

Date of Hearing: July 13, 2021

ASSEMBLY COMMITTEE ON JUDICIARY
Mark Stone, Chair
SB 41 (Umberg) – As Amended June 17, 2021

SENATE VOTE: 38-0

SUBJECT: PRIVACY: GENETIC TESTING COMPANIES

KEY ISSUE: SHOULD THE LEGISLATURE ENACT THE GENETIC INFORMATION PRIVACY ACT WHICH PROVIDES ADDITIONAL PROTECTIONS AND ENFORCEMENTS FOR REGULATING THE COLLECTION, USE, MAINTENANCE, AND DISCLOSURE OF GENETIC DATA COLLECTED OR DERIVED FROM A DIRECT-TO-CONSUMER GENETIC TESTING PRODUCT OR SERVICE?

SYNOPSIS

Consumers that use direct-to-consumer (DTC) genetic testing generate highly sensitive data about themselves and their biological relatives. Current law fails to provide adequate guidelines for what can be done with genetic information collected by companies outside of the current protective state and federal health privacy laws. Further, despite current laws on discrimination and limited use of genetic information, an individual's most personal information is still being bought, sold, and traded without clear understanding or consent from the consumer.

This bill aims to address this issue by creating the Genetic Information Privacy Act. This bill adds necessary safeguards for the privacy, confidentiality, security, and integrity of a consumer's genetic data by requiring DTC genetic testing companies to provide clear disclosures. 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 further mandates certain security measures and prohibits discrimination against consumers for exercising these rights. Finally, this bill subjects negligent and willful violations to varying ranges of civil penalties

The bill is supported by various privacy and consumer groups, and companies including Ancestry, 23andme, Consumer Reports, and Oakland Privacy. This bill is opposed unless amended by TechNet who argue that they are concerned about the overly broad definitions in the bill which would include information that goes beyond actual genetic data and could add complex challenges as it relates to workplace safety.

SUMMARY: Establishes the Genetic Information Privacy Act which provides additional protections regulating the collection, use, maintenance, and disclosure of genetic data collected or derived from a direct-to-consumer (DTC) genetic testing product or service, including enhanced notice and opt-in consent requirements. Specifically, **this bill:**

1) Finds and declares that:

- a) Direct-to-consumer genetic testing services are largely unregulated and could expose personal and genetic information, and potentially create unintended security consequences and increased risk.

- b) There is growing concern in the scientific community that outside parties are exploiting the use of genetic data for questionable purposes, including mass surveillance and the ability to track individuals without their authorization.
 - c) Genomic data is highly distinguishable. There is a confirmation that a sequence of 30 to 80 single nucleotide polymorphisms could uniquely identify an individual. Genomic data is also very stable. It undergoes little change over the lifetime of an individual and thus has a long-lived value, as opposed to other biometric data such as blood tests, which have expiry dates.
 - d) The potential information hidden within genomic data is cause for significant concern. As our knowledge in genomics evolves, so will our view on the sensitivity of genomic data.
- 2) Establishes the Genetic Information Privacy Act and defines the following terms: affirmative authorization, biological sample, consumer, dark pattern, deidentified data, direct-to-consumer genetic testing company, express consent, genetic data, genetic testing, person, and service provider.
- 3) Requires a DTC genetic testing company 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, including all of the following:
- a) A summary of its privacy practices, written in plain language;
 - b) A prominent and easily accessible privacy notice that includes, at a minimum, complete information about the company's data collection, consent, use, access, disclosure, maintenance, transfer, security, and retention and deletion practices, as well as information clearly describing how to file a complaint alleging a violation of the provisions of the bill; and
 - c) A notice that the consumer's deidentified genetic or phenotypic information may be shared or disclosed to third parties for research purposes in accordance with the federal policy for the protection of human subjects (i.e., "The Common Rule").
- 4) Requires a DTC genetic testing company to obtain a consumer's express consent for the collection, use, and disclosure of the consumer's genetic data, including, at a minimum, separate express consent for each of the following:
- a) 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, how genetic data may be shared, and the specific purposes for which it will be collected, used, and disclosed;
 - b) The storage of a consumer's biological sample after the initial testing requested by the consumer has been fulfilled;
 - c) Each use of genetic data or the biological sample beyond the primary purpose of the genetic testing product or service and inherent contextual uses;

