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

SB 41 (Umberg)
Version: December 7, 2020
Hearing Date: March 9, 2021
Fiscal: Yes
Urgency: Yes
CK

SUBJECT

Privacy: genetic testing companies

DIGEST

This bill establishes the Genetic Information Privacy Act, providing additional protections for genetic data by regulating the collection, use, maintenance, and disclosure of such data.

EXECUTIVE SUMMARY

Current law fails to provide adequate guidelines for what can be done with genetic data collected by companies outside of the protective ambit of state and federal health privacy laws. This bill fills the gap by creating the Genetic Information Privacy Act.

The bill safeguards the privacy, confidentiality, security, and integrity of a consumer's genetic data by requiring direct-to-consumer genetic testing companies ("DTC company") to provide clear disclosures and more consumer control. It also requires these companies to obtain express consent for the collection, use, and disclosure of the consumer's genetic data, including separate and express consent for specified actions. This bill mandates certain security measures and prohibits discrimination against consumers for exercising these rights. This bill subjects negligent and willful violations to varying ranges of civil penalties.

The bill is author sponsored and is supported by the University of California, genetic testing sites, and privacy and consumer protection groups. TechNet is in opposition. A previous version of the bill passed the Legislature in 2020, but was ultimately vetoed by Governor Newsom. This is an urgency measure that will take immediate effect if signed into law.

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) Specifies, through the federal Health Insurance Portability and Accountability Act (HIPAA), privacy protections for patients' protected health information and generally prohibits a covered entity, which includes a health plan, health care provider, and health care clearing house, from using or disclosing protected health information except as specified or as authorized by the patient in writing. (45 C.F.R. Sec. 164.500 et seq.)

3) Prohibits, under California's Confidentiality of Medical Information Act (CMIA), providers of health care, health care service plans, or contractors, as defined, from sharing medical information without the patient's written authorization, subject to certain exceptions. (Civ. Code Sec. 56 et seq.)

4) Subjects any provider of health care, a health care service plan, pharmaceutical company, or contractor, who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of written or electronic medical records, to damages in a civil action or an administrative fine, as specified. (Civ. Code Sec. 56.36.)

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

6) Prohibits, pursuant to federal law under the Genetic Information and Nondiscrimination Act (GINA), discrimination in group health plan coverage and employment based on genetic information. (Pub. Law 110-233.)

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

8) 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.)

9) Provides, pursuant to the CCPA, consumers the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, provide certain disclosures to the consumer. (Civ. Code § 1798.115.) It further enables a consumer, at any time, to restrict a business from selling that personal information to third parties. (Civ. Code § 1798.120.)

This bill:

1) Creates the Genetic Information Privacy Act to protect consumers' "genetic data," which is defined as any data, regardless of its format, that results from the analysis of a biological sample from a consumer, or from another element enabling equivalent information to be obtained, and concerns genetic material, except deidentified data, as provided.

2) Regulates direct-to-consumer genetic testing companies ("DTC company"), which are defined as entities that do either of the following:

    a. Sell, market, interpret, or otherwise offer consumer-initiated genetic testing products or services directly to consumers; or
    b. Analyze genetic data obtained from a consumer, except to the extent that the analysis is performed by a person licensed in the healing arts for diagnosis or treatment of a medical condition.

3) Requires a DTC company, or any other company that collects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service or directly provided by a consumer to provide clear and complete information regarding the company's policies and procedures for the collection, use, maintenance, and disclosure, as applicable, of genetic data by making certain disclosures available to a consumer.

4) Requires the above companies to also obtain a consumer's express consent for collection, use, and disclosure of the consumer's genetic data and methods to revoke such consent, as specified. DTC companies must secure separate and express consent for specified actions.

5) Provides that the requirement for separate and express consent for marketing does not require a DTC company to obtain a consumer's express consent to market to the consumer on the company's own website or mobile application, as specified.

6) Requires a DTC company, or any other company that collects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service, or provided directly by a consumer, to implement and maintain reasonable security procedures and practices. Such companies must

also develop procedures and practices to enable a consumer to easily access their genetic data, delete the consumer's account and genetic data, except as specified, and have the consumer's biological sample destroyed.

7) Prohibits these companies from disclosing a consumer's genetic data to any entity that is responsible for administering or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment, or to any entity that provides advice to an entity that is responsible for performing those functions, except as provided.

