Date of Hearing: April 22, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1355 (Ward) – As Amended April 10, 2025

SUBJECT: Location privacy

SYNOPSIS

Our phones can also reveal far more about us than we might realize: important details about our lives and where we've been. For example, our phones might be periodically sending their exact location to tech companies. This data can pinpoint our comings and goings with startling precision. Think what this might reveal: what therapist you're seeing, what medical treatment you're seeking, your visits to places of worship, and even your reproductive choices. This type of tracking can cause enormous harm to consumers, including stigma, emotional distress, discrimination, or even physical violence. [1]

– Federal Trade Commission (2022)

Despite the laws passed in California in recent years aimed at specifically protecting the privacy of vulnerable groups, survivors of intimate partner violence, government officials, and healthcare providers, precise location data is being collected, processed and sold constantly by companies collecting that data through mobile application developers, various surveillance technologies, and location data brokers. Everywhere people in California go, how often they go, how long they stay, where they sleep at night, the routes they take travelling to and from work or dropping children off at school, are all collected and available from location data brokers to anyone willing to pay.

The location information market is a multi-billion-dollar, fast growing industry centered on collecting and selling people's everyday comings and goings, often collected from people's mobile devices and often without their knowledge or express consent. Not only are location data brokers selling massive quantities of precise location data to other businesses, all of this location information, potentially tracking people to sensitive locations, is available to any paying law enforcement agency without a court order, warrant, or subpoena.

In order to close the back door that is allowing public and private entities to ignore the State's privacy protections, this bill restricts the collection, processing, sale, sharing, and disclosure of individuals' precise location information.

This bill is sponsored by Consumer Reports and supported by a number of privacy organizations, consumer and other advocacy groups, and labor organizations. It is opposed by a coalition of business associations, the California State Sheriffs' Association, and the Peace Officers Research Association of California.

If passed by this Committee, this bill will next be heard by the Judiciary Committee.

---

[1] Carol Kando-Pineda. *Consumer Alert: FTC sues company that sells consumers' sensitive location information*. FTC (Aug. 29, 2022) https://consumer.ftc.gov/consumer-alerts/2022/08/ftc-sues-company-sells-consumers-sensitive-location-information

THIS BILL:

1) Establishes the California Location Privacy Act.

2) Prohibits a covered entity – an individual, partnership, corporation, limited liability or other group, with the exception of a state or local agency or the California courts – from collecting or processing the location information of an individual within the state of California unless doing so is necessary to provide goods or services requested by the individual.

3) Makes it unlawful for a covered entity or service provider that collects location information to do any of the following:

    a) Collect or process more location information than is necessary.

        i) This prohibition does not apply to collecting or processing location information to respond to security incidents, fraud, harassment, malicious or deceptive activities or other limited purposes, as described.

        ii) Location information collected and processed under the exception is limited to that which is necessary to carry the purpose and shall not be retained for more than 24 hours.

    b) Retain location information longer than necessary.

    c) Sell, rent, trade, or lease location information to third parties.

    d) Derive or infer from location information any data that is not necessary to provide the goods or service requested.

    e) Disclose, cause to disclose or assist with or facilitate the disclosure of an individual's location information to third parties, unless the disclosure is necessary to provide the goods or services, or the individual requests disclosure.

    f) Disclose location information to any federal, state, or local government agency or official unless they are served with a valid court order issued by a California court or a court from another jurisdiction that is in keeping with California's laws.

4) Makes it unlawful for a state or local agency to monetize location information.

5) Requires a covered entity to prominently display, at the point where the location information is being captured, a notice informing people that their location information is being collected, the name of the entity and service provider collecting the information and a phone number and website where the individual can obtain more information.

6) Requires a covered entity to maintain and make available to individuals a location privacy policy.

7) Requires a covered entity, 20 business days in advance, to provide notice to any individuals who have had their location data collected if its privacy policy is changing. In addition, the covered entity is required to obtain consent before collecting or processing location information in accordance with the new policy.

8) Provides the California Privacy Protection Agency with enforcement authority.

9) Provides that a prevailing plaintiff who suffers harm as a result of a violation of these provisions may recover all of the following:

    a) Actual damages.

    b) An amount determined by a jury or the court for exemplary damages.

    c) A civil penalty of $25,000.

    d) Preventive relieve, including an injunction, restraining order, or other order against the persons responsible.

    e) Reasonable attorney fees and court costs.

10) Authorizes the Attorney General, a district attorney, county counsel, or city attorney to bring a civil action.

11) Establishes a three year statute of limitations.

12) Exempts location information collected from a patient by a health care provider or health care facility if the information is protected from disclosure under the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1), or other applicable federal and state laws and regulations pertaining to health care privacy.

13) Defines the following terms:

    a) "Automated license plate recognition information," or "ALPR information" means information or data collected through the use of an ALPR system.

    b) "Automated license plate recognition system" or "ALPR system" means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data.

    c) "Collect" means to obtain, infer, generate, create, receive, or access an individual's location information.

    d) "Covered entity" means any individual, partnership, corporation, association, or other group. A covered entity includes all agents of the entity. A covered entity does not include a state or local agency, or any court of California.

    e) "Disclose" means to make location information available to a third party, including, but not limited to, by sharing, publishing, releasing, transferring, disseminating, providing access to, or otherwise communicating that location information orally, in writing, electronically, or by any other means.

f) "Facial recognition technology" or "FRT" means a system that compares a probe image of an unidentified human face against a reference photograph database, and, based on biometric data, generates possible matches to aid in identifying the person in the probe image.

g) "Location information" means information derived from a device or from interactions between devices, with or without the knowledge of the user and regardless of the technological method used, that pertains to or directly or indirectly reveals the present or past geographical location of an individual or device within the State of California with sufficient precision to identify street-level location information within a range of five miles or less. Location information includes, but is not limited to, the following:

   i) An internet protocol address capable of revealing the physical or geographical location of an individual.

   ii) Global Positioning System (GPS) coordinates.

   iii) Cell-site location information.

   iv) Information captured by an automated license plate recognition system that could be used to identify the specific location of an automobile at a point in time.

