Date of Hearing: March 10, 2026
Counsel: Kimberly Horiuchi

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Nick Schultz, Chair

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

SUMMARY: Creates new criminal penalties for the crime of unlawful use of Deoxyribonucleic acid (DNA). Specifically, **this bill**:

1) Defines unlawful use of DNA in the first degree as any person who intentionally and without express consent sells or otherwise transfers another individual's DNA sample or genetic data to a third party, regardless of whether the original DNA sample was originally collected, retained, or analyzed with express consent.

2) States unlawful use of DNA in the first degree shall be punishable as a felony and by a term of three, four, or five years in county jail or by fine not to exceed $15,000.

3) Defines unlawful use of DNA in the second degree as any person who intentionally and without express consent does any of the following:

    a) Submits another person's DNA sample for genetic testing;

    b) Conducts genetic testing on another person's DNA;

    c) Procures the conducting of genetic testing of another person's DNA; or,

    d) Discloses another person's genetic data to a third party except if they are the person's legal representative or guardian, or a person has already volunteered to disclose their genetic data to the person who provided it to the third party.

4) States unlawful use of DNA in the second degree shall be punishable as a felony and by a term of 16 months, two, or three years in county jail and a fine not to exceed $7,500.

5) Defines unlawful use of DNA in the third degree as any person who:

    a) Collects or retains another person's DNA sample with intent to perform a DNA analysis; or,

    b) Collects or retains another person's DNA sample or genetic information by accessing a computer system either without authorization or by exceeding their authorized access to the computer system.

6) Punishes unlawful use of DNA in the third degree as a one-year misdemeanor or fine of $6,000.

7) States unlawful use of DNA does not apply to any of the following:

    a) Any DNA sample or genetic material used for law enforcement purposes, a district attorney, or the Attorney General for law enforcement purposes, including, but not limited to, inclusion in the DNA and Forensic Identification Database and Data Bank Program;

    b) Any DNA sample or genetic material collected, obtained, or presented as evidence in a criminal investigation or court hearing, presented to a grand jury, or presented as evidence in a criminal trial, including criminal discovery as required by law;

    c) A DNA sample or genetic information collected to comply with a subpoena, summons, other lawful court order, or federal law;

    d) A direct-to-consumer genetic (DTC) testing company that complies with the Genetic Information Privacy Act (GIPA);

    e) A Health Insurance Portability and Accountability Act (HIPAA)-covered entity or business associate; and,

    f) A public or private institution of higher education or any entity owned or operated by a public or private institution of higher education.

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, "AB 1727 addresses a gap in California's Penal Code. 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.

"This gap has been exploited—particularly among seniors—by patient recruiters who collect DNA samples as part of Medicare fraud schemes. Additionally, the 2023 data breach involving

23andMe demonstrated the high value of genetic data to bad actors and underscored the risks Californians face when their sensitive information is exposed.

"While GIPA was a thoughtful and important step toward strengthening privacy protections, experience over the five years since its enactment has revealed the limitations of its targeted scope. The continued misuse and unlawful collection of DNA data make clear that existing safeguards are not sufficient to fully protect Californians.

"AB 1727 does not seek to restrict law enforcement officers or investigators from carrying out their duties or pursuing justice. Instead, it expands privacy protections to ensure that all Californians are safeguarded from individuals or entities that seek to profit from the unauthorized collection or exploitation of their genetic information. As criminals become more sophisticated in their enterprises, it is critical that we act to protect the most basic identity that people have – their DNA."

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 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.

This bill differs from the GIPA in its definitions of genetic testing, genetic data, and express consent although it appears to criminalize a company or person who provides genetic material to third parties without consent. **The GIPA also 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).)

It appears the mandates and definitions of this bill are significantly different than the GIPA and provide interpretation and enforcement limitations for the Department of Justice (DOJ) in

[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

prosecuting a GIPA violation. While this bill is limited to criminal penalties, it appears to rely, in part, on the prohibitions in the GIPA aimed at DTC genetic testing companies.

The author's background statement to the committee cites a Florida law that is effectively just a version of California's GIPA. It includes most of the same civil penalties and is part of the civil rights statutes. (See § 760.40, Fla. Stat. Ann.)

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 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 its letter of support, SAG-Aftra noted that there is also an alleged rise in "genetic paparazzi" that seek a celebrity's DNA for some sort of nefarious purpose. California has numerous laws

---

[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 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

that prevent disclosure of personal identifying information, including the GIPA. While many states have expressed concern about what 23andMe would do with its expansive DNA database, it will likely only be sold in a deidentified form meaning the information will not be tied to a name or any other personal information.

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.

It is unclear to what extent, if any, people in the public eye are susceptible to people stealing their DNA. However, mandating a five-year prison or jail term depending on a defendant's criminal history seems disproportionate for what may be a completely illusory problem.