8) Prohibits discrimination by a person or public entity against a consumer based on the consumer's exercise of rights, as provided.

9) Exempts application of its provision to certain medical information, health care providers, other covered entities and their business associates. It also does not apply to scientific research or educational activities conducted by a public or private nonprofit postsecondary educational institution or the California newborn screening program.

10) Provides relevant definitions for the terms included therein, including "affirmative authorization," "express consent," and "service provider."

11) Provides that the disclosure of genetic information pursuant to this chapter shall comply with all applicable state and federal laws for the protection of privacy and security.

12) Subjects a company in violation of its provisions to specified civil penalties.

COMMENTS

1. Protecting the information most personal to individuals

The sudden rise of DNA testing, through self-administered testing kits sold by companies such as Ancestry.com or 23andMe, has made headlines. However, as people line up to find out more about their family history or their "genetic ethnicity," serious concerns about the privacy of the information have arisen. The New York Times lays out the issues:

> Home DNA testing kits usually involve taking a cheek swab or saliva sample and mailing it off to the company. In that little sample is the most personal information you can share: your genetic code. Some companies share that data with law enforcement, and most sell your DNA data to third parties, after which it can become difficult to track. For some people

> who work for small companies or serve in the military, it can affect insurance premiums and even the ability to get insurance at all.
>
> While DNA testing has been used in medical and scientific contexts for decades, direct-to-consumer testing kits are still relatively new and legal policies that govern the private use of consumer data are still being developed.
>
> According to Dr. James Hazel, a postdoctoral fellow at the Center for Genetic Privacy and Identity in Community Settings, there are fewer protections for your data with consumer DNA testing kits than there would be if you were taking a medical test. If a doctor takes a DNA sample, that sample is protected by the Health Insurance Portability and Accountability Act [(HIPAA)] and there are limits on how it can be shared.
>
> "In the United States, if you're talking about genetic data that's generated outside of the health care setting, there's a relatively low baseline of protection," Dr. Hazel said. "And that's provided generally [] by the Federal Trade Commission. So the Federal Trade Commission, although it's not specific to genetic data, has the ability to police unfair and deceptive business practices across all industries. Other than that, there are really no laws in the United States that apply specifically."[1]

As referenced, HIPAA only applies to covered entities or business associates of those entities. The genetic testing companies at issue here fall outside its bounds. Similar to HIPAA, California's Confidentiality of Medical Information Act (CMIA) protects patient confidentiality and provides that medical information may not generally be disclosed by providers of health care, health care service plans, or contractors without the patient's written authorization. (Civ. Code Sec. 56 et seq.) However, also similar to HIPAA, the sensitive genetic information being collected and the DNA testing companies collecting and selling it largely operate outside the bounds of these medical privacy laws.

At the federal level, the Genetic Information Nondiscrimination Act of 2008 (GINA) addresses discrimination based on genetic information. (42 U.S.C. § 2000ff et seq.) However, the law does not holistically protect against widespread collection, dissemination, and use of such information. For instance, GINA makes it an unlawful employment practice for an employer to request, require, or purchase genetic information of employees or their families. However, there are enumerated exceptions

---

[1] Eric Ravenscraft, *How to Protect Your DNA Data Before and After Taking an at-Home Test* (June 12, 2019) New York Times, https://www.nytimes.com/2019/06/12/smarter-living/how-to-protect-your-dna-data.html [as of February 19, 2021]. All further internet citations are current as of February 19, 2021.

and the restriction does not apply to private employers with less than 15 employees. Furthermore, the law does not even restrict discriminatory use of the information in many insurance categories. This is not to mention the fact that it does nothing to restrict the consumer genetic testing companies from collecting the information and selling it to third parties.

2. Establishing protections at the state level

California built on existing protections by enacting SB 559 (Padilla, Ch. 261, Stats. 2011). SB 559 expanded the prohibited bases of discrimination under the Unruh Civil Rights Act and the California Fair Employment and Housing Act to include genetic information.

