
THIRD READING

Bill No: AB 825
Author: Levine (D)
Amended: 3/26/21 in Assembly
Vote: 21

SENATE JUDICIARY COMMITTEE: 10-1, 6/22/21

AYES: Umberg, Borgeas, Caballero, Durazo, Gonzalez, Hertzberg, Laird, Stern,
Wieckowski, Wiener

NOES: Jones

SENATE APPROPRIATIONS COMMITTEE: 5-2, 8/26/21

AYES: Portantino, Bradford, Kamlager, Laird, McGuire

NOES: Bates, Jones

ASSEMBLY FLOOR: 75-0, 5/27/21 - See last page for vote

SUBJECT: Personal information: data breaches: genetic data

SOURCE: Author

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

ANALYSIS:

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. (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 specified data elements, when either the name or the data elements are not encrypted or redacted. (Civ. Code § 1798.81.5(d).)
- 5) Establishes the data breach notification law, which requires any specified agency, person, or business 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 specified agency, person, or business 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.

Background

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, DNA, RNA, genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, SNPs, uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom. (NOTE: For a more thorough analysis, please see the Senate Judiciary Committee analysis of the bill.)

Comments

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.

Laws to prevent and respond to data breaches

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.¹ 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 practices to prevent such breaches; and providing a right of action if such requirements are not implemented. This bill deals with three such statutes.

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.

In 2004, AB 1950 (Wiggins, Chapter 877, Statutes of 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, and certain third parties, to implement and maintain reasonable security procedures and practices, appropriate to the nature of the

¹ 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>.

information, to protect that information from unauthorized access, destruction, use, modification, or disclosure.

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.

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.”

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, this 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.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: Yes

According to the Senate Appropriations Committee:

- Ongoing investigatory and enforcement workload costs of \$366,000 annually for 1.0 Deputy Attorney General and 1.0 Legal Secretary related to this bill. (Special fund*)
- Unknown costs to various state agencies to provide increased security breach notifications related to the breach of unencrypted genetic data.
- Unknown cost pressures to various state agencies to encrypt genetic data to the extent that they do not encrypt such data currently.

*Unfair Competition Law Fund

SUPPORT: (Verified 8/26/21)

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

OPPOSITION: (Verified 8/26/21)

California Chamber of Commerce
Insights Association
TechNet

ARGUMENTS IN SUPPORT: 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. 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. In 2018, the ancestry site MyHeritage, which collects DNA data, disclosed that they left email addresses and hashed passwords unprotected on a server. 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 discriminate against consumers. For example, access to long- term care insurance can be impacted by the results of genetic testing.”

ARGUMENTS IN OPPOSITION: The California Chamber of Commerce and TechNet write: “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.”

ASSEMBLY FLOOR: 75-0, 5/27/21

AYES: Aguiar-Curry, Arambula, Bauer-Kahan, Bennett, Berman, Bigelow, Bloom, Boerner Horvath, Calderon, Carrillo, Cervantes, Chau, Chen, Chiu, Choi, Cooley, Cooper, Cunningham, Megan Dahle, Daly, Davies, Flora, Fong, Friedman, Gabriel, Gallagher, Cristina Garcia, Eduardo Garcia, Gipson, Lorena Gonzalez, Gray, Grayson, Holden, Irwin, Jones-Sawyer, Kalra, Kiley, Lackey, Lee, Levine, Low, Mathis, Mayes, McCarty, Medina, Mullin, Muratsuchi, Nazarian, Nguyen, O'Donnell, Patterson, Petrie-Norris, Quirk, Quirk-Silva, Ramos, Reyes, Luz Rivas, Robert Rivas, Rodriguez, Blanca Rubio, Salas, Santiago, Seyarto, Smith, Stone, Ting, Valladares, Villapudua, Voepel, Waldron, Ward, Akilah Weber, Wicks, Wood, Rendon

NO VOTE RECORDED: Burke, Frazier, Maienschein

Prepared by: Christian Kurpiewski / JUD. / (916) 651-4113
8/28/21 11:14:29

**** END ****