- d) Each transfer or disclosure of the consumer's genetic data or biological sample to a third party other than 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; and
 - e) The marketing or facilitation of marketing to the consumer based on the consumer's genetic data, or the marketing or facilitation of marketing by a third party based on the consumer having ordered, purchased, received or used a genetic testing product or service, except as specified.
- 5) Requires a DTC genetic testing company to implement and maintain reasonable security procedures and practices, and to develop procedures and practices to enable a consumer to access their genetic data, delete their account and genetic data, and have their biological sample destroyed.
 - 6) Requires a company subject to the consent requirements of the bill to provide effective mechanisms, without any unnecessary steps, for a consumer to revoke their consent, at least one of which utilizes the primary medium through which the company communicates with its consumers; and require a company to honor a consumer's request to revoke consent as soon as practicable, but not later than 30 days after the consumer revokes consent, in accordance with the Common Rule, and to destroy a consumer's biological sample within 30 days of receipt of the revocation of consent to store the sample.
 - 7) Prohibits a person or public entity from discriminating against a consumer because the consumer exercised any of their rights under this chapter, as specified.
 - 8) Prohibits a DTC genetic testing company from disclosing a consumer's genetic data or biological sample to any entity responsible for administering or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment, or to any entity providing advice to an entity responsible for those functions, except as specified.
 - 9) Provides that any person who negligently violates the provisions of the bill to civil penalties not to exceed \$1,000 plus court costs, as determined by the court, and any person who willfully violates the provisions of the bill to civil penalties in an amount not less than \$1,000 and not more than \$10,000 plus court costs, as determined by the court.
 - 10) Provides that the court costs recovered pursuant to enforcement of this bill shall be paid to the party or parties prosecuting the violation, and that penalties recovered shall be paid to the individual to whom the genetic data at issue pertains.
 - 11) Provides that the provisions of the bill shall be prosecuted exclusively by the Attorney General, a district attorney, a county counsel, a city attorney, a city prosecutor, as specified, in the name of the people of the State of California upon their own complaint, upon the complaint of a board, officer, person, corporation, or association, or upon the complaint of a person who has suffered injury in fact and has lost money or property as a result of the violation.
 - 12) Provides that any provision of a contract or agreement between a consumer and a person governed by the bill that has or would have the effect of delaying or limiting access to legal

remedies for violation of the bill inapplicable to the exercise of rights or enforcement pursuant to the bill.

- 13) Exclude from its provisions any medical information governed by the Confidentiality of Medical Information Act (CMIA); any protected health information that is collected, maintained, used, or disclosed by a covered entity or business associate governed by the privacy, security, and breach notification rules established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the federal Health Information Technology for Economic and Clinical Health (HI-TECH) Act; scientific research and educational activities conducted by nonprofit postsecondary educational institutions, as specified, in accordance with federal and state regulations for the protection of human subjects; tests conducted exclusively to diagnose whether an individual has a specific disease, to the extent that all persons involved in the conduct of the test maintain, use, and disclose genetic information in the same manner as medical information or protected health information; and the California Newborn Screening Program.
- 14) Clarifies that nothing in the bill shall be construed to affect access to information made available to the public by the consumer.
- 15) Provides that the provisions of this chapter are severable.

