SENATE JUDICIARY COMMITTEE
Senator Hannah-Beth Jackson, Chair
2019-2020 Regular Session

SB 980 (Umberg)
Version: April 30, 2020
Hearing Date: May 22, 2020
Fiscal: Yes
Urgency: No
CK

SUBJECT

Privacy: DNA testing companies

DIGEST

This bill establishes the Genetic Information Privacy Act, providing additional protections for genetic data collected from individuals.

EXECUTIVE SUMMARY

Current law fails to provide adequate guidelines for what can be done with genetic information 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. It requires authorization from consumers before a direct-to-consumer genetic or illness testing services company can disclose the consumers' genetic information. It further provides measures regarding notice, proper use, retention, and destruction of this highly sensitive and highly personal information.

The bill is author sponsored and has support from privacy and consumer groups and the Center for Genetics and Society. Several additional groups have written in a support if amended position, urging the author to clarify various provisions within the bill to ensure its effectiveness in adequately securing the genetic information of all Californians.

Due to the COVID-19 Pandemic and the unprecedented nature of the 2020 Legislative Session, all Senate Policy Committees are working under a compressed timeline. This timeline does not allow this bill to be referred and heard by more than one committee, as a typical timeline would allow. In order to vet the contents of this measure for the benefit of Senators and the public, this analysis includes information from the Senate Public Safety Committee.

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) Defines, pursuant to CMIA, "medical information" as individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. (Civ. Code Sec. 56.05(g).) It further defines "individually identifiable" as medical information that includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. (Civ. Code Sec. 56.05(g).)

5) 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.)

6) 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.)

7) 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.)

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

9) 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.)

10) 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.

2) Prohibits a direct-to-consumer genetic or illness testing services company, or contractor or other service provider, that obtains a DNA sample of an individual from disclosing any of the individual's genetic information, whether or not it is deidentified, to a third party without obtaining the prior written consent of the individual. It subjects a company in violation of this provision to specified civil and criminal penalties.

3) Requires certain disclosure forms to be provided to individuals in connection with the collection and testing of their genetic information.

4) Places certain restrictions and obligations on any person who obtains, analyzes, retains, or discloses the genetic information of an individual.

5) Requires a direct-to-consumer genetic or illness testing services company to verify genetic data files that are downloaded from its databases before they are transferred or uploaded to another direct-to-consumer genetic or illness testing services company's database. It subjects those in violation to criminal penalties.

6) Clarifies that it does not apply to protected health information that is collected by a covered entity or business associate governed by the privacy, security, and

breach notification rules issued by the United States Department of Health and Human Services (Parts Regulations) 160 and 164 of Title 45 of the Code of Federal Services (Parts Regulations) established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the federal Health Information Technology for Economic and Clinical Health Act (Public Law111-5).

7) Provides relevant definitions for the terms included therein, including "genetic information," "personal information," "deidentified information," and "genetic or illness test."

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 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.

In enacting SB 559 (Padilla, Ch. 261, Stats. 2011), California built on these protections by expanding 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 build 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

---

[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 May 16, 2020]. All further internet citations are current as of May 16, 2020.

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]

Although the bills 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 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.

The improper use and disclosure of this information can have serious consequences for consumers. Writing in support of this bill, Consumer Reports illustrates the potential impacts:

> [A]ccess to life, disability, and long-term care insurance can be impacted by the results of genetic testing.[4] Genetic information gathered by DTC genetic companies can be shared with or sold to third parties, with no disclosure to the consumer. Further, in a survey of DTC genetic testing companies, 71% percent of companies could use consumer information internally for purposes other than providing the results to consumers.[5]

This bill again seeks to enact California's Genetic Information Privacy Act.

---

[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.
[4] Catherine Roberts, *Should You Give the Gift of a Genetic Testing Kit?*, Consumer Reports (Dec. 16, 2019), https://www.consumerreports.org/genetic-testing/should-you-give-the-gift-of-a-genetic-testing-kit/.
[5] James W. Hazel and Christopher Slobogin, *Who Knows What, and When: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies*, 28 CORNELL J.L. & PUB POL'Y at 52 (2018).

2. 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 direct-to-consumer genetic testing companies. The bill prohibits any direct-to-consumer genetic or illness testing services company ("DTC company") that obtains a DNA sample of an individual from disclosing any of the individual's genetic information to a third party without obtaining the prior written consent of the individual. The bill requires separate authorizations for each disclosure. The bill also prescribes specific elements of the written authorization intended to ensure individuals are able to read and understand it.

Negligent and willful violations of this provision are subject to varying ranges of civil penalties, which may be sought by the Attorney General or other specified governmental entities. Individuals harmed by violations are unable to bring their own actions, and some stakeholders have written to encourage the author to consider including a consumer enforcement mechanism. In its letter of support, Oakland Privacy argues for a stronger enforcement model, asserting it has "difficulty imagining what might entitle a private right to legal action more than the loss of control of one's own DNA patterns to an unscrupulous agent." It should be noted that the civil penalty provisions do make clear that any costs and penalties assessed are to be paid to the individual to whom the relevant genetic information pertains.

