Date of Hearing: March 17, 2026
Counsel: Kimberly Horiuchi

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Nick Schultz, Chair

AB 1727 (Ta) – As Introduced February 5, 2026

As Proposed to be Amended in Committee

SUMMARY: Adds a misdemeanor penalty punishable by to one year in the county jail, fine of up to $1,000, or by both imprisonment and fine, to the Genetic Information Privacy Act (GIPA).

EXISTING LAW:

1) Creates the GIPA and defines the following terms:

   a) "Express consent" means a consumer's affirmative authorization to grant permission in response to a clear, meaningful, and prominent notice regarding the collection, use, maintenance, or disclosure of genetic data for a specific purpose. The nature of the data collection, use, maintenance, or disclosure shall be conveyed in clear and prominent terms in such a manner that an ordinary consumer would notice and understand it. Express consent cannot be inferred from inaction. Agreement obtained through use of dark patterns does not constitute consent. (Civ. Code, § 56.18, subd. (b)(6).)

   b) "Genetic data" means 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. Genetic material includes, but is not limited to, DNA, ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from the analysis of the biological sample, and any information extrapolated, derived, or inferred therefrom. (Civ. Code, § 56.18, subd. (b)(7)(A).)

   c) "Genetic data" does not include deidentified data. "Deidentified data" means data that cannot be used to infer information about, or otherwise be linked to, a particular individual, provided that the business that possesses the information does all of the following:

      i) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household;

      ii) Publicly commits to maintain and use the information only in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of GIPA, as specified, provided that the business does not use or disclose any information reidentified in this process and destroys the reidentified information upon

completion of that assessment;

iii) Contractually obligates any recipients of the information to take reasonable measures to ensure that the information cannot be associated with a consumer or household and to maintaining and using the information only in deidentified form and not to reidentify the information; and,

iv) "Genetic data" does not include data or a biological sample to the extent that data or a biological sample is collected, used, maintained, and disclosed exclusively for scientific research conducted by an investigator with an institution that holds an assurance with the United States Department of Health and Human Services, as specified. (Civ. Code, § 56.18, subd. (b)(7)(A-C).)

d) "Genetic testing" means any laboratory test of a biological sample from a consumer for the purpose of determining information concerning genetic material contained within the biological sample, or any information extrapolated, derived, or inferred therefrom. (Civ. Code, § 59.18, subd. (b)(8).)

2) Declares in order to safeguard the privacy, confidentiality, security, and integrity of a consumer's genetic data, a direct-to-consumer genetic testing company shall do both of the following:

a) 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 available to a consumer all of the following:

i) A summary of its privacy practices, written in plain language, that includes information about the company's collection, use, maintenance, and disclosure, as applicable, of genetic data;

ii) 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, and information that clearly describes how to file a complaint alleging a violation of this GIPA; and,

iii) A notice that the consumer's deidentified genetic or phenotypic information may be shared with or disclosed to third parties for research purposes in accordance with HIPAA.

b) Obtain a consumer's express consent for collection, use, and disclosure of the consumer's genetic data, including, at a minimum, separate and express consent for each of the following:

i) 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;

ii) The storage of a consumer's biological sample after the initial testing requested by the consumer has been fulfilled;

iii) Each use of genetic data or the biological sample beyond the primary purpose of the genetic testing or service and inherent contextual uses; and,

iv) 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. (Civ. Code, § 56.181, subd. (a)(1)-(2).)

3) States that a company that is subject to the requirements of the DTC rules in GIPA shall provide effective mechanisms, without any unnecessary steps, for a consumer to revoke their consent after it is given, at least one of which utilizes the primary medium through which the company communicates with consumers. (Civ. Code, § 56.181, subd. (b).)

4) Mandates if a consumer revokes the consent that they provided, the DTC DNA testing company honor the consumer's consent revocation as soon as practicable, but not later than 30 days after the individual revokes consent, as follows:

a) Revocation of consent must comply with HIPAA; and,

b) The company shall destroy a consumer's biological sample within 30 days of receipt of revocation of consent to store the sample. (Civ. Code, § 56.181, subd. (c).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Author's Statement**: According to the author, "Federal laws such as HIPAA protect Californians from the misuse of their genetic materials and information by healthcare providers, and the Genetic Information Privacy Act (GIPA) safeguards consumers from certain direct-to-consumer genetic testing companies. However, these protections leave a significant gap when it comes to private actors who collect or misuse genetic data outside of these regulated contexts.

