Date of Hearing: April 1, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1337 (Ward) – As Introduced February 21, 2025

PROPOSED AMENDMENTS

SUBJECT: Information Practices Act of 1977

SYNOPSIS

The Information Practices Act (IPA) was passed nearly 50 years ago, five years after California voters enshrined the right to privacy in the state's constitution. Generally, the IPA places several relatively modest conditions and restrictions on the collection, maintenance, and disclosure of the personal information of Californians held by state agencies, including a prohibition on the disclosure of an individual's personal information without the individual's consent except in specified circumstances.

The IPA has two key shortcomings. First, the law has remained virtually unchanged for nearly five decades. Meanwhile, the scale, sensitivity, and scope of personally identifiable information collected and stored by government agencies has expanded dramatically. The law needs updating to address the realities of today's complex, data-driven digital environment. Second, the statute applies only to state entities and does not cover local governments, leaving a major loophole in the protection of Californians' personal and sensitive information.

This bill would address both issues. It would update the IPA in a number of ways, including by updating the definitions of personal and sensitive personal information contained in the California Consumer Privacy Act (CCPA) through an amendment proposed in Comment #9. The bill would also put local agencies on the same footing as their state counterparts by requiring local agencies to follow the requirements of the IPA when it comes to handling individuals' personal information.

This bill is substantially similar to AB 2677 (Gabriel) in 2022, which received zero "no" votes in the Legislature. The local government requirement was ultimately amended out in the Senate Appropriations Committee. Despite its overwhelming support by the Legislature, the Governor vetoed the measure, citing cost concerns.

The bill is co-sponsored by Oakland Privacy and the Electronic Frontier Foundation. It is supported by the ACLU California Action, the California Immigrant Policy Center, and the California Initiative for Technology and Democracy (CITED). The bill is opposed by a coalition of local government associations including the California State Association of Counties and the California League of Cities and the El Dorado Irrigation District.

THIS BILL:

1) Adds local offices to the definition of "agency."

2) Requires agencies to inform individuals of the specific purpose for which their personal information will be used.

3) Prohibits agencies from using personal information without prior written consent for any purpose other than the purpose for which the information was collected, except as required by federal law or authorized by state law.

4) Prohibits an agency from disclosing personal information in a manner that could be linked to the individual, except in certain circumstances, as defined.

5) Limits the exemptions to those that further the purpose for which the information was collected.

6) Prohibits the agencies from sharing personal information, without consent, in response to a warrant or sharing with a law enforcement agency or regulatory agency for an investigation.

7) Requires agencies to retain records related to personal information disclosures for three years.

8) States that a negligent violation of any of the bill's provisions by an officer or employee of any agency constitutes a cause for discipline, including termination of employment.

EXISTING LAW:

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

2) Establishes the Information Practices Act (IPA) of 1977, which generally enumerates the requirements applicable to state agencies that collect, maintain, and disclose personal information from California residents, including limitations on permissible disclosure, the rights of residents to know and access the information, and required accounting of disclosures of the information. (Civ. Code § 1798, et seq.)

3) States, in the IPA, 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 that each state agency maintain in its records only personal information that is relevant and necessary to accomplish the purpose of the agency. (Civ. Code § 1798.14.)

5) Requires that each agency collect personal information to the greatest extent practicable directly from the individual who is the subject of the information rather than from another source. (Civ. Code § 1798.15.)

6) Prohibits an individual's name and address from being distributed for commercial purposes, sold, or rented by an agency unless such action is specifically authorized by law. (Civ. Code § 1798.60.)

7) Defines "personal information," for purposes of the IPA, as any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, the individual's name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. (Civ. Code § 1798.3(a).)