   v) Information or image captured by a speed safety system or other traffic monitoring system that could be used to identify the specific location of an automobile at a point in time.

   vi) A video or photographic image that is used as a probe image in a facial recognition technology system that could be used to identify the specific location of an individual at a point in time.

h) "Monetize" means to collect, process, or disclose an individual's location information for profit or in exchange for monetary or other consideration. This term includes, but is not limited to, selling, renting, trading, or leasing location information. "Monetize" does not include the disclosure of public records for purposes of the California Public Records Act (Division 10 (commencing with Section 7920.000) of Title 1 of the Government Code).

i) "Probe image" means an image of a person that is searched against a database of known, identified persons or an unsolved photograph file.

j) "Process" means any operations that are performed on location information, whether or not by automated means.

k) "Sale" means selling, auctioning, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, an individual's location information by the covered entity to a third party for monetary or other valuable consideration.

l) "Service provider " means an individual, partnership, corporation, limited liability company, association, or other group, however organized, that collects, processes, or transfers location information for the sole purpose of, and only to the extent that the

service provider is, conducting business activities on behalf of, for the benefit of, at the direction of, and under contractual agreement with a covered entity.

m) "Speed safety system" means a fixed or mobile radar or laser system or any other electronic device that utilizes automated equipment to detect a violation of speed laws and obtains a clear photograph of a speeding vehicle's license plate.

EXISTING LAW:

1) Provides, pursuant to the U.S. Constitution, that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." (U.S. Const., Fourth Amend; *see also* Cal. Const. art. 1, § 13.)

2) Provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these is the fundamental right to privacy. (Cal. Const. art. I, § 1.)

3) States 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." Further states these findings of the Legislature:

   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.

   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 § 1798.1.)

4) Requires the Fair Political Practices Commission to redact the signature, telephone number, email address, and mailing address of the filer of a statement of economic interest. In addition, at the request of the filer, redacts a business address which is the same as the filer's personal residence. (Gov. Code § 87500.3.)

5) Authorizes a current or former elected official to request that the Fair Political Practices Commission redact the names and addresses of family members, the address of their employer, and the name of an entity that includes a family member's name or address in the entity's name, if there is a privacy concern. (Gov. Code § 87500.3.)

6) Authorizes a survivor of domestic violence, sexual assault, stalking, human trafficking, child abduction, or elder or dependent abuse to petition the Secretary of State to not have their address disclosed. (Gov. Code § 6206.)

7) Authorizes a reproductive health care service provider, employee, or volunteer who is fearful for their safety to petition the Secretary of State to not have their address disclosed. (Gov. Code § 6215.2.)

8) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. (Pen. Code § 1546 et seq.)

9) Establishes the California Consumer Privacy Act (CCPA). (Civ. Code §§ 1798.100-1798.199.100.)

10) Prohibits a business from selling or sharing the personal information of a child that is 16 years of age or younger, if the business has actual knowledge of the child's age, unless the child, or the child's parent or guardian in the case of children less than 13 years old has affirmatively authorized the sharing of selling of the personal information. (Civ. Code § 1798.120(c).)

11) Provides a consumer, subject to exemptions and qualifications, various rights, including the following:

    a) The right to know the business or commercial purpose for collecting, selling, or sharing personal information and the categories of persons to whom the business discloses personal information. (Civ. Code § 1798.110.)

    b) The right to request that a business disclose the specific pieces of information the business has collected about the consumer, and the categories of third parties to whom the personal information was disclosed. (Civ. Code § 1798.110.)

    c) The right to request deletion of personal information that a business has collected from the consumer. (Civ. Code § 1798.105.)

    d) The right to opt-out of the sale of the consumer's personal information if the consumer is over 16 years of age. (Sale of the personal information of a consumer below the age of 16 is barred unless the minor opts-in to its sale.) (Civ. Code § 1798.12.)

    e) The right to direct a business that collects sensitive personal information about the consumer to limit its use of that information to specified necessary uses. (Civ. Code § 1798.121.)

    f) The right to equal service and price, despite the consumer's exercise of any of these rights, unless the difference in price is reasonably related to the value of the customer's data. (Civ. Code § 1798.125.)

12) Requires a business to provide clear and conspicuous links on its homepage allowing consumers to opt-out of the sale or sharing of their personal information and use or disclosure of their sensitive personal information. (Civ. Code § 1798.135(a).)

13) Establishes the California Privacy Protection Agency (Privacy Agency), vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. The Privacy Agency is governed by a five-member board, with the chairperson and one member appointed by the Governor, and the three remaining members are appointed by the Attorney General, the Senate Rules Committee, and the Speaker of the Assembly. (Civ. Code § 1798.199.10.)

14) Defines the following terms under the CCPA:

    a) "Personal information" means 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. Personal information includes such information as:

        i) Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other identifier.

        ii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

        iii) Biometric information.

        iv) Internet activity information, including browsing history and search history.

        v) Geolocation data.

        vi) Audio, electronic, visual, thermal, olfactory, or similar information.

        vii) Professional or employment-related information. (Civ. Code § 1798.140(v).)

    b) "Sensitive personal information" means personal information that reveals a person's:

        i) Social security, driver's license, state identification card, or passport number.

        ii) Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials.

        iii) Precise geolocation.

        iv) Racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

        v) Email, mail and text messages.

        vi) Genetic data.

        vii) Information collected and analyzed relating to health.

        viii) Information concerning sex life or sexual orientation. (Civ. Code § 1798.140(ae).)

15) Establishes the Data Broker Registration Law (DBRL). (Civ. Code §§ 1798.99.80-1798.99.88.)

16) Defines a "data broker" as a business that knowingly collects and sells the personal information of a consumer to a third party that the business that it does not have a direct relationship with. (Civ. Code § 1798.99.80.)

17) Requires data brokers to register annually with the California Privacy Protection Agency (CPPA) and provide specified information. (Civ. Code § 1798.99.82.)

18) Requires the CPPA, by January 1, 2026, to develop an accessible deletion mechanism that allows a consumer to request the every registered data broker delete any personal information held by the broker. (Civ. Code § 1798.99.86.)