4) **Criminal Penalties:** The GIPA may be enforced either by local district attorney offices or the DOJ. Penalties include fines between $1,000 and $10,000 depending on whether the breach was negligent or intentional. Criminal penalties require *mens rea*, or criminal intent. This bill appears to impose significant criminal penalties for violations of the same conduct at issue in the GIPA.

This bill would create three new crimes: (a) any person who intentionally sells or transfers another person's genetic material or DNA without express consent is guilty of unlawful use of DNA in the first degree and may be sentenced to three, four, or five years in county jail; (b) any person who submits a person's DNA for genetic testing, actually conducts the testing on another person's DNA, or discloses DNA or genetic material to a third party, as specified, without express consent is guilty of unlawful use of DNA in the second degree and may be sentenced to 16 months, two, or three years in county jail; and (c) any person who collects or retains another person's genetic material or DNA, or someone who accesses a computer system without authorization that has genetic material or DNA is guilty of unlawful use of DNA in the third degree and may be sentenced to up to one year in the county jail.

The penalty structure proposed by this bill seems both inconsistent with other crimes and does not follow criminal sentencing requirements. First, this bill sentences a person to county jail for as long as five years pursuant to Penal Code section 1170, subdivision (h). As a straight felony, in accordance with Penal Code section 1170, subdivision (h)(5), any person who is sentenced pursuant to Realignment with a prior serious or violent felony or sex offense, is sentenced to state prison. Comparatively, robbery (not home invasion, carjacking, train robbery, or taking money by force or threat of force near an ATM) is punishable by two, three, or five years. (Pen. Code, § 213, subd. (a).) The penalty for intentionally selling or transferring DNA without express consent is actually harsher on the low and middle term than robbery. Carjacking is punishable by a term of three, five, or nine years. (See Pen. Code, § 215, subd. (b).) The low and middle term for first degree unlawful use of DNA are about the same on the low and middle terms as carjacking.

Additionally, it is unclear how a prosecutor would demonstrate aggravating factors such that a jury would impose the upper term for unlawful use of DNA. Factors in aggravation in the

California Rules of Court, includes (a) great violence, great bodily harm, threat of great bodily harm, or other acts disclosing a high degree of cruelty, viciousness, or callousness; (b) the defendant was armed with or used a weapon at the time of the commission of the crime; (c) victim was particularly vulnerable; (d) defendant induced others to participate in the commission of the crime or occupied a position of leadership or dominance of other participants in its commission; (e) the defendant induced a minor to commit or assist in the commission of the crime; (f) the defendant threatened witnesses, unlawfully prevented or dissuaded witnesses from testifying, suborned perjury, or in any other way illegally interfered with the judicial process; (g) the defendant was convicted of other crimes for which consecutive sentences could have been imposed but for which concurrent sentences are being imposed; (h) the manner in which the crime was carried out indicates planning, sophistication, or professionalism; (i) the crime involved an attempted or actual taking or damage of great monetary value; (j) the crime involved a large quantity of contraband; (k) defendant took advantage of a position of trust or confidence to commit the offense; and (l) the crime constitutes a hate crime. (Cal Rules of Court, Rule 4.421, subd. (a)(1)-(12).)

This crime does not fit within possible aggravating factors. As explained above, the GIPA is aimed at DTC genetic testing companies. Corporations are obviously sentenced to jail and Chief Executive Officers, or employees of the company do not ordinarily take on criminal liability for performing work for the company even though they may be intentionally testing DNA without **express consent**. Express consent is broadly defined in this bill, but the absence of "express consent" may be hard to discern given a person may be facing up to five years in county jail for selling or transferring DNA or genetic material intentionally without express consent.

Finally, the Penal Code does not criminalize conduct in the third degree. Again, the criminal penalty structure laid out on Penal Code section 17 is based on penalty. If a person may be sentenced to up to one year in county jail, or there is no stated penalty, the crime is a misdemeanor. If a person may be sentenced to up to one year in county jail or up to three years in county jail, it is a Realigned alternate-misdemeanor felony. If a person may be sentenced to either state prison or more than one year in county jail for an offense, it is a Realigned felony. If a person may be sentenced to state prison, it is a state prison felony. While a small number of offenses may be charged as a first- or second-degree crime, those offenses have existed in our Penal Code since the beginning of statehood, including murder, robbery, and burglary. (See generally, Pen. Code, § 1182.)

Pursuant to Penal Code section 17, a criminal penalty punishable in the county jail pursuant to Realignment could be an alternate felony-misdemeanor, depending on the court's action. However, a misdemeanor may be sentenced to no more than one year. Based on existing sentencing requirements, it appears first- and second-degree unlawful use of DNA are felonies, and a third-degree offense is a misdemeanor.

5) **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 ever 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. While companies generally have opt-out options for people who do not wish to share their DNA with law enforcement or for forensic genetic genealogy purposes, this bill expressly excludes law enforcement from surreptitiously accessing a person's DNA even if they have opted out of sharing with law enforcement. The GIPA requires compliance with notice requirements for opting out and includes a much more robust definition of "express consent."