8) Defines "agency", for the purposes of the IPA, to mean every state office, officer, department, division, bureau, board, commission, or other state agency, except for the California Legislature, agencies within the judicial branch, the State Compensation Insurance Fund, and local agencies, defined to include: counties; cities, whether general law or chartered; cities and counties; school districts; municipal corporations; districts; political subdivisions; or any board, commission, or agency thereof; other local public agencies, or entities that are legislative bodies of a local agency as specified. (Civ. Code § 1798.3(b); Gov. Code § 7920.510)

9) Requires each agency to keep an accurate accounting of the date, nature, and purpose of each disclosure of a record made pursuant to specified circumstances; and requires each agency to retain that accounting for at least three years after the disclosure, or until the record is destroyed, whichever is shorter. (Civ. Code §§ 1798.25 & 1798.27.)

10) Except as specified, endows each individual with the following rights: to inquire and be notified as to whether the agency maintains a record about them; to inspect all personal information in any record maintained by reference to an identifying particular of the individual; and to submit a request in writing to amend a record containing personal information pertaining to them maintained by an agency. (Civ. Code § 1798.30, et seq.)

11) Requires each state agency, when it provides by contract for the operation or maintenance of records containing personal information to accomplish an agency function, to cause, consistent with its authority, the requirements of the IPA to be applied to those records; and specifies that for purposes of enforcing penalties for violations of the IPA, any contractor and any employee of the contractor, shall be considered to be an employee of an agency. (Civ. Code § 1798.19.)

12) Defines "Personal information" under the California Consumer Privacy Act 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. Personal information includes such information as:

a) 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.

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

c) Characteristics of protected classifications.

d) Biometric information.

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

f) Geolocation data.

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

h) Professional or employment-related information.

i) Education information.

j) Inferences drawn from any of the information identified that reflects the consumer's preferences, characteristics, psychological behavior, attitudes, intelligence, abilities, and aptitudes.

k) Sensitive information. (Civ. Code § 1798.140(v).)

COMMENTS:

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

> I introduced AB 1337 to ensure that Californians' right to privacy—explicitly protected in the state constitution—is upheld in the digital age. When the IPA was enacted nearly five decades ago, it was a groundbreaking step toward regulating how government agencies manage personally identifiable information. However, the law has not kept pace with the evolution of technology or the scale of data collected by public agencies today. As new threats to personal privacy have emerged—from geolocation tracking to biometric data collection—the need to modernize the law has become urgent.
>
> My purpose in introducing this bill is to close critical gaps in the state's governmental privacy framework and bring it into alignment with current best practices in data protection. AB 1337 ensures that privacy protections apply consistently across all levels of government, not just state agencies. It updates the legal definitions of personal and sensitive information to reflect the realities of how data is generated, tracked, and stored in the modern world. The bill prohibits unauthorized secondary uses of personal data and holds agencies accountable when harm is caused by negligence. In doing so, it provides stronger protections for all Californians, particularly for vulnerable populations whose data is at heightened risk of misuse.

> AB 1337 directly resolves the problems identified by updating the IPA's outdated provisions, aligning it with modern privacy standards, and ensuring that individuals retain control over their personal data in interactions with all branches of government. By doing so, the bill strengthens public trust, enhances accountability, and reinforces California's national leadership in protecting individual privacy rights.

2) **Historical perspective.** To fully understand how completely people in California and throughout the country have ceded the right to live their lives in private, free from both government and private surveillance, privacy experts reflect on the concerns raised by federal and state lawmakers 50 years ago when debating the creation of the FBI's National Crime Information Center's computerized data collection system (NCIC). This system allowed local, state, and federal law enforcement agencies to share personal data related to suspected criminal activities. Congress held "days and days" of hearings over two years. Members warned of the "threat of the dictatorship of dossiers."[1]

During the debates, Senator Barry Goldwater of Arizona lamented, "Where will it end? . . . Will we permit all computerized systems to interlink nationwide so that every detail of our personal lives can be assembled instantly for use by a single bureaucrat or institution?"[2] Senator Charles H. Percy of Illinois in foreshadowing of what would come to pass in the 21st century warned:

> I hope that we never see the day when a bureaucrat in Washington or Chicago or Los Angeles can use his organization's computer facilities to assemble a complete dossier of all known information about an individual. But, I fear that is the trend. . . . Federal agencies have become omnivorous fact collectors—gathering, combining, using, and trading information about persons without regard for his or her rights of privacy. Simultaneously, numerous private institutions have also amassed huge files . . . of unprotected information on millions of Americans.[3]

During the same period when Congress was expressing concern about the erosion of individuals' privacy protections, the people of California used the initiative process to add "privacy" to the list of "inalienable rights" in the state constitution in 1972.[4] 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. . . ."[5]

As the co-sponsors so eloquently detail:

> In 1972, in the wake of revelations about the abuses of J. Edgar Hoover's FBI and the Cointelpro program, Californians, by a 62.9% yes vote, added the right to privacy to California's state constitution via Prop 11. ACA 51, introduced by assembly member Ken

---

[1] Citron, Danielle Keats, *A More Perfect Privacy*, 104 Boston University Law Review, 1073–1086 (2024).
[2] *Ibid.*
[3] *Ibid.*
[4] California Proposition 11 (1972), "Constitutional Right to Privacy Amendment."
[5] *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.

Cory added privacy to the list of the inalienable rights of the people of the state and replaced the word "men" with the word "people" in the state constitution.

Cory explained:

> *In the face of a cybernetics revolution and the increasingly pervasive amount of information being compiled, it would be highly desirable that our constitution state in clear terms that each person has a fundamental right to privacy… The constitutional amendment would create a positive, inalienable right to privacy and "put the State and private firms on notice that the people have this fundamental right and it can only be abridged when the public concern is an overriding concern.*

Cory battled opposition from private industry, the Department of Motor Vehicles and law enforcement, but was eventually able to corral support from 2/3 of both houses of the Legislature. Prop 11 went on the November 1972 ballot with an argument in support from State Senate Majority Leader George Moscone:

> *"The proliferation of government snooping and data collecting is threatening to destroy our traditional freedoms. Government agencies seem to be competing to compile the most extensive sets of dossiers of American citizens. Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American. At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian."*
>
> *"The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose. 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 or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives"* [Citations omitted.]

Arguably, the present is even more of a dictatorship of dossiers than the 92nd and 93rd Congresses and the voters of California envisioned, with not only governments, our own and others, being able to monitor individual's private lives, but virtually every private business or individual with enough resources and technological savvy having access to those dossiers as well. 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."[6]

Professor Citron continues to raise alarms about the on-going decimation of the right to privacy:

> In the United States, the quantity of personal data collected, used, shared, sold, and stored has grown to the point of international embarrassment. NCIC is one node in the criminal justice and intelligence "information sharing environment." Private- and public-sector databases reveal the most intimate details of people's lives, including their thoughts, searches, browsing habits, bodies, health, sexual orientation, gender, sexual activities, and close relationships. The quantity and quality of personal data being amassed has exceeded all warning; the distinction between public and private collection efforts has vanished; the privacy that people want, expect, and deserve has been, and continues to be, under assault.[7] [Citations omitted.]

Catherine Powell, adjunct senior fellow for women and foreign policy at the Council on Foreign Relations, pointed out in 2023 in a blog post for the Council:

> If you've engaged with any form of technology recently—whether through a smartphone, social media, a fitness tracker, even a seemingly innocuous game like Candy Crush—you have accumulated a substantial amount of intimate privacy data. Intimate data ranges from your location, to when you fall asleep, to even more closely guarded information like your menstrual cycle or sexual partners. And every day, this data is scraped, bought, and sold by data brokers to third parties. Beyond violating our privacy, this repurposing of our personal data undermines our security.[8]

3) **The Information Practices Act of 1977.** The Information Practices Act of 1977 (IPA; Civ. Code § 1798, et seq.), modeled after the Federal Privacy Act of 1974, is the primary privacy statute governing the collection, maintenance, and disclosure of personal information by California state agencies. As outlined in the **EXISTING LAW** section previously, along with the substantive provisions of the IPA, the Legislature codified findings and declarations upon its passage justifying the need for the consistent limits on the maintenance and dissemination of personal information by government agencies.