COMMENTS:

1) **Author's statement**. According to the author:

> Location data is among our most sensitive information; it can expose sensitive information such as medical conditions, sexual orientation, political actives, and religious beliefs. The sale of location data undermines our civil liberties, and puts our most vulnerable populations at risk of discrimination, intimidation and violence. AB 1355 allows Californian's to take back control of their sensitive information and ensures that our location data is never sold to the highest bidder.

2) **Tracking our every move.** Americans leave a trail of personal data with almost every action they take either in the physical world or online, including every website visited, credit card payment, browser search.[2] As the author notes, Californians are more vulnerable to digital exploitation than ever before.

In the physical world, we cannot step out of our homes without being monitored and tracked. Cars collect location data everywhere we drive. Phones, our constant companions, collect location data everywhere we go. If a car is too old to collect location data and a person leaves their phone at home, license plate readers and traffic cameras are at virtually every intersection, on freeways, at the entrance of parking garages, in store parking lots, and toll roads. These devices are tracking the movement of every single car that passes by. Even if someone walks or rides a bicycle, security cameras on homes and business can capture their movements and their location. Our faces may not be captured by the cameras we travel past every day, but with advances in technology our face no longer needs to be captured. Analyzing a person's walk and movements using gait recognition technology is enough to identify them.[3] In addition, most stores and businesses use security cameras and images from those cameras can easily be run through facial recognition systems to identify the people walking through their doors. It has become virtually impossible for people to move through the United States without being tracked.

---

[2] Emile Ayoub and Elizabeth Goitein. *Closing the Data Broker Loophole*, The Brennan Center for Justice (Feb. 13, 2024).
[3] *Gait recognition system: deep dive into this future tech*, recfaces.com blog post, https://recfaces.com/articles/what-is-gait-recognition

The slow erosion of privacy, through the collection of what seem to be relatively small pieces of personal information, may not cause people to be overly concerned. However, those pieces of information are being amassed into dossiers that disclose every aspect of the lives of everyone in the United States. The fact that these dossiers are being made available to individuals, private companies, and local, state, and federal government agencies should alarm everyone. University of Virginia Law Professor Danielle Citron warned in an interview with *The Guardian* in 2022, "We don't viscerally appreciate the ways in which companies and governments surveil our lives by amassing intimate information about our bodies, our health, our closest relationships, our sexual activities and our innermost thoughts. Companies are selling this information to data brokers, who are compiling dossiers with about 3,000 data points on each of us."[4]

A 2023 investigation by Consumer Reports on the surveillance economy looked at the companies that share people's personal information with Facebook. Consumer Reports explains:

> One way to understand [the surveillance economy] is as the subset of consumer marketing in which the data being used is obtained from the surveillance, or covert observation, of ordinary consumer activities such as visiting websites, buying goods or services from an online or physical retailer, using one's credit card, and consuming entertainment content.
>
> The surveillance economy is "cross-contextual," meaning that it uses information about individuals that's been collected in one context—such as a website visit, an action taken in an app, or a visit to a physical location—and applies it to another context to affect how you are advertised to, what prices you see, and how you are otherwise treated.[5]

The findings of the study were breathtaking. 709 of their participants had their personal information shared by 186,892 companies. On average, each participant was represented in data shared by 2,230 different companies and some were represented in data shared by over 7,000 companies.[6] In a state that requires its residents to contact businesses and request that they delete their information or opt out of its collection in the first place, it would be virtually impossible for a California consumer to identify which companies have their personal information, much less request that it be deleted. Notably, once the Delete Act[7] is fully implemented, it will become significantly easier for consumers to request deletion from data brokers. However, even with that act, the onus remains on consumers to find CPPA's website and request that their information be deleted.

The information in these dossiers is not benign. It goes well beyond information on the products people purchase, the websites they visit, and other data that reflects their general interest. The reality is these dossiers contain sensitive personal information that can be dangerous if disclosed to the wrong entity. Perhaps the most dangerous data being collected and sold on every Californian is detailed information on their precise location. Despite the laws passed in California in recent years aimed at protecting the privacy of vulnerable groups, government

---

[4] Laurie Clarke. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.
[5] Don Marti, et al. "Who Shares Your Information with Facebook? Sampling the Surveillance Economy 2023," *Consumer Reports* (Jan. 2024) https://advocacy.consumerreports.org/research/report-who-shares-your-information-with-facebook/
[6] *Ibid.*
[7] See Section #6.

officials, healthcare workers, or Californians in general – everywhere people in California go, how often they go, how long they stay, where they sleep at night, the routes they take travelling to and from work or dropping children off at school, are all collected and available from location data brokers to anyone who is willing to pay.

Location data brokers collect billions of location data points linked to unique persistent identifiers and timestamps that could provide detailed insights into people's movements. This information is then repackaged and sold to their clients, who often use it to trace the movements of individuals to and from sensitive locations. These include medical facilities, places of religious worship, places used to infer an LGBTQ+ identification, domestic abuse shelters, substance use disorder treatment facilities, and homeless shelters. Further, data collected is not anonymized, it is possible to identify the exact identity of the mobile device owner.

As an example of the information location data brokers are capable of providing, a customer could request individualized data on everyone on the Assembly floor during a floor session on a specific date from a location broker. They could then ask the broker to track the movements of those mobile devices over a two week period, allowing them to determine where individual members stay in Sacramento and where they stay when they return to their districts. The customer could then ask the broker to geo-fence their homes and identify the distinct devices within the home and track the movements of those individuals over the same time period. One could do the same for reproductive healthcare workers, judges, or any other group of individuals who may be at risk of being targeted during this politically volatile period in the United States.

3) **Federal Trade Commission (FTC) Complaints.** According to the author, over the last few years, the FTC has recieved numerous complaints against location data brokers who are collecting and selling the location information on hundreds of millions of people. Four of those complaints were filed in 2024. A review of five of the complaints filed by the FTC reveals common business practices among the location data brokers, among them:

- The brokers amass and sell raw location data that tracks consumers' movements so that their customers can glean insights into the consumers' private lives.

- The brokers also use the data to identify consumers based on attributes and behaviors the data reveals, including sensitive and personal attributes and behaviors, and they disclose the information to their customers.

