File.

AB 1950 (Wiggins, Ch. 877, Stats. 2004) required a business that owns or licenses personal information about a California resident to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure.

SB 1386 (Peace, Ch. 915, Stats. 2002) created the DBNL.

PRIOR VOTES:

Assembly Floor (Ayes 65, Noes 0)
Assembly Appropriations Committee (Ayes 14, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)

****