Generally, the IPA places several conditions and restrictions on the collection, maintenance, and disclosure of the personal information of Californians held by state agencies, including a prohibition on the disclosure of an individual's personal information without the individual's consent except in specified circumstances. In addition, the IPA requires that along with any form requesting personal information from an individual, an agency must provide notice of information pertaining to the individual's rights with respect to their personal information, the purposes for which the personal information will be used, and any foreseeable disclosures of that personal information.

---

[6] Clarke, Laurie. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) *available at* https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.
[7] Citron, 2024.
[8] Powell, Catherine. "Data is the New Gold, But May Threaten Democracy and Dignity," *Council on Foreign Relations* (Jan. 5, 2023) https://www.cfr.org/blog/data-new-gold-may-threaten-democracy-and-dignity-0.

The IPA also provides individuals with certain rights to be informed of what personal information an agency holds relating to that individual; to access and inspect that personal information; and to request corrections to that personal information, subject to specified exceptions. Finally, when state agencies contract with private entities for services, the contractors are typically governed by the IPA, with few additional privacy protections generally stipulated in the contracts themselves.

However, as the state has moved to allow individuals to opt-out from allowing large, private companies to share and sell their personal information through the passage of the CCPA and CPRA, it has not yet updated the laws that are designed to protect Californians' privacy from state and local government agencies. Despite the creation of the internet and the advent of technology that allows for the massive collection, manipulation, and analysis of millions of data points on nearly 40 million California residents, the state's IPA has remained largely untouched since it was first passed in 1977.

5) **Challenges with California's privacy laws.** Of particular concern for this bill is the fact that, though far from perfect, the privacy protections contained in the IPA do not apply to local agencies. As a result, local governments are free to broadly share the personal information they have collected on people residing within or passing through their jurisdictions without seeking the individuals' consent, with the general exception of information subject to medical, child welfare services, and education-related privacy laws.

The bill's opposition argues that "the bill in its current form does not appear to contemplate the vast technical effort that would be required for thousands of agencies to come into compliance. The effort would certainly require technological changes, including in many cases new equipment, coding for proprietary systems, and software purchases. It would also require personnel changes, including hiring new specialized staff and widespread training, which is not only required by the IPA but also important to local agency employees given the statutorily required discipline in the Act, up to and including termination, for errors made due to negligence."

However, in the past local governments have argued that they have systems in place to protect individual's personal information from unnecessary sharing and disclosure. If that is indeed the case, arguably the overall purpose of the IPA, acquiring consent before sharing an individual's personal information, except in certain instances, should not be particularly onerous. To the extent that there are specific requirements in the bill that should only apply to state agencies, the opposition may wish to work with the author to highlight those provisions and provide alternate language.

As the country becomes more fractured, the risks grow for people seeking abortion care and gender affirming care; Californians who emigrated from other countries; and people exercising their first amendment rights by peacefully protesting the actions of their government. If the State intends to remain a sanctuary state for vulnerable populations, it is imperative that all of California's privacy protection laws be reviewed in the context of the current environment and updated as necessary to allow all Californians to achieve their constitutional right to have a private life.

6) **What this bill would do.** This bill would strengthen the IPA in several ways. Specifically, the bill:

1. Requires local government agencies to comply with the privacy protections contained in the IPA.

2. Removes terms that weaken the protections contained in the IPA. For example, instead of allowing information to be disclosed if it "is related to" the purpose for which it was gathered, disclosures, under this bill would only be allowed if it "furthers" the purpose.