2) GIPA: In response to concerns about DNA testing companies selling information to third parties such as other companies, law enforcement, and the government, the Legislature passed, and the Governor signed, the GIPA in 2022. The GIPA requires DTC genetic testing companies to comply with certain privacy and data security provisions such as mandating consumers' affirmative consent regarding the collection, use, maintenance, and disclosure of genetic data, and enabling consumers to access and destroy their genetic data. According to the New York Times:

> 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]

The GIPA applies to companies that sell, market, interpret, or otherwise offer DTC genetic testing products or services; analyze genetic data obtained from consumers; collect, use, maintain, or disclose genetic data collected or derived from a direct-to-consumer genetic testing product, service or directly provided by a consumer.

It covers "genetic data," which is defined as any data, regardless of the format, that results from analysis of a biological sample from a consumer or from another element enabling equivalent information to be obtained and concerns genetic material. Genetic material includes, but is not limited to, DNA, RNA, genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphism (SNPs), uninterpreted data that results from analysis of the biological sample, and any information extrapolated, derived, or inferred from materials in this list.

Genetic data does not include **de-identified** data (meaning data not linked to any personal identifying information) or a biological sample to the extent that data or a biological sample is collected, used, maintained, and disclosed exclusively for scientific research under very particular circumstances described in the law. GIPA requires DTC genetic testing companies to: (a) provide clear and complete information regarding the company's policies and procedures for the collection, use, maintenance, and disclosure of genetic data; (b) obtain a

---

[1] Eric Ravenscraft, *How to Protect Your DNA Data Before and After Taking an at-Home Test* (June 12, 2019) N.Y. Times, https://www.nytimes.com/2019/06/12/smarter-living/how-to-protect-your-dna-data.html

consumer's express consent for the collection, use, and disclosure of the consumer's genetic data; (c) provide effective mechanisms, without dark patterns, for how a consumer may file to revoke consent; (d) implement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure; and (e) prohibits discrimination against a consumer because the consumer exercised any of the consumer's rights under GIPA.

The **GIPA makes clear that express consent is required for access by government actors pursuant to state and federal privacy laws.** This bill provides broad protections to information shared with government actors. Civil Code section 56.184 states in relevant part:

> The provisions of this chapter shall not reduce a direct-to-consumer genetic testing company's duties, obligations, requirements, or standards under any applicable state and federal laws for the protection of privacy and security. **In the event of a conflict between the provisions of this chapter and any other law, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.** (Civ. Code, § 56.184, subd. (a) & (b).)

3) **Data Breach Notification Law (DBNL)**: In 2003, California's security breach notification law went into effect. (See Civ. Code, §§ 1798.29, 1798.82.) There are two provisions governing data breach notification requirements, Civil Code sections 1798.29 and 1798.82. The two provisions are nearly identical, but the former applies to public agencies, and the latter applies to persons or businesses.

   California's DBNL requires any person or business that owns or licenses computerized data that includes personal information to disclose a breach to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Any breach notifications must be titled "Notice of Data Breach," are required to meet certain formatting requirements, and must include specific information. This notification requirement ensures that residents are made aware of a breach, thus allowing them to take appropriate action to mitigate or prevent potential financial losses due to fraudulent activity such as changing passwords, monitoring accounts, or placing credit freezes.

   Notification must also be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. With regard to the law enforcement provision, the notification required may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification must be made promptly after the law enforcement agency determines that it will not compromise the investigation.

   In 2023, 23andMe suffered a data breach affecting approximately 7 million users, roughly half its customer base—via a credential-stuffing attack.[2] Hackers accessed sensitive personal

[2] According to ID Theft Resource Center: Credential stuffing is a widespread cyberattack where hackers use automated bots to test massive lists of stolen username/password pairs (from previous data breaches) against various

information, including ancestry, DNA matches, and health data. A $30 million class-action settlement was reached to address the security failures. Reports as of March 2025 indicate the company has faced significant reputational damage and financial distress following the breach. Shortly thereafter, the company filed for Chapter 11 bankruptcy. Multiple Attorneys General are investigating possible identity theft or fraud, and requests have been made to the U.S. Department of Justice to also investigate.

