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

SB 1189 (Wieckowski)
Version: March 28, 2022
Hearing Date: April 5, 2022
Fiscal: No
Urgency: No
CK

SUBJECT

Biometric information

DIGEST

This bill places protections on biometric information collected, used, disclosed, and retained by private entities.

EXECUTIVE SUMMARY

Biometric information includes fingerprints, retina or iris images, and gait patterns and is generally used to authenticate a specific individual. The collection and use of this information by businesses has skyrocketed in recent years. In 2020, the global biometrics market was estimated to be $24 billion. The trajectory is not anticipated to plateau either. The market is forecasted to reach $82.8 billion by 2027.

While the use of this information provides many benefits, serious concerns have arisen with the widespread collection and disclosure of this highly sensitive biometric information without the informed consent of the people to whom the information pertains. These issues are compounded by the commodification of biometric data and its disclosure for for-profit purposes.

This bill places guardrails around the collection, use, disclosure, and retention of biometric information by private entities in California. The collection and use of this information can only be carried out after receiving a written release from the subject after they have been adequately informed of the relevant details. Entities must have a valid business purpose for collecting and using the information and must have a policy for the retention and destruction of the information. Disclosure of this information is tightly restricted and safeguards must be put into place. Private entities are prohibited from selling, leasing, trading, or otherwise profiting from the disclosure of biometric information.

This bill is sponsored by the Electronic Frontier Foundation and Privacy Rights Clearinghouse. It is supported by various privacy and consumer groups. It is opposed by a number of organizations, including a coalition led by the California Chamber of Commerce.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, Sec. 1.)

2) Establishes the Information Practices Act of 1977, which declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. It further states the following legislative findings:

    a) the right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies;
    b) the increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information; and
    c) in order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code § 1798 et seq.)

3) Establishes the California Customer Records Act, which provides requirements for the maintenance and disposal of customer records and the personal information contained therein. (Civ. Code § 1798.80 et seq.) It further states it is the intent of the Legislature to ensure that personal information about California residents is protected and to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information. (Civ. Code § 1798.81.5(a).)

4) Establishes the California Consumer Privacy Act of 2018 (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

5) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and creates the California Privacy Protection Agency (PPA), which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

6) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers of the following:
    a) the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section;
    b) if the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section; and
    c) the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose. (Civ. Code § 1798.100(a).)

7) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
    a) the categories of personal information it has collected about that consumer;
    b) the categories of sources from which the personal information is collected;
    c) the business or commercial purpose for collecting or selling personal information;
    d) the categories of third parties with whom the business shares personal information; and
    e) the specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110.)

8) Provides consumers the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer the following:
    a) the categories of personal information that the business collected about the consumer;
    b) the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and
    c) the categories of personal information that the business disclosed about the consumer for a business purpose. (Civ. Code § 1798.115.)

9) Provides a consumer the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold and that consumers have the right to opt out of the sale of their personal information. (Civ. Code § 1798.120.)

10) Provides that these provisions do not restrict a business' ability to collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information. (Civ. Code § 1798.145(a)(6).)

11) Defines "personal information" as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including biometric information, geolocation data, and "sensitive personal information." (Civ. Code § 1798.140(v)(1).)

12) Extends additional protections to "sensitive personal information," which is defined as personal information that reveals particularly sensitive information such as genetic data and the processing of biometric information for the purpose of uniquely identifying a consumer. (Civ. Code § 1798.140(ae).)

13) Provides various exemptions from the obligations imposed by the CCPA. (Civ. Code § 1798.145.)

14) Permits amendment of the CPRA by a majority vote of each house of the Legislature and the signature of the Governor provided such amendments are consistent with and further the purpose and intent of the act as set forth therein. (Proposition 24 § 25 (2020).)

15) Establishes the Genetic Information Privacy Act (GIPA) to protect consumers' "genetic data," which is defined as any data, regardless of its format, that results

from the analysis of a biological sample from a consumer, or from another element enabling equivalent information to be obtained, and concerns genetic material, except deidentified data, as provided. GIPA regulates direct-to-consumer genetic testing companies. (Civ. Code § 56.18.)