   Similarly, instead of prohibiting the disclosure of information in a manner that "would" link the information to the individual, this bill would prohibit disclosure of information if it "could" link it to the individual. While this particular change may appear minor, the current state of technology and artificial intelligence allows information gathered from various data sources to be combined and analyzed in order to re-identify an individual after their personal information is de-identified.

3. Adds data minimization language that restricts agencies from using records containing personal information for any purpose other than that for which the information was collected, unless it is required by federal law or authorized by state law.

7) **California is a sanctuary state.** California leads the nation with pro-immigrant policies that have sparked change nationwide, including expanding access to higher education, expanding access to health care and public benefits, advancing protections for immigrant workers, supporting immigrant students through partnerships with school districts, and improving opportunities for economic mobility and inclusion through access to driver's licenses and pro bono immigration services.

Senate Bill 54, the California Values Act, which took effect on January 1, 2018, is considered one of the strongest state protections for undocumented immigrants. The law builds on previous "sanctuary" policies with regard to assisting federal immigration efforts—and extends them—by establishing statewide non-cooperative policies between state law enforcement officials and federal immigration authorities.

California prohibits state or local law enforcement agencies from the following actions:

1. Detaining an individual on a hold request from the federal government unless there is a felony or a warrant.

2. Transferring undocumented immigrants into federal custody unless they've been convicted in the last 15 years of a crime that is one of the listed offenses under California's TRUST Act of 2013 or the individual is a registered sex offender.

3. Asking about a person's immigration status or sharing any information with federal immigration authorities that is not available to the general public.

In addition to protecting Californians who emigrated from other countries, California is a reproductive freedom state. In 1969, the California Supreme Court held that the state constitution's implied right to privacy extends to an individual's decision about whether or not to

have an abortion.[9] This was the first time an individual's right to abortion was upheld in a court and came before the *Roe* decision. In 1972, the California voters passed a constitutional amendment that explicitly provided for the right to privacy in the state constitution.[10] The Reproductive Privacy Act's findings and declarations state that every individual possesses a fundamental right of privacy with respect to personal reproductive decisions, which entails the right to make and effectuate decisions about all matters relating to pregnancy; therefore, the Legislature has declared that it is the public policy of the State of California that every individual has the fundamental right to choose or refuse birth control, and every individual who may become pregnant has the fundamental right to choose to bear a child or to choose to obtain an abortion.[11] In 2019, Governor Newsom issued a proclamation reaffirming California's commitment to making reproductive freedom a fundamental right in response to the numerous attacks on reproductive rights across the nation.[12]

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.[13] In response to the *Dobbs*[14] 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 1and 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.[15]

This bill is in keeping with, and arguably critical to maintaining, the Legislature's longstanding goal of ensuring that California is a place of sanctuary and refuge for all that need it.

8) **Prior legislation.** This bill is substantially similar to AB 2677 (Gabriel) in 2022. That bill received no "no" votes in the Assembly and the Senate; passed this Committee on a 10 – 0 – 1 vote and passed off of the floor on a 73 – 0 – 5 vote. The local government requirement was ultimately amended out in the Senate Appropriations Committee. Despite its overwhelming support by the Legislature, the Governor vetoed the measure, stating:

> I commend the author for his commitment to data privacy and am supportive of expanding security protocols to further protect personal information collected by state agencies and businesses. However, I am concerned this bill is overly prescriptive and could conflict with the State's goal to provide person-centered, data driven, and integrated services. Additionally, this bill would cost tens of millions of dollars to implement across multiple state agencies that were not accounted for in the budget.

---

[9] *People v. Belous* (1969) 71 Cal. 2d 954.
[10] Prop. 11, Nov. 7, 1972 gen. elec.
[11] Health & Saf. Code § 123462.
[12] California Proclamation on Reproductive Freedom (May 31, 2019) https://www.gov.ca.gov/wp-content/uploads/2019/05/Proclamation-on-Reproductive-Freedom.pdf.
[13] (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.
[14] *Dobbs v. Jackson Women's Health Organization* (2022) 945 F. 3d 265,
[15](Nov. 8, 2022 gen. elec.)