- The brokers do not collect the mobile location data directly from consumers. Generally the location brokers obtain the location data from other data brokers. Those brokers, in turn, obtain the data from other brokers, the mobile advertising marketplace, or mobile applications.

- For the most part, consumers have no interactions with the brokers and have no idea that they have obtained their location data.

- Once the information is collected, the information can be sold multiple times to companies that the consumer has never heard of and the consumers have no insight into how this data is used and the associated risks. Because of the opaque nature of this industry, consumers are unable to take any reasonable steps to contain their data.

- The data collected is not anonymized making it possible to identify the exact identity of the mobile device owner by combining the consumer's geolocation data and the mobile device's Mobile advertising ID (MAID), which are alphanumeric identifiers that iOS or Android platforms assign to each mobile device.

Gravy Analytics, Inc. This location broker claims that it collects, processes, and curates over 17 billion signals from approximately one billion mobile devices on a daily basis. They further claim that their location data is accurate within approximately one meter (3.3 feet). The company, in its marketing materials, also claims that they associate each data signal with a location by tracing the walls of the building so that their data is "based on real people visiting real locations" without any "modeling."[8]

Gravy Analytics also sells a tool that allows their customer to geo-fence a location and obtain a list of MAIDs that were present at that location during a specific timeframe. The FTC complaint found that Gravy Analytics had used geo-fencing to create a list of MAIDs that visited specific churches and health-related events for their customers.

Gravy Analytics focuses on selling the location data to commercial customers, while its subsidiary, Venntel, sells the information to public sector customers. Venntel offers enhanced tools to its customers, including allowing their customer to continuously track a single device. The location data and enhanced tools are marketed as available for use for government purposes. Venntel also tells potential customers that "location data makes it possible to gain real-life insight into a device users' patterns-of-life (POL), locations visited and known associates." It further notes that over a 90-day tracking the company is able to identify a user's "bed down location, work location, and visits to other [United States Government] building."[9]

Gravy Analytics explains to its customers that the geolocation data it collects and sells not only reveals where consumers go and what they do, but that it can also be used for "psychographic analysis" meaning that it is analyzed to understand consumers "values, interests, [and] lifestyles." It asserts that the location data is "deterministic." The company uses this analysis to create "audience segments" or subsets of consumers who share interests or characteristics. Among they segments they advertise are "Early Risers," "Healthy Dads," "Sports betting Enthusiasts," "Political Activists," "Women's Health," and "New Parents/Expecting." It claims that it has associated over 250 million MAIDs of consumers with at least one audience segment.[10]

Mobilewalla, Inc. This company claims that it collects 50 billion mobile signals a day from 2.2 billion devises for 40 countries and stores over five years worth of data. This broker touts its ability to "create a comprehensive, cross channel view of the customer, understanding online and offline behavior." Mobilewalla estimates that it collected more than 2 billion unique advertising identifiers between 2018 and 2020. According to a March 2020 email from the company's CEO obtained by the FTC, the company has the ability to identify consumers' home addressing using a consumer's mobile device location history and it is more accurate than its competitors because

[8] 212-3035 In the matter of Gravy Analytics, Inc. and Venntel, Inc. U.S. Federal Trade Commission.
[9] *Ibid.*
[10] *Ibid.*

of their ability to store longer periods of data. Mobilewalla claims it can target geolocation to a radius as small as 25 meters (approximately 82 feet). [11]

The company has used sensitive information to create audience segments that helped clients target pregnant women, Hispanic churchgoers, and members of the LGBTQ+ community. It has created geo-fences around pregnancy centers and maternity clinics; created retroactive geo-fences around the sites of political rallies and protests; and, geo-fenced polling places and state capitols to identify devices belonging to consumers who visited those locations and identifying home addresses found within the geo-fence by tracking where the individuals spends the evening. In addition, for one client Mobilewalla created a geo-fence around the home addresses of a set of employees and certain healthcare centers, in order for the client to "poach these nurses from these centers to a competitor." Finally, in other non-advertising activities, it attempted to geo-fence a work location to track where union organizers travel.[12]

Kochava, Inc. According to FTC court filings, this location broker sold data that allows entities to track individuals' movements from sensitive locations, including locations associated with medical care, reproductive health, religious worship, mental health, and domestic violence shelters. The company claims that its location data feed delivers latitude/longitude data of around 94 billion geo transactions per month, 125 million monthly active users, and 35 million daily users, on average observing more than 90 daily transactions per device."[13]

The company has sold access to its data feeds on online marketplaces that are publicly accessible. It typically charges a monthly subscription fee of thousands of dollars to access its data feed, but it also offers a free sample. The sample consisted of a subset of the paid data feed, covering a rolling seven-day period. According to the FTC, in just using the data sample it was possible to identify a mobile device that had visited a women's reproductive health clinic and trace that device to a single-family residence. The data set also revealed that the same device was at a particular location at least three evenings in the same week, suggesting the device user's routine. The sample data also identified a device that appears to have spent the night at a temporary shelter for at-risk, pregnant young women or new mothers.[14]

5) **Other types of data that could disclose someone's location.** As noted previously, it is not just location data collected by mobile devices that can track an individual's location. The author notes that technologies like automated license plate readers and facial recognition cameras have become ubiquitous in public spaces. This means even if a consumer takes steps to reduce their personal device use, they are not able to avoid near constant surveillance while interacting in public.