Willful violations of the above provision that result in harm to certain individual consumers are also guilty of a misdemeanor punishable by fine of up to $10,000 and/or imprisonment for up to six months. Various groups have expressed concern about these latter penalties, arguing against making violations a criminal matter. This penalty provision of the bill is within the jurisdiction of the Senate Public Safety Committee. Senate Public Safety Committee staff note: "This bill has a misdemeanor with up to 6 months in county jail and/or a fine of $10,000. Because an approximately 310% penalty assessment is added to every criminal fine, a $10,000 fine is actually closer to $41,000." They present the question of whether a criminal penalty is appropriate for these violations. In response, the author has agreed to remove subdivision (d) of Section 56.20, as well as Section 56.21, removing all criminal penalties from the bill. In order to ensure adequate penalties for willful violations in the absence of criminal penalties, the author is amending the bill to increase the maximum civil penalty provided for in subdivision (c) of Section 56.20 for willful violations from $5000 to $10,000.

Section 56.20(h)(2) of the bill includes the following provision, with a subsequent model form included:

> Any person who obtains, analyzes, retains, or discloses the genetic information of an individual shall use the following written form, to the extent that the form is applicable to the services it provides, to obtain the authorization of the individual to whom the information pertains as

> required by subdivision (a) so that the individual may make a decision and provide direction regarding the use of their genetic information:

The form ensures individuals are given clear and thorough notice as to what will be done with their information, including the purposes it is being collected for, whether the information will remain identifiable, and how it will be stored. In addition, the form provides individuals a large measure of control over their personal information. This includes the ability to limit the purposes for which the information is used and the universe of people who will have access to it. These protections are important because they build on and supplement the protections provided for in the CCPA, which only provides an opt-out mechanism for the sale of personal information.

The Electronic Frontier Foundation (EFF) highlights that this provision does not directly target DTC companies, but focuses on "[a]ny person who obtains, analyzes, retains, or discloses the genetic information of an individual." They argue more clarity is needed from a compliance standpoint. The author may wish to elaborate on exactly who is encompassed by this phrase, but it is arguably sound policy to ensure that these privacy protections are broadly applicable. A discussion of the parameters of who is covered by the bill and the precision of other definitions is below.

This same language is used in subdivision (i) of Section 56.20, placing requirements on such persons to timely destroy the genetic information and DNA samples, to permit individuals to restrict access to the information and revoke any previous authorization, and to provide the individual with a copy of any authorization upon request. It further restricts such persons from obtaining, analyzing, retaining, or disclosing the genetic information of individuals for any purpose other than the purposes authorized. These are strong privacy protections that again empower individuals to have more control over their highly sensitive genetic information.

The bill also requires DTC companies to provide individuals with a written or electronic form enabling them to opt out of any further use of their genetic information for any purpose when the company provides that person genetic or illness test results. This again places more control in the hands of individuals. One consideration highlighted by stakeholders is the manner of form required. Many DTC companies provide results electronically and that may be the primary form of communication between the two. The author may wish to consider requiring a form for opting out that matches the primary manner of communication between the parties.

Section 56.21 of the bill requires DTC companies to "verify genetic data files that are downloaded from its databases before they are transferred or uploaded to another direct-to-consumer genetic or illness testing services company's database." Violations of this provision are subject to criminal penalties. Amendments removing this provision are discussed below.

Finally, Section 56.22 makes clear that all disclosures of genetic information pursuant to the bill "comply with all state and federal laws for the protection of privacy and security." In order to avoid confusion and interference with federal law, the section also provides that the Genetic Information Privacy Act does not apply to protected health information collected by covered entities or business associates that are governed by specified federal law, including federal regulations promulgated pursuant to HIPAA and the federal Health Information Technology for Economic and Clinical Health Act.

3. Ensuring the important goals of the Genetic Information Privacy Act are effectuated

According to the author:

> The Pentagon recently sent out a memo asking service members to not use 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 980 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 DTC from disclosing genetic data without explicit consent even if it is deidentified. In addition, this bill creates civil penalties for companies that fail to comply with the provisions within it. Therefore, 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.

Various stakeholders write in support of the bill, echoing its critical importance. Consumer Reports supports the bill "because it would strengthen privacy protections to uniquely sensitive personal information collected by direct-to-consumer (DTC) genetic testing companies. It writes:

> This bill will ensure that genetic information remains confidential by providing detailed requirements to allow for authorization to disclose the information to specific recipients, and appropriately limits the ways in which companies can use this information.
>
> With increasing developments of at-home healthcare solutions, testing, and products, it is important to ensure that our laws protect consumers in the rapidly changing market. Currently, no federal law directly addresses consumer privacy issues resulting from DTC genetic testing. While the

> California Consumer Privacy Act gives consumers the right to opt out of the sale of this information, this protection kicks in only after the consumer takes action. As a result, by default, DTC genetic testing companies can do whatever they want with consumers' most personal information.
>
> . . . By curbing unauthorized disclosure and curbing secondary uses of this sensitive data, this bill would extend important privacy protections to consumers.