This bill:

1) Defines "biometric information" as the data of an individual generated by automatic measurements of an individual's unique biological or behavioral characteristics, including a faceprint, fingerprint, voiceprint, retina or iris image, or any other biological characteristic that can be used to authenticate the individual's identity. This specifically does not include:
    a) writing sample or written signature;
    b) a photograph or video;
    c) a human biological sample used for valid scientific testing or screening;
    d) a physical description, including height, weight, hair color, eye color, or a tattoo description;
    e) a donated portion of a human body stored on behalf of a recipient or potential recipient of a living or cadaveric transplant and obtained or stored by a federally designated organ procurement agency, including an organ, tissue, eye, bone, artery, blood, or any other fluid or serum;
    f) information captured from a patient in a health care setting; or
    g) an image or film of the human anatomy used to diagnose, provide a prognosis for, or treat an illness or other medical condition or to further validate scientific testing or screening, including an x-ray, roentgen process, computed tomography, magnetic resonance image, positron emission tomography scan, or mammography.

2) Requires, by September 1, 2023, private entities that possess biometric information to make public a policy on retaining and ultimately destroying that biometric information. Except for biometric information that is the subject of a valid warrant or court-issued subpoena, the information must be destroyed on or before the earliest of the following:
    a) the date on which the initial purpose for collecting or obtaining the biometric information is satisfied;
    b) one year after the individual's last intentional interaction with the private entity; or
    c) within 30 days after the private entity receives a verified request to delete the biometric information submitted by the individual or the individual's representative, notwithstanding Section 1798.130 of the Civil Code.

3) Provides that "private entity" does not include a federal, state, or local government agency or an academic institution.

4) Prohibits a private entity from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's biometric information unless all of the following are true:
    a) the private entity requires the biometric information to provide a service requested or authorized by the subject of the information or for another valid business purpose specified in its written policy;
    b) the private entity informs the person or a representative, in writing, of what biometric information is being collected, stored, or used, the specific purpose for it, and the relevant length of time;
    c) receives a written release executed by the subject of the biometric information or by the subject's legally authorized representative that is separate from other similar releases or employment contracts. Such a release for a minor must be obtained through the minor's parent or guardian.

5) Provides that a private entity shall not sell, lease, trade, or otherwise profit from the disclosure of a person's biometric information or use for advertising purposes a person's biometric information.

6) Prohibits a private entity from disclosing biometric information unless any of the following are true:
    a) the subject of the biometric information, or their representative, provides a written release that authorizes the disclosure immediately beforehand and includes a description of the data that will be disclosed, the reason for disclosure, and the recipients;
    b) the disclosure completes a financial transaction requested or authorized by the subject or a representative; or
    c) it is required by law or pursuant to a valid warrant or subpoena issued by a court.

7) Prohibits a private entity from conditioning the provision of a service on the collection, use, disclosure, transfer, sale, or processing of biometric information unless biometric information is strictly necessary to provide the service. A private entity shall not charge different prices or rates for goods or services or provide a different level or quality of a good or service to an individual who exercises the individual's rights under this law.

8) Requires a private entity to store, transmit, and protect from disclosure biometric information using the reasonable standard of care within the private entity's industry and in a manner that is the same as, or more protective than, the manner in which it stores, transmits, and protects other confidential and sensitive information.

9) Authorizes individuals to enforce the law through a civil action for any of the following relief:
    a) the greater of either statutory damages of $100 to $1,000 per violation per day or actual damages;
    b) punitive damages;
    c) reasonable attorney's fees and litigation costs; and
    d) any other relief, including equitable or declaratory relief, that the court determines appropriate.