Specifically, the proliferation of both privately owned and publicly owned license plate readers track where people drive and park. Fixed and mobile license plate recognition cameras take photos of license plates, capturing the date, time, and GPS coordinates of where the photo was taken. Each plate image captured, along with the data for that image (date, time, location), is stored in a database as records that can be searched. At least one company, Vigilant Solutions,

---

[11] 202-2196 In the Matter of Mobilewalla, Inc. United States Federal Trade Commission.
[12] *Ibid.*
[13] *Federal Trade Commission v. Kochava, Inc*., 2:22-cv-00377, (D. Idaho).(Aug. 12, 2022) https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc
[14] *Ibid.*

has amassed billions of license plate records throughout the county that allow law enforcement officials to monitor the movements of individuals. In their marketing materials, Vigilant claims:

> Vigilant Solutions creates highly innovative and essential tools for law enforcement – tools that ultimately saves lives. As an example, Vigilant Solutions' Automated License Plate Recognition (ALPR / LPR) product is the most comprehensive offering available, with over tens of thousands of users around the world and thousands of success stories.
>
> Data is cumbersome; intelligence is actionable. Vigilant Solutions' products are designed to collect, organize and share data to credentialed law enforcement personnel, providing intelligence that is readily accessible and easy to use. This intelligence provides more efficient and effective law enforcement while enhancing officer safety.
>
> *Vigilant Solutions creates intelligence by merging previously disparate data sets such as fixed and mobile license plate recognition, privately collected LPR data, facial recognition, and more.*[15] Vigilant's LEARN Intelligence Network provides an easy to use and intuitive interface to all of this information for unmatched investigative capability in a secure, hosted environment to reduce demands on agency IT resources and to facilitate nationwide interoperability and data sharing.[16]

All of this tracking information, potentially tracking people to sensitive locations, is available to any paying law enforcement agency eliminating the need for them to obtain a court order, warrant, or subpoena. Vigilant boasts, "Even without [license plate reader] cameras, you can benefit by using our Commercial Data. We are the only [license plate reader] provider that can offer over 5 billion nationwide detections and over 150 million more added monthly. We believe the power of LPR is in the data and analytics. In addition to access to our commercial data, agencies can choose to share with other law enforcement agencies to gain access to another 1.5B detections nationwide."[17]

Beyond license plate readers, facial recognition technology (FRT) is becoming more ubiquitous. Private entities, including small business and home security services have begun using FRT systems that identify individuals by their faces, or in some cases their bodies. All of this data is captured and stored in private or commercial databases, identifying the individual, the GPS data, and the date and time the image was captured. Real time FRT can be used by commercial businesses to determine when an individual walks into a store, allowing the person to be closely monitored and tracked as they move throughout the store.

Home security systems that include facial recognition, facial detection, and automobile detection can be purchased on Amazon for less than $500. Similarly, door bells and door locks using facial recognition and other biometric data are available for around $200. All of this biometric data that is captured needs to be stored and depending on the companies' terms and conditions, could potentially wind up in a commercial database that may be accessed by data brokers and others, revealing the identity and location of any individual who passes by those security cameras.

---

[15] Emphasis added.
[16] https://www.ra-comm.com/vigilant-solutions/
[17] https://induscom.com/motorola/vigilant/

6) **The Delete Act.** The California Privacy Protection Agency (Privacy Agency) is currently in the process of implementing SB 362 (Becker; Stats. 2023, Ch. 709), commonly known as the Delete Act. Under this act, the Privacy Agency is required to develop a mechanism that allows Californians, with one request, to require that data brokers who have registered with the Privacy Agency delete their personal information. The Privacy Agency estimates that the mechanism will be available on its website by January 1, 2026. By August 1, 2026, registered brokers are required to access the deletion site once every 45 days to carry out the requested deletions.[18]

To the extent Californians are aware of the option once it is implemented, this mechanism will significantly improve their ability to control which entities have access to their personal information. This bill goes beyond the Delete Act in several ways, including:

1. It places the onus on the businesses by prohibiting them from collecting and processing location information beyond the data necessary to provide a requested good or service. In addition, it strictly prohibits the sharing and sale of location data and requires its deletion once the good or service is provided. The Delete Act, like the CCPA, requires people to opt out of the sharing and sale of their personal information, no matter how sensitive, and requires them to request deletion.

2. It applies to any entity that collects location data, with the exception of state and local government agencies and the state courts. The Delete Act only applies to data brokers.

3. The collection, sale, sharing, and use of location information is protected for anyone within the borders of the state, meaning that anyone who enters the state, perhaps seeking abortion care or gender affirming care would be protected. The protections in the Delete Act are only available for California residents.

4. Precise location is protected within a radius of five miles. Precise geo-location data that is protected as sensitive personal information is limited to within 1,850 feet under the Delete Act.

5. "Location information" is defined much more broadly in this bill, including, but not limited to, GPS data, internet protocol addresses, cell-site information, and data captured by license plate readers and traffic cameras. In addition, it includes any device or data that is capable of determining a person's location, whether or not that is the intention of the particular device. Geolocation data in the Delete Act is limited to "data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area."[19]

6) **What this bill would do.** The author's intent in carrying this bill is to safeguard the privacy of Californians and those visiting the state by placing strict restrictions on the collection, use and sale of location data. The bill would accomplish that by doing the following:

- Restricting covered entities – an individual, partnership, corporation, limited liability or other group, with the exception of a state or local agency or the California courts – from collecting and processing the location data of an individual within the borders of

[18] Civ. Code §§ 1798.99.80 – 1798.99.89.
[19] Civ. Code § 1798.140(w)

California unless doing so is necessary to provide goods or services requested by the individual.

- Making it unlawful for covered entities who collect location information to do any of the following:
    - Collect or process more location data than is necessary to provide the specific goods or services.
    - Retain location information longer than necessary to provide the requested goods or services, with the exception of the collection or processing of information to respond to security incidents, fraud, harassment or other legal activities. In those instances the information can only be retained for up to 24 hours.
    - Sell, rent, trade, or lease location information to third parties.
    - Disclose or cause to be disclosed an individual's location information unless the disclosure is necessary for the service being provided or is requested by the individual to whom the information pertains.
    - Disclose location information to any federal, state, or local government agency or official unless the covered entity is served with a valid court order issued by a California court or a court order from another jurisdiction that is in keeping with California's laws.
    - Derive or infer from the location information any additional information that is not necessary for the service being provided.
- Making it unlawful for a state or local entity to monetize location information.
- Requiring a covered entity to prominently display, at the point where the location information is being captured, a notice informing individuals of the collection of their location data, the name of the covered entity and service provider collecting the information, and a phone number and internet website where individuals can obtain more information.
- Requiring a covered entity to make available a privacy policy that includes, at a minimum, the following:
    - The good or service that requires the collection and use of location information.
    - The type of location information collected, including the precision of the data.
    - The identities of service providers who the covered entity has contracted with to collect and process the data.
    - Any disclosures of the location information that are necessary in order to provide the good or service requested and the identities of the third parties with whom the location data could be disclosed.
    - Data management and security policies.