The Consumer Federation of California writes in support of the bill, highlighting the "increasing scientific concern that this data could be used for surveillance purposes or to otherwise exploit one's unique genetic make-up." It argues the bill ensures "that consumers will explicitly and affirmatively 'opt-in' to have their genetic information disclosed should they make that personal choice."

The Center for Genetics and Society also support the measure, stressing that "[i]n the absence of Federal legislation, it is incumbent on the States to take the lead on this increasingly important issue."

Writing in support, Oakland Privacy outlines the importance of taking action in this context and highlights the possible misuse of this data in the law enforcement context. It writes:

> The use of DNA by law enforcement to pursue long-cold cases has received much publicity and, when used with restraint, may sometimes function as a genetic "lineup" for criminal identification purposes. However, as with the jailhouse version, the individuals providing the backdrop have consented to participating or are already in law enforcement custody, and the shift to an electronic search should not place anyone, much less 26 million people in a perpetual DNA lineup for life without their permission.

The letter highlights a particularly disturbing example where one of the largest DTC companies, FamilyTreeDNA, was found to have been sharing the genetic information of its millions of customers with federal law enforcement, including analyzing DNA samples in its lab on law enforcement's behalf, all without the consent of its customers and without any disclosures to them and without the existence of a subpoena or warrant for the information.[6]

---

[6] Matthew Haag, *FamilyTreeDNA Admits to Sharing Genetic Data With F.B.I.* (February 4, 2019) The New York Times, https://www.nytimes.com/2019/02/04/business/family-tree-dna-fbi.html [as of May 16, 2020].

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. However, a number of concerns have arisen about exactly what the scope of the bill is. Many of these issues center around the definitions of the terms included within the bill. As highlighted above, the main target of this legislation are DTC companies; however, certain provisions apply to a person "who obtains, analyzes, retains, or discloses the genetic information of an individual." As argued by EFF, this ambiguity puts in doubt whether "the duties on entities are sufficiently clear from a compliance standpoint." Another example of this is where the form requires notice as to whether the genetic information will remain "identifiable." This term is not used elsewhere within the bill and it is unclear how it may differ from "deidentified" information, which is defined.

In addition, Section 56.21 requires a DTC company to "verify" genetic data files. However, there is no definition for what this entails and what would be sufficient to meet this requirement. Without more clarity, this requirement could lead to litigation despite a company's best efforts to comply.

Another example is presented by the Coalition for Genetic Data Protection (CGDP). Recent amendments include "illness testing" in the scope of the services to be covered by the bill, a clear attempt to address commercial COVID-19 testing. However, CGDP argues that, as currently crafted, the language within the bill does not accomplish this goal:

> Any test that is designed to detect the presence of COVID-19 would be, by definition, looking for genetic information or material that is not human and does <u>not</u> belong to the individual tested. All of the available COVID-19 tests detect the presence of RNA from the SARS-Cov-2 virus itself – genetic information which belongs to a *foreign pathogen*. While our Coalition is unaware of any legally marketed direct-to-consumer COVID-19 testing at this time, we maintain that the current definitions in the bill would not capture a direct-to-consumer COVID-19 test even if the FDA approved one.

CGDP further argues that the definition used for "genetic data" is antiquated and encourages the author to substitute a more expansive definition.

Another area that could benefit from greater clarity is the remedies provisions. For instance, Section 56.20 (b) and (c) provide for civil penalties, but only in connection with violations of Section 56.20 (a). It is unclear whether a failure to provide the opt-out form required in Section 56.20(g) or the written form required in Section 56.20(h)(2) is subject to those civil penalties.

In response, the author has committed to work with stakeholders and the Committee to hone the definitions and make clear who is encompassed by each provision in order to ensure that the bill effectively carries out its stated intention. The author has further agreed to take the following amendments that remove Section 56.21 and that apply the civil-penalties provisions to all violations of the bill.

4. Amendments

Replace "subdivision (a)" with "this chapter" in Section 56.20(b) and (c)

Replace "five thousand dollars ($5,000)" with "ten thousand dollars ($10,000)" in Section 56.20(c)

Remove Section 56.20(d)

Replace "section" with "chapter" in Section 56.20(f)

Remove Section 56.21

SUPPORT

Center for Genetics and Society
Consumer Federation of California
Consumer Reports
Oakland Privacy

OPPOSITION

None known

RELATED LEGISLATION

Pending: AB 2301 (Levine, 2020) 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:

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 1.

SB 1267 (Padilla, 2012) *See* Comment 1.

SB 559 (Padilla, Ch. 261, Stats. 2011) *See* Comment 1.

****