EXISTING LAW:

- 1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (California Constitution, Article. I, Section 1.)
- 2) Prohibits discrimination on the basis of genetic information under the Unruh Civil Rights Act and the Fair Employment and Housing Act (FEHA). (Civil Code Section 51; Government Code Section 12920 *et seq.*)
- 3) Prohibits, pursuant to federal law under the Genetic Information and Nondiscrimination Act (GINA), discrimination based on genetic information in group health plan coverage and employment. (Public Law 110-233.)
- 4) Subjects any person who improperly discloses genetic test results contained in a health care service plan applicant or enrollee's medical records, or pursuant to a genetic test requested by an insurer, to civil and criminal penalties. (Civil Code Section 56.17; Insurance Code Section 10149.1.)
- 5) Subjects any provider of health care, 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. (Civil Code Section 56.36.)
- 6) Specifies, under 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. Section 164.500 *et seq.*)

- 7) Prohibits, under 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. (Civil Code Section 56 *et seq.*)
- 8) Defines "medical information," for purposes of CMIA, to mean 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. (Civil Code Section 56.05(g).)
- 9) Establishes the California Consumer Privacy Act of 2018 (CCPA), which grants consumers certain rights with regard to their PI (personal information), including enhanced notice, access, and disclosure when their PI 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. (Civil Code Section 1798.100 *et seq.*)
- 10) Provides consumers the right, pursuant to the CCPA, to request that a business that sells the consumer's PI, or that discloses it for a business purpose, provide certain disclosures to the consumer, and enables a consumer, at any time, to restrict a business from selling that PI to third parties. (Civil Code Sections 1798.115 and 1798.120.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: Consumers who use direct-to-consumer (DTC) genetic testing generate highly sensitive data about themselves and their biological relatives. Current law fails to provide adequate guidelines for what can be done with genetic information collected by companies outside of the current protective state and federal health privacy laws. Further, despite current laws on discrimination and limited use of genetic information, an individual's most personal information is still being bought, sold, and traded without clear understanding or consent from the consumer. This bill aims to address this issue by creating the Genetic Information Privacy Act, which provides various safeguards and enforcement mechanisms to ensure that genetic data from a DTC genetic test is protected. The author writes in support:

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.

Background on DTC genetic testing. Genetic testing is a type of test that identifies changes in chromosomes, genes, or proteins. The results of a genetic test can confirm or rule out a suspected genetic condition or help determine a person's chance of developing or passing on a genetic disorder. Traditionally genetic testing was administered through healthcare providers. However, due to the development of DTC genetic testing, these tests are marketed directly to consumers who send their samples directly to the companies. As genetic sequencing becomes increasingly inexpensive and accessible, DTC genetic testing is becoming more ubiquitous. Businesses such as 23andMe and Ancestry.com market these products as opportunities to be knowledgeable about oneself, based on their capacity to reveal individual traits, medical predispositions, ethnicities and nations of origin, and blood relationships to others. When purchased, DTC genetic testing products provide a kit through which a sample, typically saliva, can be collected and mailed to the company for analysis. The company then provides results to the consumer, generally online, through landing pages where consumers can access their raw genetic data as well as inferences drawn from those analyses. The information that can be extrapolated or inferred from these data continues to grow each year, as the scientific understanding of genetics and genomics improves, and new uses for databases of such genetic information continue to emerge. (Consumer Reports, *Direct-to-Consumer Genetic Testing: The Law Must Protect Consumers' Genetic Privacy*, (July 2020), available at <https://advocacy.consumerreports.org/wp-content/uploads/2020/07/DTC-Genetic-Testing-White-Paper-4.pdf>.)

Background on the sensitivity and potential usage of genetic data. In April of 2018, police arrested Joseph James DeAngelo, alleging that he was the "Golden State Killer" suspected of at least 13 murders, 50 rapes, and 100 burglaries in California between 1974 and 1986. Using the killer's DNA profile collected from a rape kit, investigators submitted the killer's genetic information to GEDMatch, a freely accessible genealogical database to which users upload their genetic data received from DTC genetic tests in order to identify familial matches among other users, and identified ten to twenty relatives who shared the killer's great-great-great grandparents. Investigators then reconstructed a putative family tree using this information, ultimately identifying two prime suspects, one of which was exonerated by a family member's submitted genetic data; the other, DeAngelo, was a genetic match with the killer.