Bills in successive sessions, SB 1267 (Padilla, 2012) and SB 222 (Padilla, 2014) sought to further expand on this by creating the Genetic Information Privacy Act. The bills would have explicitly deemed genetic test information protected by the right of privacy pursuant to the California Constitution. They would have further prohibited a DNA sample from being obtained or analyzed without the written authorization of the individual to whom the DNA sample pertains. The bills laid out a series of elements that would have been required in the authorization, including that it be written in plain language, that it specify the authorized purposes for which the DNA sample was being collected and the persons authorized to collect the sample and to receive the test results.

According to this Committee's analyses, the effort was an early response to the rise of direct-to-consumer genetic testing and its attendant privacy concerns. It highlighted concerns found by the United States Government Accountability Office (GAO) that called into question the validity of these tests and the potentially deceptive practices of the companies.[2]

3. Genetic Information Privacy Act

Although SB 1267 and SB 222 failed passage, the concerns with such tests have not abated. In December 2019, a memo issued by United States Department of Defense officials concerning DNA testing kits was obtained and reported on by news media.[3] In it, Under Secretary of Defense for Intelligence Joseph Kernan, and James Stewart, acting Under Secretary of Defense for Personnel and Readiness, laid out a series of warnings about the tests and the information they collected. The memo called into question the validity of the testing, asserted that certain military members were being targeted by the companies, and warned of nefarious efforts to exploit the sensitive information

[2] GAO, *Direct-to-Consumer Genetic Tests: Misleading Test Results are Further Complicated by Deceptive Marketing and Other Questionable Practices* (Jul. 22, 2010), https://www.gao.gov/assets/130/125079.pdf.
[3] 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.

being collected. The memo stated: "Moreover, there 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." The officials authoring the memo instructed military personnel to refrain from using the testing kits.

In response, SB 980 (Umberg, 2020) was introduced last year attempting to finally establish the Genetic Information Privacy Act. SB 980 was nearly identical to the current bill and passed through both houses of the Legislature. However, it was vetoed by Governor Newsom. He shared his reasoning in his veto message:

> This bill would establish requirements for direct-to-consumer genetic testing companies, providing opt-in privacy rights and protections for consumers.
>
> I share the perspective that the sensitive nature of human genetic data warrants strong privacy rights and protections.
>
> However, the broad language in this bill risks unintended consequences, as the "opt-in" provisions of the bill could interfere with laboratories' mandatory requirement to report COVID-19 test outcomes to local public health departments, who report that information to the California Department of Public Health. This reporting requirement is critical to California's public health response to the COVID-19 pandemic, and we cannot afford to unintentionally impede that effort.
>
> Because I agree with the primary goal of this bill, I am directing the California Health and Human Services Agency and the Department of Public Health to work with the Legislature on a solution that achieves the privacy aims of the bill while preventing inadvertent impacts on COVID-19 testing efforts.

This bill again seeks to enact California's Genetic Information Privacy Act. Similar to the earlier attempts in SB 1267 and SB 222, this bill attempts to protect the sensitive information being collected by DTC companies by attaching a series of requirements to the collection, use, maintenance, and disclosure of genetic data. These companies are required to provide clear and complete information regarding the company's policies and procedures by making certain information available to consumers. First, they are required to provide a plainly written summary of their privacy practices and a prominent and easily accessible privacy notice that includes information about the company's data collection, consent, use, access, disclosure, maintenance, transfer, security, and retention and deletion practices. They must also clearly indicate how to file a complaint alleging a violation of the act. Consumers must be notified that their deidentified genetic or phenotypic information may be shared with or disclosed to third

parties for research purposes, as such exemptions are written in to the definition of "genetic data."

In addition to the above, the bill requires DTC companies to obtain a consumer's *express* consent to the collection, use, and disclosure of the consumer's genetic data. The bill includes a robust definition for "express consent" that ensures meaningful consumer control. This is all the more significant because many companies deploy methods to undermine truly informed consent. In fact, a term has been coined to describe this, and other troubling techniques, "dark patterns."[4] The term describes elements of technical design that erode user control and privacy and ultimately hinder data protection. United States Federal Trade Commissioner Rohit Chopra explains it:

> Dark patterns are design features used to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often harmful to users or contrary to their intent. Since Harry Brignull first coined the phrase in 2010, researchers have identified a wide variety of dark patterns – each one aimed at a nefarious outcome that almost certainly could not be achieved without deception.
>
> Dark patterns are the online successor to decades of dirty dealing in direct mail marketing. Scams by mail have never gone away, but they have been eclipsed by digital deception, often using dark patterns. But, because dark patterns are not limited by physical constraints and costs, these digital tricks and traps pose an even bigger menace than their paper precursors.
>
> Typically, digital tricks and traps work in concert, and dark patterns often employ a wide array of both. Dark pattern tricks involve an online sleight of hand using visual misdirection, confusing language, hidden alternatives, or fake urgency to steer people toward or away from certain choices. This could include using buttons with the same style but different language, a checkbox with double negative language, disguised ads, or time pressure designed to dupe users into clicking, subscribing, consenting, or buying.[5]

In order to ensure more meaningful control and informed decision making, the bill requires a consumer's affirmative authorization in response to a "clear, meaningful, and prominent notice" regarding the relevant actions taken with the genetic data and the specific purpose for it. Securing express consent also requires DTC companies to communicate in "clear and prominent terms" the nature of the data collection, use,

---

[4] Thomas Germain, *How to Spot Manipulative "Dark Patterns" Online* (January 30, 2019) Consumer Reports, https://www.consumerreports.org/privacy/how-to-spot-manipulative-dark-patterns-online/.
[5] *Statement of Rohit Chopra* (September 2, 2020) United States Federal Trade Commission, https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.

maintenance, or disclosure such that "an ordinary consumer would notice and understand it." Further strengthening this concept are provisions that rule out inferring consent from inaction and specifically call out the use of dark patterns to obtain it. The bill defines the term to mean "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice."

To avoid the notorious dark pattern of securing consent through an easily accessible method but then hiding the process for revocation of that consent or limiting it to an entirely different medium, the bill requires these companies to provide effective mechanisms, without any unnecessary steps, for a consumer to revoke consent after it is given and specifically mandates that at least one of the mechanisms must utilize "the primary medium through which the company communicates with consumers." To further ensure consumers maintain control over their sensitive data, the bill requires DTC companies to develop procedures and practices to enable a consumer to easily access and delete their genetic data and account. To prevent any retaliation or other adverse consequences, the bill prohibits discrimination against consumers based on their exercise of these rights.

Furthermore, to avoid another dark pattern involving a company securing consent in a single instance for a broad array of purposes, the obligation for securing consent in the bill includes the requirement that these companies, at a minimum, secure *separate* and express consent for each of the following:

- the use of the genetic data collected through the genetic testing product or service offered to the consumer, including who has access to genetic data, and how genetic data may be shared, and the specific purposes for which it will be collected, used, and disclosed;
- the storage of a consumer's biological sample after the initial testing requested by the consumer has been fulfilled;
- each use of genetic data or the biological sample beyond the primary purpose of the genetic testing or service and inherent contextual uses;
- each transfer or disclosure of the consumer's genetic data or biological sample to a third party other than to a service provider, including the name of the third party to which the consumer's genetic data or biological sample will be transferred or disclosed; or
- the marketing or facilitation of marketing to a consumer based on the consumer's genetic data or the marketing or facilitation of marketing by a third party based upon the consumer having ordered, purchased, received or used a genetic testing product or service.

Regarding consent for marketing, the bill does not require such separate express consent when the marketing is contained to the DTC's own platform so long as the content of the marketing does not utilize information specific to that consumer, except

for that information related to the relevant products or services of the DTC. However, the bill still restricts placement of advertisements based on specified characteristics. In addition, the bill exempts certain third parties from these requirements, including academic institutions for research or educational activities.

Unlike SB 980, the bill specifically excludes private institutions "contracted with the State of California for the purposes of public health testing or reporting during a declared pandemic of State of Emergency." This broad carve out has raised some concerns. A coalition of privacy, consumer protection, and civil liberties groups, including ACLU and the Consumer Federation of America, have requested the removal of this provision. Although supportive of the bill otherwise, they argue the provision creates "a troubling loophole in these protections," and take a support if amended position. Writing in support, Consumer Reports also highlights concerns with the only provision of the bill not included in SB 980. It encourages the author "to tighten the exemption for companies with state public health testing contracts so that they are prevented from engaging in secondary use and disclosure of this information." In response, the author has agreed to remove this provision.