- The retention schedule and guidelines for deleting the data.

- Defining location information as information derived from a device or from interaction between devices that identifies the present or past geographical location of an individual or device within the State with sufficient precision to identify street level location information within a range of five miles or less.

- Defining location information as including, but not limited to, the following:

  - An internet protocol address capable of revealing an individual's location.

  - GPS coordinates.

  - Cell-site location information.

  - Information captured by an automated license plate recognition system.

  - Information or an image captured by a speed safety system or other traffic monitoring system.

  - A video or photographic images used for facial recognition.

7) **Challenges with California's privacy laws.** In 1972, at the Legislature's urging, the people of California used the initiative process to add "privacy" to the list of "inalienable rights" in the state constitution.[20] Proponents noted the initiative was specifically designed to preserve Californians' private lives and fundamental rights in the face of technological advances. They argued: "The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes. . . ."[21]

In 2018, the Legislature enacted the California Consumer Privacy Act (CCPA; AB 375 (Chau, Chap. 55, Stats. 2018)), which gave consumers certain rights regarding their personal information,[22] such as the right to: (1) know what personal categories of information about them are collected and sold; (2) request the deletion of personal information; and (3) opt-out of the sale of their personal information, or opt in, in the case of minors under 16 years of age.

Subsequently, in 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which established additional privacy rights for Californians. Chief among these rights was the right of a consumer to limit a business's use of sensitive personal information.[23] One of the key components of the initiative was establishing that the CCPA was a floor and not a ceiling for privacy protection. Essentially, to protect Californians from any future legislative efforts to weaken statutory protections in the CPRA, Proposition 24 provided that the CPRA's contents may be amended by a majority vote of the Legislature only if the amendments are

---

[20] California Proposition 11 (1972), "Constitutional Right to Privacy Amendment."
[21] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.
[22] Civ. Code § 1798.140(v). See **EXISTING LAW** #14(a) for definition.
[23] Civ. Code § 1798.140(ae). See **EXISTING LAW** #14(b) for definition.

consistent with and further the purpose and intent of the CPRA, which is to further protect consumers' rights, including the constitutional right of privacy.[24]

At the time, California had the most comprehensive laws in the country when it came to protecting consumers' rights to privacy. Since the passage of the CCPA, however, 19 additional states have passed comprehensive privacy laws. Of those states, 17 have laws that are more privacy protective. 16 states require consumers to "opt in" to the sharing and sale of sensitive information and one state, Maryland, prohibits the sharing of sensitive information entirely.[25] In the states that have come after California, privacy is the default.

The CCPA, on the other hand, relies on consumers actively exercising their rights to "opt out" of the sharing and sale of their personal information and the sharing, sale and use of their sensitive personal information. The challenge is that in order to exercise those rights, consumers must first find the businesses that have collected their personal information and then find a way to contact the company to exercise those rights. It is likely that the average consumer often does not even realize that their personal information is being harvested, used to micro target them for advertising, and sold as a commodity to other companies.

As it pertains to this bill, it is unlikely that the Legislature and the voters contemplated the proliferation of location data brokers and the constant surveillance of everyone in the United States when considering the CCPA and the CPRA. The location intelligence market in the United States was estimated to be around $3 billion in 2020, the year voters approved the CPRA.[26] By 2025, it has nearly doubled and is expected to grow to over $12 billion by 2030.[27] Globally, the market revenue was over $21 billion and is estimated to grow to approximately $54 billion by 2030. Fortunately, as noted above, the proponents of the CPRA and the voters understood that the Legislature may need to move beyond the CCPA in order to continue to protect Californian's right to privacy.

Overall, one could argue that the State's current privacy laws, including laws protecting Californians from government surveillance and protections against unreasonable searches and seizures without an appropriate court order, fall short of the protections envisioned by the Legislature and the voters in 1972. The proponents argued for a much more stringent level of protection – the right to be left alone. The authors of that proposition promised that adding a right to privacy would ensure the protection of "our homes, our families, thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose."[28] In 2025, a person would be hard-pressed to find that level of privacy in their homes, much less in public spaces the moment they step outside.

---

[24] Ballot Pamphlet. Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74
[25] A comparison chart of state privacy laws can be accessed at https://45555314.fs1.hubspotusercontent-na1.net/hubfs/45555314/Slides%20and%20one-pagers/US%20state%20law%20comparison%20chart_2024_July_1.pdf.
[26] *Global Location Intelligence Industry (2020 to 2027) - Key Market Trends and Drivers*, BusinessWire (May 19, 2021) https://www.businesswire.com/news/home/20210319005168/en/Global-Location-Intelligence-Industry-2020-to-2027---Key-Market-Trends-and-Drivers---ResearchAndMarkets.com
[27] *U.S. Location Intelligence Market Size & Outlook*, Horizon Grandview Research https://www.grandviewresearch.com/horizon/outlook/location-intelligence-market/united-states
[28] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props..

Opponents of the bill argue that "[c]onsumers already have significant protections around how their location data can be collected and used by businesses under the CCPA, and by government entities under the California Electronic Privacy Act (CalECPA)."

One could argue, if the CCPA were sufficient, government officials, stalking victims, and survivors of intimate partner violence would be protected from having their location and the locations of their loved ones made available for a price by data location brokers. Similarly, the ability of law enforcement to purchase sensitive personal information, including location data, from third party vendors without first seeking permission from a court also renders CalECPA largely ineffective.

Prioritizing protecting vulnerable Californians. In recent years the Legislature has passed numerous laws designed to protect California's most vulnerable populations by passing laws like the California Values Act, which built on previous "sanctuary" policies with regard to assisting federal immigration efforts—and extended them—by establishing statewide non-cooperative policies between state law enforcement officials and federal immigration authorities.