The arrest of the alleged Golden State Killer has been hailed as an exemplary use of consumer genetic data in the investigation of crimes, but it also spotlighted the issue of genetic privacy and the unforeseen uses of commercially obtained genetic data. As of 2019, over twenty-six million people had used some form of DTC genetic testing service, and that number continues to grow as new companies enter the market. (Antonio Regalado, *More than 26 Million People Have Taken an At-Home Ancestry Test*, *MIT Tech. Rev.*, (Feb. 11, 2019), available at <https://technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test>.) However, the capacity to reveal sensitive information about family members is not limited to the law enforcement. A genetic test has the potential to uncover information about biological parentage and about inherited genetic traits that could reveal sensitive health conditions of parents or other relatives. It has been demonstrated that several genes are associated with certain health conditions and behavioral traits. Unlike usernames, passwords, credit card numbers, and other identifying information often subject to data breaches, genetic data cannot be changed or removed from the individual in the event it falls into the wrong hands. As a result, it is critical that privacy and consumer protection laws are in place to ensure these data are protected from misuse.

Genetic data, privacy, and Fourth Amendment considerations. The Fourth Amendment of the United States Constitution protects against “unreasonable searches and seizures.” (U.S. Constitution, 4th Amendment.) It has been well recognized that the fundamental purpose of the Amendment is to safeguard the privacy and security of individuals against invasion by governmental officials. This principle has continued to evolve over time, and has come to protect, to some extent, individuals’ interest in their digital privacy. For example, in the 2018 case of *Carpenter v. United States*, the Supreme Court concluded that the Fourth Amendment’s protection of privacy extended to protecting some information from government intrusion even where that information was shared with a third party. (*See Carpenter v. United States* (2018) 138 S. Ct. 2206.) In *Carpenter*, the Court concluded that individuals maintain an expectation of privacy, protected by the Fourth Amendment, in the record of their movements as recorded by their cellular provider. *Carpenter* distinguished earlier cases which had relied upon the principle that information shared with third parties was generally not subject to Fourth Amendment scrutiny. (*See Katz v. United States*, (1967) 389 U.S. 347.) The Court’s holding means that, in the future, the government must obtain a warrant supported by probable cause to obtain this information.

Further, in regards to privacy of genetic data, it is not entirely clear whether genetic data can ever truly be fully deidentified. While the genetic sequence information can be separated from personal information such as an individual’s name or email address, it nonetheless provides information sufficient to specify a particular individual. Notably, the Supreme Court of California has ruled that a unique DNA profile, in the absence of a name, is sufficient to describe a particular person for the purposes of an arrest warrant, holding:

For the purposes of the Fourth Amendment, we conclude that the arrest warrant in question, which described the defendant by his 13-loci DNA profile and included an explanation that the profile had a random match probability such that there was essentially not chance of its being duplicated in the human population except in the case of genetically identical sibling [sic.], complied with the mandate of our federal constitution that the person seized be described with particularity. (*See People v. Robinson* (2010) 47 Cal. 4th 1104, 1130-1134.)

While the Fourth Amendment, which protects against Government intrusions, is not implicated by this bill, which applies to private entities, the Fourth Amendment case law does support the broader principle that people have a “reasonable expectation of privacy” in their genetic information. Currently, an individual’s rights involving privacy, focuses on public disclosure of private facts. This focus limits the potential influence on modern data privacy debates, which extends beyond the disclosure issue to more broadly concern how data is collected, protected, and used. As stated in a report to Congress by the Congressional Research Services, “[O]nly government action is subject to scrutiny under the Constitution, but purely private conduct is not proscribed, no matter how unfair that conduct may be. As a result, neither the common nor constitutional law provides a complete framework for considering many of the potential threats to digital privacy and consumer data. Rather, the most important data protection standards come from statutory law.” (*See Congressional Research Services, Data Protection Law: An Overview* (Mar. 25, 2020), available at <https://crsreports.congress.gov/product/pdf/R/R45631>, at p. 7.) In conclusion, clear statutory safeguards should be put in place to ensure Californians are guaranteed their right to privacy, especially when disclosing sensitive information such as genetic test results.