10) Clarifies that it does not do any of the following:
    a) impact the admission or discovery of biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.
    b) conflict with the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA); or
    c) conflict with Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

COMMENTS

1. The immutability and sensitivity of biometric information

Biometrics are measurable physiological or behavioral characteristics that can be used to verify the identity of an individual. Physiological characteristics include the shape or composition of the body while behavioral characteristics concern the behavior of an individual. Physiological biometrics includes facial recognition, fingerprint scanning, hand geometry, iris scanning, and DNA. Behavioral biometrics include an individual's keystroke, signature, gait patterns, and voice recognition. The use of biometrics in business is widespread, and the types of usage are constantly evolving. With new technological developments and the technology itself becoming more readily available, industries of all sizes and kinds are turning to biometric data collection to enhance their time management, security access, safety, and employer-provided health plans.

Biometric information is immutable and therefore more sensitive than most other personal information. Therefore, it is of heightened importance to protect such information given its increased collection and use in connection with various surveillance technologies, identity confirmation, and in connection with personal devices and smartphones.

2. Collection and use of biometric information by private entities

There are a plethora of examples of how industry is collecting and utilizing the biometric information of consumers and employees. For instance, Walgreens has

piloted the use of "smart coolers."[1] The coolers are equipped with cameras and technology that scan shoppers' faces and make inferences about their age and gender. The value of this to retailers is immense:

> If, for example, Pepsi launched an ad campaign targeting young women, it could use smart-cooler data to see if its campaign was working. These machines can draw all kinds of useful inferences: Maybe young men buy more Sprite if it's displayed next to Mountain Dew. Maybe older women buy more ice cream on Thursday nights than any other day of the week. The tech also has "iris tracking" capabilities, meaning the company can collect data on which displayed items are the most looked at.

On the employee side, it is reported that Walmart requires employees to record their voice using voice recognition software:

> Once the voice recognition system learns their voice, workers are required to communicate with the system as they move about the warehouse, pulling requested merchandise in response to customer orders. "Through the headset they receive orders to fill and are required to respond into the headset telling it where they are in the warehouse, the product that they have just pulled from storage, the amount of that product that they have pulled, and the order that they are filling[.]"[2]

In addition, TopGolf recently settled a lawsuit that alleged the company was improperly collecting biometric information from its employees without informed consent when it required them to scan their fingerprints to "punch the clock" at work.[3]

Ultimately, the collection and use of biometric information is exploding, with use by finance companies, airports, social media companies, law enforcement, and the military.[4] The technology is embedded into the products and services many consumers use on a daily basis. Our phones are unlocked with fingerprints or facial scans; even our cars are using cameras with facial recognition software and other biometric indicators to

---

[1] Sidney Fussell, *Now Your Groceries See You, Too* (January 25, 2019) The Atlantic, https://www.theatlantic.com/technology/archive/2019/01/walgreens-tests-new-smart-coolers/581248/. All internet citations herein are current as of March 20, 2022.
[2] Jonathan Bilyk, *Class action: Walmart improperly tracks warehouse workers using their 'voiceprints' without consent* (July 8, 2021) Cook County Record, https://cookcountyrecord.com/stories/605642967-class-action-walmart-improperly-tracks-warehouse-workers-using-their-voiceprints-without-consent (information according to a filed complaint by former employees).
[3] Roy Maurer, *Topgolf Settles Biometric Privacy Lawsuit* (July 19, 2021) SHRM, https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/topgolf-settles-biometric-privacy-lawsuit.aspx.
[4] Tom Simonite, *Face Recognition Is Being Banned – but It's Still Everywhere* (December 22, 2021) WIRED, https://www.wired.com/story/face-recognition-banned-but-everywhere/.

read drivers' emotions and to attempt to predict their behavior.[5] The technology and uses are seductive but also controversial. This bill is motivated by concerns that without bolstered privacy protections, the widespread collection, disclosure, use, and retention of biometric information risks empowering discriminative business practices, degrading privacy, and imposing heightened security risks on consumers.

3. Following the lead of Illinois: California's Biometric Information Privacy Act

At the forefront of protecting this particularly sensitive data, Illinois enacted the Biometric Information Privacy Act (BIPA) in 2008, one of the first state laws to address business' collection of biometric data. (740 ILCS 14 et seq.) BIPA establishes a comprehensive set of parameters for companies collecting the biometric information of state residents. Specifically, BIPA does the following:

- requires informed consent prior to collection;
- permits a limited right to disclosure;
- establishes protection obligations and retention guidelines;
- prohibits profiting from biometric data; and
- authorizes a private right of action for individuals harmed by violations.