In addition to protecting Californians who emigrated from other countries, California is a reproductive freedom state. In September 2021, over 40 organizations came together to form the California Future Abortion Council (CA FAB) to identify barriers to accessing abortion services and to recommend policy proposals to support equitable and affordable access for not only Californians, but all who seek care in this state. CA FAB issued its first report in December 2021, which included 45 policy recommendations to protect, strengthen, and expand abortion access in California.[29]

On June 24, 2022, the Supreme Court overturned *Roe v. Wade.* In response to that decision and CA FAB's report, California enacted a comprehensive package of legislation that protects the rights of patients seeking abortion in the state and those supporting them. Finally, the voters overwhelmingly approved Proposition 1 and enacted an express constitutional right in the state constitution that prohibits the state from interfering with an individual's reproductive freedom in their most intimate decisions.[30] The Legislature continues to work to make sure that the sensitive personal information of the women and girls who come to California seeking abortion care and the doctors who treat them are protected. In addition, with increasing attacks on people who are transgender, especially young people seeking gender affirming care, the Legislature has taken steps to ensure that their rights are protected, particularly their right to privacy.

This bill is not only in keeping with the Legislature's longstanding goal of ensuring that California is a place of sanctuary and refuge for all that need it, by arguably closing a back door that allows other jurisdictions to circumvent California's protections by simply purchasing massive amounts of location data from location data brokers.

ARGUMENTS IN SUPPORT: Consumer Reports, sponsors of the bill, write in support:

> The location information market is a multi-billion-dollar industry centered on collecting and selling people's everyday comings and goings, often collected from people's mobile devices

---

[29] California Future of Abortion Council, *Recommendations to Protect, Strengthen, and Expand Abortion Care in California* (Dec. 2021) https://www.cafabcouncil.org/_files/ugd/ddc900_0beac0c75cb54445a230168863566b55.pdf.

[30] Nov. 8, 2022 gen. elec.

and often without their knowledge or explicit consent. Location data is an extremely sensitive form of personal information. Researchers have shown that 95 percent of individuals can be uniquely identified from just four location points in time and 50 percent of individuals can be uniquely identified from just two spatio-temporal points; most companies that collect this information have orders of magnitude more data than that.

Much of this information is amassed by data brokers, entities that compile extensive dossiers on virtually every American that include thousands of data points, including extremely granular information about people's behavior, as well as inferences about individuals based on their information. Some companies collect and share consumers' location information as often as every three seconds. This information is then sold and resold, often for marketing but for a variety of other purposes as well, eroding consumers' basic expectation of privacy in the process. This activity poses a host of significant risks to California residents.

A few examples of location information-driven harms include:

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use location data brokers to target vulnerable individuals for scams, or otherwise use personal information to cause harm. For example, scammers can use commercially available location information to increase the specificity of their phishing or social engineering scams, such as by including location-specific details like mentioning a nearby business or the individual's recent activity. Location data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.

- *Predatory use of consumer data*. Data brokers sell information about people who rarely even know the companies even exist—and who have rarely ever affirmatively, expressly consented to this information collection and sale. In some instances, this can result in financially disastrous consequences for consumers. Some data brokers sell lists of consumers sorted by characteristics like "Rural and Barely Making It" and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products. And a recent case brought by the Texas Attorney General alleged that Arity, a data broker owned by the insurance company Allstate, secretly harvested information from drivers, including their precise geolocation data, which it used in some cases to raise consumers' premiums or deny them coverage altogether. They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

- *Enhanced risks of data breaches.* Data brokers collect trillions of data points on Americans, so they are unsurprisingly a top target for hackers and cyber criminals. Location data broker Gravy Analytics, which has claimed to "collect, process and curate" more than 17 billion signals from people's smartphones every day, reportedly suffered a massive data breach that may have leaked the location information of millions of individuals. This type of information makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.

The California Immigrant Policy Center argues:

> Californians are in a state of constant surveillance, and our location, either past or present, is constantly being tracked, and stored for uses not disclosed at the time of collection. Entities referred to as Location Data Brokers (LDB) are amassing this information for the purpose of selling products or services created form or based on consumer location data. The Federal Trade Commission recently reported in a 2024 complaint that among their top customers are hedge funds, insurance companies, advertisers, and government agencies Immigration and Customs Enforcement (ICE).
>
> Location data is among our most sensitive information; it can expose sensitive information such as medical conditions, sexual orientation, political activities, and religious beliefs. When collected across time, this data can reveal every aspect of a consumer's life. The sale of location data undermines our civil liberties, and puts our most vulnerable populations at risk of stigma, discrimination, and violence. California must take bold action to ensure consumers are protected, and their most sensitive information is secure.

A coalition of supporters, including the Electronic Frontier Foundation and PFLAG Sacramento further state:

> [I]t is imperative we protect the privacy rights of our communities, especially with increased attacks targeting our immigrant, Black, and Brown community members, and individuals seeking health services, such as reproductive health and gender-affirming care.
>
> California must take bold action to ensure consumers are protected and their location information is secure. The California Location Privacy Act answers this call.

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of business organizations argue:

> The California Chamber of Commerce and the undersigned must respectfully OPPOSE AB 1355 (Ward), as amended on April 10, 2025, because it seeks to place new restrictions around location data collection and use practices by businesses in California in a manner that will undermine and cause confusion with the California Consumer Privacy Act, which already addresses these policy questions and data privacy concerns. The CCPA is a comprehensive, industry neutral, and technology neutral statutory scheme that already provides strong consumer privacy protections around the collection, use, and disclosure of all Californians' personal information – including location data.
>
> That has been the case since the law was first enacted in 2018, and voters both reaffirmed that in 2020 and strengthened those protection when they made a consumer's precise geolocation sensitive personal information as well, granting the consumer additional privacy rights and control over that information. Notably, it was only on March 31, 2023, that the new California Privacy Rights Agency's first package of Proposition 24 implementing regulations became effective, yet at every turn, businesses face additional legislation that seeks to duplicate rights and renegotiate elements of the law in new statutes outside of the CCPA.
>
> [. . .]
>
> Should AB 1355 move forward, there are a host of practical outcomes that should be considered. To name just a few, but not all:

Emergency Alerts. The sale of precise geolocation data powers important emergency notices, such as missing children alerts and severe weather alerts. The sale or transfer of precise geolocation data allows AMBER alert notices as well as information regarding extreme weather to be immediately displayed to users in the impacted area on any device they are using. Even if you exempt the use of data for certain emergency purposes, if AB 1355 becomes law, precise geolocation data will lose much of its utility in the marketplace. As a result, this data will be less likely to be collected and used, making it less procurable for use for emergency alert purposes. Californians may therefore lose access to these important, real-time alerts, which rely on the transfer or sale of precise geolocation data.