> With our state facing lower-than-expected revenues over the first few months of this fiscal year, it is important to remain disciplined when it comes to spending, particularly spending that is ongoing. We must prioritize existing obligations and priorities, including education, health care, public safety and safety-net programs.

While there are clearly costs associated with updating and expanding the IPA, the current national climate, and the voracious appetite of developers of artificial intelligence for more and more personal data, arguably call for increasing the protection of personal information of Californians by adding in local agencies and updating the definition of "personal information."

The Governor also expressed concern related to the data sharing that is necessary to accomplish the State's goal of increasing integrated services for people. The author and sponsors may wish to consider whether or not restrictions related to data sharing between the state and local agencies and among agencies could be eased if all of the agencies are bound by the privacy protections contained in the IPA.

In addition, AB 2388 (Joe Patterson; 2024) would have updated the definition of personal information to bring it more in alignment with other definitions of personal information, including the CCPA. The following Committee amendments are in alignment with that goal. AB 2388 received no "no" votes in the Assembly or in the Senate Judiciary Committee, but was ultimately held on suspense in the Senate Appropriations Committee.

9) **Amendments.** The author has agreed to the following amendments:

> In order to update the definition of personal information to more closely track with personal information and sensitive personal information in the CCPA, Civ Code § 1798.3(a) would be amended as follows:
>
> (a) *(1)* The term "personal information" means ~~any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, the individual's name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.~~ ***any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to:***
>
> ***(a) 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.***
>
> ***(b) Vehicle registration information (including license plate numbers).***
>
> ***(c) The contents of an individual's mail, email, and text messages unless the agency is the intended recipient of the communication.***
>
> ***(d) Characteristics of protected classifications.***
>
> ***(e) Racial or ethnic origin, citizenship or immigration status, religious beliefs, political positions or affiliations, or union membership.***

(f) Biometric information.

(g) Genetic data.

(h) Precise Geolocation data.

(i) "Precise geolocation data" means any data that is derived from a device and that is used or intended to be used to locate an individual within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet.

(i) Audio, electronic, visual, thermal, olfactory, or similar information.

(j) Insurance policy numbers.

(k) Neural data.

(i) "Neural data" means information that is generated by measuring the activity of an individual's central or peripheral nervous system, and that is not inferred from nonneural information.

(l) Personal information collected and analyzed concerning an individual's health.

(m) Personal information collected and analyzed concerning an individual's gender, sex life or sexual orientation.

(2) "Personal information" can exist in various formats, including, but not limited to, all of the following:

(a) Physical formats, including paper documents, printed images, vinyl records, or video tapes.

(b) Digital formats, including text, image, audio, or video files.

(c) Abstract digital formats, including compressed or encrypted files, metadata, or artificial intelligence systems that are capable of outputting personal information.

The other two amendments are technical, clean up amendments.

1798.3 (b) The term "agency" means every state and local office, officer, department, division, bureau, board, commission, or other ~~**state**~~ agency, except that the term agency shall not include:

(1) The California Legislature.

(2) Any agency established under Article VI of the California Constitution.

(3) The State Compensation Insurance Fund, except as to any records that contain personal information about the employees of the State Compensation Insurance Fund.

1798.24 (q) To a committee of the Legislature or to a Member of the Legislature, or the Member~~'s~~ of the Legislature's staff if authorized in writing by the Member, ***~~of the Legislature~~*** if the Member of the Legislature has permission to obtain the information from the individual to whom it pertains or if the Member of the Legislature provides reasonable assurance that the Member of the Legislature is acting on behalf of the individual.