BIPA has been used to hold many major corporations accountable for their widespread collection and use of biometric information without proper consent. In early 2019, the Illinois Supreme Court unanimously ruled that when companies collect biometric data without informed, opt-in consent, they can be sued, and individuals do not need to prove an injury or harm to prevail, generally a high hurdle to enforce similar laws.[6]

This bill, partially based on BIPA, prohibits private entities from collecting or disclosing biometric data without first acquiring informed affirmative consent from persons whose data is being collected or disclosed. Consumers must be informed, in detail, about what information is being collected, stored, used, or disclosed; the respective purposes; and any recipients of the data. Furthermore, it requires private entities to publish a written policy establishing a retention schedule and guidelines for permanently destroying the biometric information. The bill imposes a firm restriction on private entities selling, leasing, trading, or otherwise profiting from the disclosure of a person's biometric information or using it for advertising purposes. Private entities are also required to implement reasonable industry security practices to protect this information, given the enhanced risks should such information be subject to breach. Consumers and others affected by violations are provided a mechanism to enforce their rights.

---

[5] John R. Quain, *Soon, Your Car May Be Able to Read Your Expressions* (April 6, 2017) The New York Times, https://www.nytimes.com/2017/04/06/automobiles/wheels/cars-facial-recognition-expressions.html.
[6] Jennifer Lynch & Adam Schwartz, *Victory! Illinois Supreme Court Protects Biometric Privacy* (January 25, 2019) Electric Frontier Foundation, https://www.eff.org/deeplinks/2019/01/victory-illinois-supreme-court-protects-biometric-privacy.

The bill builds on and expands existing rights provided through the CCPA/CPRA. Generally, the CCPA requires certain businesses to provide notice to consumers about what "personal information" is being collected and the possible uses of that data. Consumers are able to request the information that has been collected and to opt out of the sale of that information, with certain enhanced protections for "sensitive information."

This bill places stronger protections specifically around biometric information. The bill deploys an opt-in mechanism, focusing on prior informed consent, rather than placing the onus on consumers to affirmatively seek its protections, and covers the initial collection of the information. While biometric information is included within the definition of personal information in the CCPA, it includes only that information "that is used or is intended to be used . . . to establish individual identity." This bill includes all such information that *can be used* to establish identity.

To ensure compliance and that consumers are able to protect their rights under this law, the bill provides that an individual alleging a violation may bring a civil action for specified relief. This includes the greater of either actual damages or statutory damages of $100 to $1000 per violation per day. Plaintiffs in such cases can also seek punitive damages, reasonable attorney's fees and litigation costs, and any other relief the court determines appropriate.

4. Stakeholder positions

According to the author:

> SB 1189 strengthens privacy protections around data that is uniquely sensitive and personal. The right to privacy is a cornerstone of the American constitution. Yet, companies hoping to augment processes such as automated authentication, surveillance, and targeted marketing increasingly collect forms of data that risk further eroding privacy. Biometric information relates to permanent and highly distinctive traits such as the ridges of our fingerprints, the texture and color of our eyes, or the geometric attributes of our faces. Such data may also reveal intimate and intangible traits, such as preferences and emotion. The possibility of knowing consumers inside and out to further market their products has sparked a flood of companies looking to collecting biometric information. This comes with great individual and societal risks. Without additional privacy protections, widespread use of biometrics risks empowering discriminative business practices and degrading privacy, all while imposing heightened security risks on the average consumer.
>
> At a minimum, the use of biometric information should come with clear rules that place the consumer in control of their data while limiting the

> inherent risks that come with its use. Otherwise, we risk ceding control of data irrevocably tied to our identities to private entities that sell and trade it like any other commodity while creating highly detailed composites of our habits and likes. SB 1189 would look to empower consumers and make them active participants in the collection, use, and disclosure of their data. It would ensure that biometric information is used in a responsible manner that prioritizes individual privacy by expanding control over data.