Background on current genetic privacy laws. Currently, there are very few protections provided by state and federal laws to limit the use and disclosure of the genetic data collected by DTC genetic testing companies. For example, HIPAA requires written authorization for a covered entity, including a healthcare provider, a health insurance provider, or a business associate of either, to disclose the protected health information of a patient, which may include genetic testing history and results. (45 CFR 164.500 *et seq.*) The DTC 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. (Civil Code Section 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. Further, the California Insurance Code provides these same protections with respect to disclosure of the results of a test for a genetic characteristic requested by an insurer. (Insurance Code Section 10149.1.) However, because the businesses offering DTC genetic testing are not health care service plans or insurance providers, typical protections for medical information or other protected health information do not apply to the test results.

In 2018, California enacted landmark privacy legislation, the California Consumer Privacy Act or CCPA (AB 375, Chau, Ch. 55, Stats. 2018), giving consumers certain rights regarding their personal information. The CCPA includes in its definition of personal information "biometric information," which it defines to mean "an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA) that can be used, singly or in combination with each other or with other identifying data to establish individual identity." (Civil Code Section 1798.140.) Accordingly, the protections provided by the CCPA are available with respect to genetic data maintained by a DTC genetic testing company to the extent that the data are identifiable. The CCPA also provides a private right of action in the event a consumer's nonencrypted and nonredacted PI is subject to unauthorized access, theft, or disclosure, which would apply if the unauthorized access, theft, or disclosure were the result of negligence by the business. (Civil Code Section 1798.150.)

At the federal level, the Genetic Information Nondiscrimination Act of 2008 (GINA) addresses discrimination based on genetic information. (42 U.S.C. Section 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. Further, the law does not restrict discriminatory use of the information in many insurance categories. Additionally, under the Fair Employment and Housing Act (FEHA; Government Code Section 12900 *et seq.*), California prohibits discrimination in employment and housing contexts on the basis of genetic information, and more generally prohibits discrimination based on genetic information pursuant to the Unruh Civil Rights Act (Civil Code Section 51 *et seq.*) While these prohibitions on discrimination may limit the harms of disclosure of genetic data by DTC genetic testing companies in some contexts, they do little to protect a consumer's general privacy interest in their own genetic data.

Past legislative efforts to enact stronger protections for genetic data. In 2011, the Legislature passed and the Governor signed SB 559 (Padilla, Ch. 261, Stats. 2011), which 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 introduced 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, which borrowed language from CMIA and Insurance Code provisions dealing with the disclosure of genetic information. These 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. Both of these bills died in the Senate Appropriations committee. Further, 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. The veto message and efforts to address the issues it raises will be discussed below.

This bill addresses the Governor's veto message by ensuring the provisions provided by this bill do not hinder any public health efforts. As mentioned above, SB 980 (Umberg, 2020) was introduced last year and approved by the Legislature, attempting to establish the Genetic Information Privacy Act, but was vetoed by Governor Newsom who stated in his veto message the following:

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.

To address this concern, this bill was recently amended to exempt from its provisions, "tests conducted exclusively to diagnose whether an individual has a specific disease, to the extent that all persons involved in the conduct of the test maintain, use, and disclose genetic information in the same manner as medical information or protected health information." This amendment seems to strike an appropriate balance between avoiding unforeseen obstacles to public health objectives, and ensuring that resulting genetic information is subject to some privacy protections.