ARGUMENTS IN SUPPORT: Oakland Privacy and the Electronic Frontier Foundation, co-sponsors of the bill, write in support:

> Many of the privacy bills on the committee's agenda focus, rightfully, on keeping private companies in line. Assembly Bill 1337 turns the privacy focus inward towards the activities of California state and local government to ensure that we have our own house in order as we seek to continue regulating the private sector.
>
> [. . .]
>
> [T]he IPA is a critical component of California's heritage and came into being by way of a dramatic statewide consensus. We have seen through the CCPA/CPRA process some 40 years later that California retains that commitment to privacy rights in both the public and private sectors.
>
> For a law from 1977, especially one focusing on such a rapidly changing landscape as information and data, the IPA's original language has remained remarkably intact. The lack of wholesale changes for 48 years demonstrates the fundamental soundness of the law. We want to underline that: California state government has largely functioned under the umbrella of this law for almost half a century. It is one of the foundational building blocks of our state and it has passed the test of time. But most five decade old laws could benefit from a little updating and that time has come. Not only because so much time has passed, but because we are in a historical moment of great import when privacy from governmental intrusions is being deeply challenged by a federal government, that whatever your political inclinations, has totally upended the civil society consensus on data privacy in two months.
>
> We know the committee is aware of the funding freezes, the incursion into the treasury database, the vulnerability of social security, the revocations of legal status, the detentions of American citizens by ICE, the rendition of undocumented immigrants to foreign prisons, and the targeting of transgender Americans and women seeking to terminate their pregnancies. And we are only 64 days into this brave new world.
>
> All of the information the federal government has been collecting for decades about all of us is now in service of an agenda for weaponization against the people on the wrong side of the culture war. If California is to protect the people who live here, as the Governor and AG Bonta have stated it is their intention to do, then now is the time to update the state's data handling regulations, including what is shared with the feds, and most importantly, to make sure that all data collected by California governmental agencies has the same baseline of privacy protections, no matter which branch of government collected it. [Citations omitted.]

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of local government associations argues:

> [T]he Act as it exists was not designed with local agencies in mind and is peppered with requirements that do not make sense in that context. To give just one example, as AB 1337 would amend the law, agencies under the IPA would be required to adopt policies consistent with the State Administrative Manual and the State Information Management Manual, highly detailed documents that are prepared for state agencies and departments by a state agency. State agencies with questions about those materials are assigned account leads and oversight managers by the California Department of Technology (CDT). Would CDT likewise assign oversight managers to local agencies to answer questions?
>
> Local agencies already have in place policies and procedures to protect personal information. These efforts would need to be scrapped to the extent they do not take the same approach as those outlined in the Act, regardless of their effectiveness or the cost of doing so.
>
> To add to these challenges, the bill allows local agencies little time to prepare for compliance. Because the bill would take effect January 1, 2026, and because local agencies may not know if the bill will become law until the Governor's October 12, 2025, deadline to sign or veto bills, local agencies could have fewer than three months to prepare for compliance with the Act.
>
> Finally, Section 17 of the bill asserts that no reimbursement is required by the act, suggesting that the only state-mandated activity directed by the bill is due to the adjustments to a crime or infraction. We believe the language is inappropriate and should be amended to clearly declare that the bill would establish a new mandate reimbursable under state law, as the bill clearly mandates a new activity by local agencies: compliance with the IPA, which requires significant changes to software, internal practices, and duties of local agency workforces.

REGISTERED SUPPORT / OPPOSITION:

Support

Electronic Frontier Foundation (co-sponsor)
Oakland Privacy (co-sponsor)
ACLU California Action
California Immigrant Policy Center
California Initiative for Technology & Democracy, a Project of California Common CAUSE

Opposition

Association of California Healthcare Districts (ACHD)
California State Association of Counties (CSAC)
El Dorado Irrigation District
League of California Cities
Rural County Representatives of California (RCRC)
Urban Counties of California (UCC)

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