The co-sponsors of this bill, the Electronic Frontier Foundation and Privacy Rights Clearinghouse, make the case:

> S.B. 1189 does not bar private entities from using biometric information. It simply ensures that people are well-informed before companies collect their data. In this way, S.B. 1189 properly checks the harms of unconsented biometric data collection while still giving individuals the choice to use these technologies. For example, some users may choose to deploy it to lock their mobile devices. S.B. 1189 properly allows individuals to make the choice that works best for their personal situations.
>
> Biometric information is deeply personal. It is only right that people should be in control of how their own personal data is collected, and be fully informed about how it will be used.

National Payroll Reporting Consortium writes in strong opposition to the bill as written:

> SB 1189 would have severe adverse consequences, based on our experience with Illinois' similar Biometric Information Privacy Act (BIPA.) In brief, the Illinois BIPA adversely affected many employers that were using finger-scan, hand- scan, and face-scan timeclocks to more accurately record employees' time worked. In Illinois, timeclock systems were not a concern - - and in fact were not referenced at all in the Illinois legislation. Nevertheless, roughly 90% of the 900+ class action lawsuits filed under the Illinois BIPA have been related to timeclocks.
>
> Because the law provided for a private right of action and statutory penalties, which in the context of employment yielded astronomical claims, the law became a target for abusive and frivolous litigation. The law enabled aggressive plaintiffs' attorneys to seek out common time-keeping systems for any failure to meet the statutory disclosure and consent requirements, and to seek huge statutory penalties with no requirement to demonstrate any harm.

Writing in opposition, a group of life sciences organizations argues the bill is overly broad and "inappropriately applies to health care information." They assert:

> SB 1189 contains overly-broad and poorly defined new categories of information that threaten to sweep up important categories of information that are already well-regulated under several bodies of law.
>
> The breadth of information covered under the bill combined with a private right of action guarantee that the State of California and businesses that provide care to patients will become mired in long and ultimately pointless litigation that does not advance the public's interest.

With regard to concerns that the exemption for information captured from a patient in a health care setting is not precise enough, the author has agreed to take the following amendment:

> Amendment
>
> Amend Section 1798.300(a)(2)(F) as follows:
>
> Information captured from a patient ~~in a health care setting~~ by a provider of health care, as defined in Section 56.05(m) of the Civil Code, including physicians and surgeons licensed by the Medical Board of California, for the purpose of health care treatment, payment, or operations under federal Health Insurance Portability and Accountability Act of 1996 or the California Confidentiality of Medical Information Act.

Additional concerns were raised by the University of California regarding the impact on the use of biometric information for educational and research purposes. In response, the author has agreed to the following amendment:

> Amendment
>
> Add the following provision:
>
> Section 1798.301(d): This section shall not apply to any disclosures made to a public or private nonprofit postsecondary educational institution that holds an assurance with the United States Department of Health and Human Services pursuant to Part 46 of Title 45 of the Code of Federal Regulations, to the extent that the subject's biometric information is disclosed to a public or private nonprofit postsecondary educational institution for the purpose of scientific research or educational activities as described in paragraph (4) of subdivision (c) of Section 56.184.

A coalition of groups, led by the California Chamber of Commerce, also write in opposition:

> SB 1189 poses significant liability risks to businesses, opening the floodgates to potentially abusive class action lawsuits that are based on minor, technical violations, instead of actual injury. This is not just a matter of speculation. One need only look to Illinois' Biometric Information Privacy Act (BIPA) to see the avalanche of class action lawsuits that would ensue, often for minor technical violations which resulted in no harm to the individual who knew that their biometric information was being used and the purpose for that use (such as where a person knows their fingerprint is scanned to clock in and out of work). Illinois has seen over 1,100 class action suits against companies of all types and sizes since 2017. According to the National Law Review, BIPA cases in 2021 "settled in the six-, seven-, eight-, and even nine-figure ranges, even in cases where there have been no allegations that the plaintiffs' biometric data was hacked or improperly accessed by a nefarious third party." That is what this bill is ultimately about, not affirmative consent.