Amendment

Remove Section 56.181(a)(2)(G)

To protect consumers' genetic data from being compromised or used against the consumer's interests, DTC companies are also required to implement and maintain reasonable security procedures and practices and are prohibited from disclosing a consumer's genetic data to various entities, including those responsible for administering or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment, except under certain conditions.

Negligent and willful violations of this provision are subject to varying ranges of civil penalties, up to $10,000 for willful violations. The bill includes language mirroring that of Business and Professions Code Section 17204:

> Actions for relief pursuant to this chapter shall be prosecuted exclusively in a court of competent jurisdiction by the Attorney General or a district attorney or by a county counsel authorized by agreement with the district attorney in actions involving violation of a county ordinance, or by a city attorney of a city having a population in excess of 750,000, or by a city attorney in a city and county or, with the consent of the district attorney, by a city prosecutor in a city having a full-time city prosecutor in the name of the people of the State of California upon their own complaint or upon the complaint of a board, officer, person, corporation, or association, or by a person who has suffered injury in fact and has lost money or property as a result of the violation of this chapter.

In order to make the injured party whole, any penalties recovered, regardless of the party bringing suit, are to be paid to the individual to whom the genetic data at issue pertains, with recovered court costs going to the party ultimately prosecuting the action.

4. Stakeholder positions

According to the author:

> The Pentagon has asked service members to not use direct-to-consumer genetic testing companies (DTCs) due to "the increased concern in the scientific community that outside parties are exploiting the use of genetic materials for questionable purposes … without their (consumers') authorization or awareness." Furthermore, a study reported by Business Insider showed that 40 to 60 percent of genetic data is re-identifiable when compared against public databases. The evidence is clear: The laws regulating DTCs are inadequate and need to be strengthened to better protect consumers.
>
> SB 41 creates strict guidelines for authorization forms in a manner that allows consumers to have control over how their DNA will be used. Due to the fact that genetic data can be reidentified, the act also prohibits DTCs from disclosing genetic data without explicit consumer consent even if it is deidentified. In addition, this bill creates civil penalties for companies that fail to comply with the provisions within it. By passing this bill, California would be joining multiple other states that have made it clear that consumers should control their genetic data without fear of third parties exploiting it.

Writing in support, Oakland Privacy outlines the importance of taking action in this context:

> Senate Bill 41 recognizes the inter-related nature of DNA data and elevates its use threshold to an explicit consent standard that includes revocation rights, data destruction and addresses the provision of genetic data to insurance, employer, health and other bodies that potentially could base significant life outcomes on genetic information. This protects not only the source of the DNA from unintended consequences, but also their known and sometimes unknown relatives whose gene patterns are tied to their own.

Consumer Reports also writes in support of the bill, stating it will "extend important privacy protections to consumers," and highlighting the "strong definition of consent."

TechNet opposes the bill. It states that it is "concerned about the overly broad definitions in the bill which will put in scope information that in fact goes beyond actual genetic data." It also points to concerns raised in the Governor's veto message.

In response, the author has committed to working with the Governor's office and key stakeholders to ensure any concerns related to COVID-19 testing are properly addressed with thoughtful and well-tailored amendments, as necessary.

The clear intent of the bill is to further protect the privacy of consumers, with regards to this particularly sensitive category of personal information, and the protections it implements are a significant improvement on the baseline protections provided for by the CCPA, and the recently approved CPRA.

SUPPORT

23andMe
Ancestry
Coalition for Genetic Data Protection
Consumer Reports
Oakland Privacy
University of California

OPPOSITION

TechNet

RELATED LEGISLATION

Pending Legislation: AB 825 (Levine, 2021) 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. Businesses are also required to disclose a breach of genetic information. This bill is in the Assembly Privacy and Consumer Protection Committee.

Prior Legislation:

SB 980 (Umberg, 2020) *See* Comment 3.

AB 2301 (Levine, 2020) would have 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. Businesses are also required to

disclose a breach of genetic information. This bill died in the Assembly Privacy and Consumer Protection Committee.

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) expanded the definition of personal information in various consumer protection statutes to include certain additional information that is particularly sensitive but was not then explicitly included in those statutes, including biometric data and certain identification numbers.

SB 222 (Padilla, 2014) *See* Comment 2.

SB 1267 (Padilla, 2012) *See* Comment 2.

SB 559 (Padilla, Ch. 261, Stats. 2011) *See* Comment 2.

****