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

AB 825 (Levine)
Version: March 26, 2021
Hearing Date: June 22, 2021
Fiscal: Yes
Urgency: No
CK

SUBJECT

Personal information: data breaches: genetic data

DIGEST

This bill adds "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. The bill requires businesses and agencies that maintain personal information to disclose a breach of genetic information.

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 expands the definition of personal information in each of those statutes to include genetic data. That term is defined as any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

This bill is author-sponsored. It is supported by genetic testing companies and consumer groups. It is opposed by the California Chamber of Commerce and TechNet.

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 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).)

4) 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).) "Personal information" for these purposes means either of the following:

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

b) an individual's first name or first initial and their 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, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;
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; or
vi. unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes. (Civ. Code § 1798.81.5(d).)

5) 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).)

6) 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).)

7) 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).)

8) 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).)

9) Prohibits discrimination under the Unruh Civil Rights Act and the Fair Employment and Housing Act on the basis of genetic information. (Civ. Code § 51; Gov. Code § 12920 et seq.)

10) Subjects those improperly disclosing genetic test results to civil and criminal penalties. (Civ. Code § 56.17; Ins. Code § 10149.1.)

11) Establishes the California Consumer Privacy Act of 2018 (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure when their personal information is collected; 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.)

This bill:

1) Adds "genetic data" to the definition of "personal information" for purposes of the data breach notification laws and Section 1798.81.5.

2) Defines "genetic data" to mean any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs),

uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

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.

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

---

[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 10, 2021.
[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.
[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.

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 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

---

[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.

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

a. Data breach notification law

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, all but three states have enacted similar security breach notification laws, and governments around the world have or are considering enacting such laws. There are two 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 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. 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.

b. Implementation of reasonable security features

In 2004, AB 1950 (Wiggins, Ch. 877, Stats. 2004) added Section 1798.81.5 to the Civil Code. The stated intent of that section is "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."

Section 1798.81.5 currently requires businesses that own, license, or maintain certain personal information to implement and maintain reasonable security procedures and practices, appropriate to the nature of the information, to protect that information from unauthorized access, destruction, use, modification, or disclosure.

Businesses that disclose personal information about a California resident pursuant to a contract with a nonaffiliated third party, that is not covered by the requirement above, must require by contract that the third party 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. (Civ. Code § 1798.81.5.)

c. Accountability for negligent data breaches

Included in the CCPA is one avenue for consumers to assert their own privacy rights. The CCPA provides an enforcement mechanism to consumers whose nonencrypted or nonredacted personal information is breached. In order for this cause of action to lie, the breach must have been the "result of the business's 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." (Civ. Code § 1798.150.)

The aggrieved consumer is entitled to recover damages between $100 and $750 per incident or actual damages, whichever is greater. The consumer is also entitled to injunctive or declaratory relief, and any other relief the court deems proper.

3. Ensuring sensitive, personal information is included in these protections

Each of these statutes provides Californians enhanced protections over their personal information, as respectively defined. This bill updates the definition of "personal information" applicable in these statutes to include "genetic data."

Currently, the breach notification statutes define "personal information" to mean either of the following:

- a username or email address, in combination with a password or security question and answer that would permit access to an online account; or
- an individual's first name or first initial and 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:
    - social security number;
    - driver's license number or California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;
    - account number or 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;
    - medical information;
    - health insurance information;
    - unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not

include a physical or digital photograph, unless used or stored for facial recognition purposes; or
- information or data collected through the use or operation of an automated license plate recognition system.

(Civ. Code §§ 1798.29(g); 1798.82(h).)

In order to ensure that residents are likewise informed when their most sensitive and immutable data, their genetic data, is subject to a breach, this bill expands the definition of personal information to include such data.

Similarly, the bill expands the definition of "personal information" in Section 1798.81.5, the reasonable security statute, to include an individual's genetic data. For purposes of the consumer enforcement mechanism in the CCPA, "personal information" is defined by cross-reference to the definition in Section 1798.81.5.

According to the author:

> AB 825 will require Californians to be notified if there has been a breach of their personal genetic data by including "genetic data" in California's Data Breach Notification Law. Just as a company or government agency must disclose to an individual if their personal financial information or other identifying information has been breached, AB 825 will provide Californians with timely notification if there is a breach of a person's most personal information, their genetic data.

This bill builds on previous bills by this author. AB 1130 (Levine, Ch. 750, Stats. 2019) was similar to this bill, as it amended the definition of "personal information" in these same three statutes. It added biometric information, as specified, as well as certain government identification numbers.

Last year, AB 2301 (Levine, 2020) was introduced. It would have added "genetic information" to the definition of personal information for purposes of the reasonable security statute and the data breach notification law applicable to persons and businesses. That bill defined "genetic information" as information about any of the following:

- the individual's genetic tests;
- the genetic tests of family members of the individual;
- the manifestation of a disease or disorder in family members of the individual.