Currently the bill provides that each individual alleging a violation can seek, among other relief, either actual damages or statutory damages of $100 to $1000 per violation per day. As referenced in the coalition letter, there is concern that allowing each affected individual to separately seek a statutory penalty for each violation that accrues each day in violation is overly onerous. In response, the author has agreed to remove the "per violation" element of this cause of action. Therefore, each individual seeking to recover the statutory penalty will be limited to damages of $100 to $1000 per day.

> <u>Amendment</u>
>
> Amend Section 1798.306(a)(1) as follows:
>
> Statutory damages in an amount not less than one hundred dollars ($100) and not greater than one thousand dollars ($1,000) ~~per violation~~ per day.

Secure Justice highlights the need for the bill:

> This wide use of biometrics comes with great individual and societal risks. Steady improvements in technology make biometric identification through mobile or covert means more possible. This can have a chilling effect on free speech, free association, and other cornerstones of a democratic society by erasing our ability to go about our daily lives without threat of surveillance. Such threats also extend to the digital world; biometric information can facilitate price point discrimination and targeted advertising based on race, preferences, emotion, etc. These highly

curated interactions can heighten socioeconomic disparities that disproportionally affect minority communities while nudging consumer behavior towards substandard, even harmful, routines.

SUPPORT

Electronic Frontier Foundation (co-sponsor)
Privacy Rights Clearinghouse (co-sponsor)
ACLU California Action
Consumer Action
Consumer Attorneys of California
Consumer Federation of America
Consumer Federation of California
Electronic Privacy Information Center
Fairplay
The Greenlining Institute
Media Alliance
Oakland Privacy
Secure Justice

OPPOSITION

Advanced Medical Technology Association
American Property Casualty Insurance Association
Association of National Advertisers
Biocom California
California Bankers Association
California Business Properties Association
California Chamber of Commerce
California Land Title Association
California Life Sciences
California Retailers Association
California Trucking Association
Cemetery and Mortuary Association of California
Civil Justice Association of California
Electronic Transactions Association
Insights Association
National Payroll Reporting Consortium
Netchoice
Plumbing Manufacturers International
Security Industry Association
Software & Information Industry Association
State Privacy and Security Coalition, Inc.
Technet

Technology Industry Association of California

RELATED LEGISLATION

Pending Legislation:

SB 346 (Wieckowski, 2021) requires certain disclosures connected to in-vehicle cameras installed by the manufacturer and places restrictions on what can be done with video recordings from such cameras and where such recordings can be retained. This bill is currently in the Assembly Privacy and Consumer Protection Committee.

SB 1038 (Bradford, 2022) deletes the sunset date on the ban on biometric surveillance established by AB 1215 (see below). This bill is currently on the Senate Floor.

AB 1262 (Cunningham, 2022) implements stronger consumer protections in connection with the use of voice recognition features on smart speaker devices and any transcripts or recordings collected or retained in connection with that use. This bill is currently in the Senate Appropriations Committee.

Prior Legislation:

SB 41 (Umberg, Ch. 596, Stats. 2021) establishes the Genetic Information Privacy Act, providing additional protections for genetic data by regulating the collection, use, maintenance, and disclosure of such data.

AB 1436 (Chau, 2021) would have provided that a business shall not knowingly use, disclose, or permit the use or disclosure of personal health record information without a signed authorization and restricted further disclosure. The bill died in the Senate Appropriations Committee.

SB 1010 (Jackson, 2020) would have prohibited a law enforcement agency or law enforcement officer from developing, acquiring, possessing, accessing, using, or sharing any facial recognition or other biometric surveillance system. This bill died in the Senate Rules Committee.

AB 1130 (Levine, Ch. 750, Stats. 2019) updated the definition of "personal information" in various consumer protection statutes to include certain government identification numbers and biometric data.

AB 1215 (Ting, Ch. 579, Stats. 2019) banned the use of facial recognition technology and other biometric surveillance systems in connection with cameras worn or carried by law enforcement, including body-worn cameras, for the purpose of identifying individuals using biometric data.

****