6) **Argument in Support**: According to *California Civil Liberties Advocacy*, "Genetic data represents some of the most intimate and revealing information a person possesses. A DNA sample can expose deeply personal details about an individual's health predispositions, ancestry, and familial relationships. Unlike other forms of personal data, genetic information cannot be changed once compromised. As such, it warrants the highest level of legal protection.

"While California has taken important steps to regulate direct-to-consumer genetic testing companies through the Genetic Information Privacy Act, significant gaps remain in current law. Existing statutes focus primarily on corporate actors and do not adequately address the growing risk of unauthorized DNA collection and analysis by private individuals or third parties.

"AB 1727 fills this gap by clearly prohibiting the intentional collection, testing, or transfer of another person's genetic material without their consent and establishing appropriate criminal penalties for violations. The need for such protections is becoming increasingly urgent. Advances in genetic testing technology have dramatically lowered the cost and accessibility of DNA analysis. Today, individuals can obtain genetic profiles from discarded items such as drinking glasses, hair strands, or cigarette butts and submit those samples to private laboratories for testing. Without clear legal safeguards, these practices create the potential for serious abuses, including covert paternity testing, nonconsensual ancestry testing, genetic surveillance, and the unauthorized disclosure of highly sensitive health and family information.

"AB 1727 appropriately balances privacy protections with legitimate public interests. The bill includes sensible exemptions for law enforcement investigations conducted pursuant to existing legal authority, as well as for institutions that operate under established federal privacy frameworks such as HIPAA. These provisions ensure that the measure protects individual rights without interfering with legitimate medical research, criminal investigations, or court-authorized procedures.

"California's Constitution explicitly recognizes privacy as a fundamental right. Genetic information lies at the very core of that right. By establishing clear criminal penalties for the intentional misuse of another person's DNA, AB 1727 strengthens California's longstanding commitment to protecting personal privacy in the face of rapidly evolving technologies."

7) **Argument in Opposition**: According to *ACLU California Action*: "Our DNA can reveal some of our most personal and private information. As medical records are increasingly digitized and genetic sequencing becomes faster and cheaper, threats to our privacy and autonomy intensify. Whether it is police seeking to search for medical records or conduct DNA tests without a warrant, or private corporations patenting human genes, the ACLU is fighting to preserve privacy rights of all people.

For instance, we have long fought to maintain the privacy of sensitive medical and genetic information. In *Maryland v. King*,[3] we filed a brief in the U.S. Supreme Court opposing the drastic expansion of state DNA databases to include samples from people who have been arrested but not yet convicted. And in a similar case, *Center for Genetics and Society, et al. v. Rob Bonta, et al*., we are challenging the state of California for its retention of genetic samples and profiles from people arrested but never convicted of a felony.[4]

While we advocate for strong consumer privacy protections in the face of growing surveillance across this nation, we believe we can impose robust safeguards through a regulatory and civil enforcement framework without creating new criminal penalties to protect people's privacy. Specifically, the legislature can design a regime with sufficiently strong civil penalties, meaningful reporting requirements, and real enforcement mechanism that would both protect consumers and make it financially untenable for companies to misuse sensitive DNA information. Well-calibrated fines, private rights of action, and both reporting and transparency obligations can create a powerful deterrence without needing to create new crimes.

Furthermore, the current exemptions in the proposed Penal Code §367(g) seem overbroad. We believe that any genetic privacy law that does not apply to some of the worst actors in this space, such as the large direct-to-consumer genetic testing companies, is insufficient in safeguarding people's sensitive genetic information.

Finally, we find issue with the term 'deidentified' data not being defined in the proposed Penal Code §367(a)(4)(B). While the term is defined in the California Consumer Privacy Act, that definition is meant to allow some analysis of people's personal information when it cannot be linked back to them as an individual. For genetic information, this is significantly more difficult given the uniquely identifying nature of the information. This presents a potential issue, as any Artificial Intelligence model trained on people's genetic data would be considered a form of "deidentified" data. In this scenario, the model itself could be shared or sold without people having any rights to consent. This brings us to a familiar question about when people should be able to decide when information about them is used to train an algorithmic system. Examples could include software to diagnose and screen for genetic diseases, or possibly software to simulate the effect of a biological weapon on a population.

We encourage the author to explore an alternative approach that shifts us away from failed carceral solutions and instead craft a robust regulatory and civil enforcement framework to hold bad actors accountable without exempting large direct-to-consumer genetic testing companies.

---

[3] Maryland v. King, 569 U.S. 435 (2013)
[4] Center for Genetics and Society, et al. v. Rob Bonta, et al. No. CPF-18-516440

8) **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.

9) **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

A Voice for Choice Advocacy
California Civil Liberties Advocacy
City of Los Alamitos
SAG-AFTRA

Opposition

ACLU California Action
California Attorneys for Criminal Justice

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