"Genetic information" also included any request for, or receipt of, genetic services, or participation in clinical research that includes genetic services, by the individual or any

family member of the individual, but excluded information about the sex or age of the individual.

In contrast, this bill uses the term genetic *data* and defines it much more broadly:

> "[G]enetic data" means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

The thorough definition ensures that businesses are properly safeguarding this most private of information, including data that has been produced but has not or cannot be interpreted.

Writing in support, Consumer Reports and Privacy Rights Clearinghouse make the case for these protections:

> Genetic data clearly warrants strong security protections, particularly in light of the plethora of data breaches in recent years, including a recent security breach involving customer genetic data at GEDMatch in July of last year.[9] Companies need incentives to safeguard the data: in 2019, the genetic-testing startup Veritas, which uses DNA data to identify potential health risks, suffered a data breach involving unauthorized access to consumer data.[10] In 2018, the ancestry site MyHeritage, which collects DNA data, disclosed that they left email addresses and hashed passwords unprotected on a server.[11] Aside from the inherent privacy interest in keeping this information secure, if this data becomes publicly available due a data breach, it could potentially be accessed by others and used to

[9] Zach Whittaker, *GEDMatch Confirms Data Breach After Users' Profile Data Made Available to Police* (July 22, 2020) TECHCRUNCH, https://techcrunch.com/2020/07/22/gedmatch-investigating-dna-profile-law-enforcement/.
[10] Zach Whittaker, *DNA Testing Startup Veritas Genetics Confirms Data Breach* (Nov. 7, 2019) TECHCRUNCH, https://techcrunch.com/2019/11/07/veritas-genetics-data-breach/.
[11] Makena Kelly, *MyHeritage breach leaks millions of account details* (Jun. 5, 2018) THE VERGE, https://www.theverge.com/2018/6/5/17430146/dna-myheritage-ancestry-accounts-compromised-hack-breach.

> discriminate against consumers.[12] For example, access to long- term care insurance can be impacted by the results of genetic testing.[13]

Even the United States Department of Defense has issued a memo raising security concerns relating to genetic data: "[T]here is increased concern in the scientific community that outside parties are exploiting the use of genetic materials for questionable purposes, including mass surveillance and the ability to track individuals without their authorization or awareness."[14]

The California Chamber of Commerce and TechNet write in opposition to the bill:

> AB 825 would create confusion by scoping-in existing language into the definition of "genetic data." Health data and biometric data are already separately defined in this code section. Creating a definition for a new term that scopes-in this data would cause confusion with regards to interpretation, enforcement, and compliance.
>
> AB 825 states that results from "another source enabling equivalent information to be obtained" can also be included in the definition of "genetic data." The term "equivalent information" is not limited to genetic material or information, making it broader than necessary.

SUPPORT

23andme
Ancestry
California Public Interest Research Group
Coalition for Genetic Data Protection
Consumer Attorneys of California
Consumer Reports
Privacy Rights Clearinghouse

OPPOSITION

California Chamber of Commerce
TechNet

---

[12] Angela Chen, *Why a DNA Data Breach Is Much Worse than a Credit Card Leak* (Jun. 6, 2018) THE VERGE, https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics.
[13] Ins. Code § 10233.2. Under the prohibited provisions governing long-term insurance, prohibiting the use of genetic information is not mentioned, and neither genetic testing nor genetic information is referenced.
[14] Tim Stelloh & Pete Williams, *Pentagon tells military personnel not to use at-home DNA kits* (December 23, 2019) NBC News, https://www.nbcnews.com/news/military/pentagon-tells-military-personnel-not-use-home-dna-kits-n1106761.

RELATED LEGISLATION

Pending Legislation:

SB 41 (Umberg, 2021) establishes the Genetic Information Privacy Act, providing additional protections for genetic data by regulating the collection, use, maintenance, and disclosure of such data. This bill is currently in the Assembly Privacy and Consumer Protection Committee.

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

Prior Legislation:

AB 2301 (Levine, 2020) *See* Comment 3.

SB 180 (Chang, Ch. 140, Stats. 2019) requires a person selling a gene therapy kit, such as CRISPR-Cas9 kits, in California to include a notice on their website that is displayed to the consumer prior to the point of sale, and to place the notice on a label on the package containing the gene therapy kit, in plain view and readily legible, stating that the kit is not for self-administration.

AB 1130 (Levine, Ch. 750, Stats. 2019) *See* Comment 3.

AB 1950 (Wiggins, Ch. 877, Stats. 2004) *See* Comment 2.

PRIOR VOTES:

Assembly Floor (Ayes 75, Noes 0)
Assembly Appropriations Committee (Ayes 16, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 0)

****