This bill ensures a comprehensive framework is in place in order to protect genetic data collected, used, maintained, or disclosed by a DTC genetic testing company. Building upon past legislative efforts, 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 also be notified if their deidentified genetic or phenotypic information might 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 protections 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, which is essential because many companies deploy methods to undermine truly informed consent. In fact, a term has been coined to describe this, and other troubling techniques, known as “dark patterns.” (Thomas Germain, *How to Spot Manipulative “Dark Patterns” Online* (January 30, 2019) Consumer Reports, *available at* <https://www.consumerreports.org/privacy/how-to-spot-manipulative-dark-patterns-online/>.) Dark patterns are typically described as elements of technical design that erode user control and privacy and ultimately hinder data protection.

To avoid dark patterns, this 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 any DTC genetic testing company to develop procedures and practices to enable the consumer to access their genetic data, delete their account and genetic data, and have their biological sample destroyed. To prevent any retaliation or other adverse consequences, the bill prohibits discrimination against consumers based on their exercise of these rights.

Further, to avoid another form of dark patterns 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.

Further, to prevent the use of genetic data for potential discrimination in insurance contexts not covered by existing Insurance Code provisions, the bill prohibits a DTC genetic testing company from disclosing a consumer's genetic data to any entity responsible for administering or making decisions regarding health insurance, life insurance, long-term care insurance, disability insurance, or employment, or any entity that provides advice to an entity that is responsible for performing those functions, unless certain criteria are met to ensure that the entity does not primarily operate in the insurance space, and that any component of the entity that does manage insurance cannot access the genetic data.

In order to avoid complications resulting from inconsistencies or conflicts with existing state and federal laws, the bill excludes from its scope any medical information governed by CMIA, and protected health information that is collected, maintained, used, or disclosed by a covered entity or business associate governed by the privacy, security, and breach notification rules pursuant to HIPAA. The bill also exempts from its definition of "genetic data" data and biological samples subject to the federal policy for the protection of human subjects, otherwise known as the Common Rule, to the extent that the data are collected, used, maintained, and disclosed in compliance with the provisions of the Common Rule. This exemption would prevent logistical compliance complications for genetic researchers, since the Common Rule already includes informed consent and notice provisions, and genetic data used for this purpose would otherwise be subject to two separate, independent standards governing its use.

Finally, it should be noted that this bill does not require separate express consent process for marketing, when the marketing is placed on the DTC's own platform as 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. Further, this bill does not require the consumer's express consent, if the advertisement *is not intended to* result in disparate exposure to advertising content on the basis of any protected characteristic, as described in the Unruh Civil Rights Act (Civil Code Section 51). Demonstrating *intent* to present advertisements in a manner that discriminates based on protected characteristics for the purpose of legal action may be difficult to prove. As the Equal Justice Society, a non-profit dedicated to strengthening anti-discrimination protections, explains, "because contemporary discrimination is frequently structural in nature, unconscious, and/or hidden behind pretexts (despite the fact that a tangible harm has resulted from their actions), the showing of 'intent' becomes a near impossible burden for plaintiffs." (See Equal Justice Society, *Intent Standard*, (accessed 7/7/21), available at <https://equaljusticesociety.org/law/intentdoctrine/>.) Further, it should be noted that in cases of disparate impact, almost by definition, intent is not typically the issue at hand. Instead, it is the downstream practices that have discriminatory results that negatively affect a protected class. *The author may further wish to consider strengthening this provision to ensure that contextual advertisements do not have the purpose or effect of resulting in disparate exposure.*

The enforcement mechanisms provided under this bill. As stated above, SB 41 aims to protect consumers' genetic data from being compromised or used against the consumer's interests. In order to ensure consumers are protected, enforcement mechanisms similar to those available in the CMIA and Insurance Code provisions concerning unlawful disclosure of genetic test results, are incorporated into SB 41. This bill provides that any person who negligently or willfully violates the provisions provided under the Genetic Information Privacy Act to civil penalties, to be paid to the individual whose genetic information was affected. In the event of a negligent violation, a civil penalty of up to \$1,000 would be assessed, and in the event of a willful violation, a civil penalty of not less than \$1,000 and not more than \$10,000 would be assessed.