Advertising and Marketing. The modern digital economy relies on data being available from third parties and on the programmatic exchange of data, which often constitute a "sale" under state law. Precise geolocation data is an integral component for consumer personalization and marketing that allows companies to reach consumers with relevant content and ads at the right time and in the right place.

For example, an owner of a newly open restaurant with limited marketing budget would like to advertise to individuals within two miles of its location. By working with an advertising company, that local business owner can target devices that have opted into the processing of geolocation data within two miles of the restaurant with a targeted ad. Without the ability to sell or transfer such data subject to consumer consent, businesses will have a more difficult time, and a higher cost, reaching consumers with relevant marketing and consumers will not be alerted to products and services they desire that are near to them.

Identity and fraud protection. Financial institutions, retailers, and others rely on anti-fraud services that include precise geolocation data provided by third parties. The sale of precise geolocation data allows anti-fraud and identity protection services to flag suspicious behavior and protect vulnerable communities. For example, companies can more easily detect credit card theft or fraud if they or their service providers have access to precise geolocation data showing that a consumer is not in the location where a purchase is being made. The ability to use and transfer precise geolocation data helps companies to detect and prevent fraudulent and illegal activity and reach out to consumers to confirm their purchases. Again, even if AB 1355 were to exempt uses of data for anti-fraud purposes, companies may collect and use it less, making it less available for this important anti-fraud and identity protection use. Meaning, the bill would still inhibit the use of precise geolocation data to protect consumers from fraud and identity theft in effect.

In some contexts, it not entirely clear what might be "necessary to provide goods or services requested by that individual". For example, hospitals put location anklets on newborns. An alarm sounds if the baby is taken out of the perinatal area, and there's a tracker so the hospital can find the baby if someone tries to kidnap it. The anklet is removed when the baby is discharged. Assuming that's not "necessary to provide goods or services requested by the individual," if a mother comes in on an emergency basis and prior consent cannot be obtained, what then? Also, hospitals often track their equipment. If they were to have a tracker on an infusion pump and a patient is hooked up to the

infusion pump, would this bill consider them to be tracking the patient? Is an opt-in needed?

Neither of these situations appear covered by the exemption for data collected from a patient by a health care provider or health care facility, or collected, processed, used, or stored exclusively for medical education or research, public health or epidemiological purposes, health care treatment, health insurance, payment, or operations, if the information is protected from disclosure under the federal Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1), or other applicable federal and state laws and regulations pertaining to health care privacy.

Definition of "individual" has broad implications for certain industries and for public entity employees as well. The broad definition of individual captures both consumers and employees, which especially raises concerns for certain industries involving commercial vehicles where GPS devices are needed to track equipment, but also from a state and federal government mandate for employee drivers to utilize an electronic logging device (e.g. the trucking industry).

And because "individual" is so broad that it captures both private and public employees, AB 1355 will also impact any entity, public or private, that maintains location data for its employees, via a tracking system for its vehicle fleet, phone, or other technology, if a private vendor is involved or the data is maintained in a cloud maintained by a private entity . Any location tracking will require employers to receive consent from an employee in order to track a vehicle for an employee's safety, because a job site is in a remote location, or for security, because their vehicles or materials inside are highly valuable.

Definition of "location information" does not exclude publicly available data including data that is collected from public records. There are First Amendment rights to data in such records, which is why the Legislature passed AB 874 (Irwin, Ch. 748, Stats. 2019) following the passage of the CCPA, to ensure that the rights of privacy did not unlawfully infringe upon First Amendment rights. Voters in fact expanded upon the exception passed by the Legislature in AB 874 in Proposition 24, so this would directly contravene voters' intent. Doing so by enacting a new statute on the same issues, as opposed to amending the existing statutes does not change that fact.

Preexisting data. What of all preexisting data? Does the bill apply prospectively only? Or does it apply to all data currently in existence?

Also writing in opposition, the California State Sheriffs Association writes:

> Though this bill excludes public agencies from the definition of "covered entity," the impacts of AB 1355 will limit the availability of data collected by covered entities that are ultimately shared with and used by law enforcement. License plate reader systems, GPS coordinates, cell-site location information, and facial recognition technology used by non-public entities gather data that are shared with law enforcement to identify suspects, solve crimes, and protect victims. AB 1355's requirements will have a chilling effect on the collection of these data, which limits their availability for law enforcement use.

Additionally, requiring a court order for disclosure to law enforcement of the vast amount of data covered by this bill goes far beyond any existing statute or case law.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Reports (sponsor)

Access Humboldt
California Federation of Labor Unions, Afl-cio
California Immigrant Policy Center
California Initiative for Technology & Democracy, a Project of California Common CAUSE
California Labor Federation, Afl-cio
California School Employees Association
Calpirg, California Public Interest Research Group
Consumer Action
Consumer Federation of America
Consumer Federation of California
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Oakland Privacy
Pflag Sacramento
Privacy Rights Clearinghouse
Secure Justice
Tech Oversight California
Techequity Action

Opposition

Association of California Life and Health Insurance Companies
Association of National Advertisers
Calbroadband
California Chamber of Commerce
California Credit Union League
California Financial Services Association
California League of Food Producers
California Police Chiefs Association
California Retailers Association
California State Sheriffs' Association
Computer and Communications Industry Association
Consumer Data Industry Association
CTIA
Insights Association
Network Advertising Initiative
Peace Officers Research Association of California (PORAC)
Security Industry Association
Software Information Industry Association
Techca
Technet

Oppose Unless Amended

National Insurance Crime Bureau

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200