In July 2025, the U.S. Bankruptcy Court for the Eastern District of Missouri approved the sale of 23andMe's genetic data. On July 14, 2025, a notice of the closing of the sale was filed in bankruptcy court. This sale process informs best practices for companies and other entities handling sensitive personal information. The Court approved the sale of 23andMe's genetic data and personal information assets to TTAM Research Institute, an entity founded by Anne Wojcicki, the former CEO and co-founder of 23andMe. TTAM was deemed the successful bidder over the bid of a leading biotechnology company, Regeneron.

4) **Medicare Fraud:** The author provided the committee several articles related to Medicare/CMS fraud nationwide related to access to genetic testing via medical companies. Offenders in Texas, Illinois, and New York were charged, tried, and convicted of Medicare fraud for soliciting medical professionals for genetic testing simply to bill Medicare/CMS for the testing. In the Texas case, medical professionals were receiving kickbacks from solicitors to generate unnecessary genetic testing requests. Defendants in those cases were sentenced to up to ten years in federal prison. It is not clear from those cases that there was any genetic sequencing performed or if it was merely a ruse to generate Medicare billings.

   As noted above, the GIPA was aimed at DTC companies like 23andMe selling genetic sequencing to third parties generally or in response to ordinary bankruptcy liquidation. In those cases, individual perpetrators may be hard to prosecute because the selling of genetic sequencing may have been a corporate decision and not the decision of one person acting rogue. Prior to 2022, if a person did not opt out on a DTC DNA testing form, it was not illegal to sell DNA to third parties in the ordinary course of business (although some did not do so). Finally, protecting DNA should also extend to state actors.

5) **Argument in Support**: No longer applicable.

6) **Argument in Opposition**: No longer applicable.

7) **Related Legislation**: AB 2018 (Ramos), would require the DOJ to take all reasonable steps to ensure that genetic data is used and disclosed only in a manner consistent with, and designed to advance, the purposes of identifying an unidentified person or locating a high-risk missing person. AB 2018 is pending hearing in this committee.

---

websites, exploiting the habit of password reuse to gain unauthorized access. It causes account takeovers, financial fraud, and data theft, costing organizations millions. (See https://www.idtheftcenter.org/post/the-difference-between-credential-hacking-and-credential-stuffing/?utm_campaign={campaignname}&utm_term=&utm_source=google&utm_medium=cpc&gad_source=1&gad_campaignid=22212099742&gbraid=0AAAAAD_RqESmwT-LrjvIMlgJAE3xZnOSf&gclid=EAIaIQobChMIgOKa8qWJkwMVUCGtBh0--hZTEAMYASAAEgLFlvD_BwE

8) **Prior Legislation**:

a) AB 3042 (Nguyen), Chapter 428, Statutes of 2024, extended the sunset date from January 1, 2025, to January 1, 2030, to collect and deposit funds into the DNA Identification Fund pursuant to Proposition 69 (2004), the DNA Fingerprint, Unsolved Crime and Innocence Protection Act, or a longer period of time if necessary to make payments on any lease or leaseback arrangement utilized to finance any specific projects.

b) SB 1228 (Weiner), Chapter 994, Statutes of 2022, adds to the Sexual Assault Victims' DNA Bill of Rights that DNA collected directly from a victim of sexual assault, and samples of DNA collected from intimate partners for the purposes of exclusion shall be protected in accordance with existing privacy provisions.

c) SB 41 (Umberg), Chapter 596, Statutes of 2022, establishes the GIPA providing additional protections for genetic data by regulating the collection, use, maintenance, and disclosure of such data.

REGISTERED SUPPORT / OPPOSITION:

Support

No longer applicable

Opposition

No longer applicable

Analysis Prepared by: Kimberly Horiuchi / PUB. S. / (916) 319-3744