Further, actions for relief can only be prosecuted by the Attorney General, a district attorney, a county counsel, a city attorney, or a city prosecutor, “upon their own complaint or upon the complaint of a board, officer, person, corporation, or association, or upon a complaint by a person who has suffered injury in fact and has lost money or property as a result of the violation of the bill’s provisions. Additionally, the bill would direct the court costs recovered to the prosecuting party or parties, and the civil penalties to the individual. This would offset the cost of prosecution to the agency, and encourage enforcement. Finally, 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.

It should be noted that unlike the CMIA and Insurance Code provisions, this bill lacks a private right of action, which would arguably strengthen the protections provided by this bill. Oakland Privacy, a “citizen’s coalition that works regionally to defend the right to privacy, enhance public transparency, and increase oversight of law enforcement, particularly regarding the use of surveillance techniques and equipment,” supports this bill, but asks the Committee to consider the utility of a private right of action. Oakland privacy writes, “In our opinion, the committee and the author should also strongly consider a private right of action as we have difficulty imagining what might entitle one to a private right to legal action more than the loss of control of one’s own DNA patterns.”

The author may wish to consider adding a private right of action to ensure a robust enforcement mechanism is provided under this important bill.

ARGUMENTS IN SUPPORT: In support of this bill, various consumer and privacy protection groups as well as the Consumer Reports write in support:

We are strong proponents of public policy that bolsters consumers’ privacy and their control over who accesses their data and for what purposes. It is within this framework that we support this bill, because it would strengthen privacy protections for uniquely sensitive personal information collected by direct-to-consumer (DTC) genetic testing companies. This bill will help ensure that genetic information remains confidential by requiring consent before disclosure of this information to third parties, and by limiting the ways in which companies can use this information.

Importantly, the bill has a strong definition of consent, including a clear prohibition on deceptive interfaces known as “dark patterns,” to make sure that consumers have a meaningful choice over how their data is used. Subverting consumer intent online has become a real problem, and it’s important to address, particularly since genetic data is so sensitive. Sites often make it much easier to agree to a potential transaction than to say no, relying on consumers’ limited attention span and the habit of clicking “OK.”

ARGUMENTS IN OPPOSITION: TechNet writes in opposition unless amended that:

We understand the goal of the author is to place important protections around direct-to-consumer genetic testing data, but we are concerned about the overly broad definitions in the bill which will put in scope information that in fact goes beyond actual genetic data and could add complex challenges as it relates to workplace safety and COVID-19 protocol.

[...O]ur concern is that the latest amendments still do not address the issue we raised previously which is that “genetic data” is too broad in that it includes any data derived from results. That, in conjunction with how broadly a direct-to-consumer genetic testing company is defined, means that even a casual conversation in the workplace resulting from a test someone had taken for any genetic test will be in scope. It is certainly helpful that there is that exclusion for disease, but since the definition of genetic data includes data resulting from, etc. it goes beyond just simply the “test”. For this reason we posit, is COVID-19 considered a disease but not also considered a condition?

It should first be noted “disease” appears to be sufficient and in the case of COVID-19, the CDC defines it as “a respiratory *disease* caused by SARS-CoV-2. (See Center for Disease Control, *Coronavirus Disease 2019*, (accessed 7/7/21), available at <https://www.cdc.gov/dotw/covid-19/index.html>.) In the event these tests were used for diagnostic purposes in the workplace, the recent amendments addressing the Governor’s veto message would ensure that the provisions of the bill would not apply, as long as any genetic information is treated as medical information.

REGISTERED SUPPORT / OPPOSITION:

Support

23andme
Ancestry
Consumer Reports
Oakland Privacy
University of California

Oppose Unless Amended

TechNet

Analysis Prepared by: Mary Soliman and Thomas Clark / JUD. / (916) 319-2334