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

AB 2677 (Gabriel)
Version: June 20, 2022
Hearing Date: June 28, 2022
Fiscal: Yes
Urgency: No
CK

## SUBJECT

Information Practices Act of 1977

## DIGEST

This bill amends the Information Practices Act by updating definitions, bolstering existing protections, applying data minimization principles, limiting disclosure, and increasing accountability.

## EXECUTIVE SUMMARY

The Information Practices Act of 1977 is the statutory scheme that governs the collection, use, retention, and disclosure of personal information by state agencies in California. Passed over 40 years ago, it has not been meaningfully updated since.

This bill makes a number of changes to the Information Practices Act, including updating the definition of personal information to include information that is reasonably capable of identifying an individual, prohibiting an agency from using records containing personal information for any purposes other than those for which the PI was collected, except as specified, and adjusting penalties for violations of the law to include discipline for negligent violations and to eliminate injury-in-fact requirements for intentional disclosures of sensitive information.

These changes bring a long overdue modernization of this important but woefully antiquated privacy protection statute.

The bill is author sponsored. It is supported by various groups, including ACLU California Action and the League of Women Voters of California. There is no known opposition.

## PROPOSED CHANGES TO THE LAW

Existing law:

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

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

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

3) Defines "personal information" (PI) 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. It includes statements made by, or attributed to, the individual. (Civ. Code § 1798.3(a).)

4) Defines "agency" to include every state office, officer, department, division, bureau, board, commission, or other state agency. "Agency" explicitly excludes:
    a) the California Legislature;
    b) any agency established under Article VI of the California Constitution;
    c) the State Compensation Insurance Fund, except as to any records that contain personal information about the employees of the State Compensation Insurance Fund; or
    d) a local agency, as defined. (Civ. Code § 1798.3(b).)

5) Defines "record" to mean any file or grouping of information about an individual that is maintained by an agency by reference to an identifying particular such as the individual's name, photograph, finger or voice print, or a number or symbol assigned to the individual. (Civ. Code § 1798.3(g).)

6) Provides that each agency shall maintain in its records only PI which is relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government; and requires each agency to maintain all records, to the maximum extent possible, with accuracy, relevance, timeliness, and completeness. (Civ. Code §§ 1798.14, 1798.18.)

7) Requires an agency that collects PI to maintain the source of that information, except as specified; and specifies that each agency shall collect PI to the greatest extent practicable directly from the individual who is the subject of the PI. (Civ. Code §§ 1798.15, 1798.16.)

8) Requires each agency to provide with any form used to collect PI from individuals a notice containing specified information including: the name and specified contact information of the agency requesting the information; the statutory, regulatory, or executive authority that authorizes the maintenance of the information; whether submission of the information is mandatory or voluntary; the consequences, if any, of not providing all or any part of the requested information; the principal purpose or purposes for which the information is to be used; any known or foreseeable disclosures that may be made of the information; and the individual's right of access to records containing PI which are maintained by the agency. (Civ. Code § 1798.17.)

9) Requires each agency to establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing PI and to instruct each such person with respect to those rules; and further requires each agency to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of the IPA, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in an injury. (Civ. Code § 1798.20.)

10) Prohibits an agency from disclosing any PI in a manner that would link the information disclosed to the individual to whom it pertains unless the information is disclosed as specified, including:
    a) with the prior written voluntary consent of the individual to whom the PI pertains within the preceding 30 days;
    b) to a person or another agency if the transfer is necessary for the transferee agency to perform its constitutional or statutory duties, and the use is compatible with a purpose for which the information was collected;
    c) to a governmental entity if required by state or federal law;
    d) pursuant to the California Public Records Act (Gov. Code § 6250, et seq.);

e) pursuant to a subpoena, court order, search warrant, or other compulsory legal process with notification to the individual, unless notification is prohibited by law; and
f) for statistical and research purposes, as specified. (Civ. Code § 1798.24.)

11) 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.)

12) Grants individuals with specified rights in connection with their PI, including the right to inquire and be notified as to whether the agency maintains a record about them; to inspect all PI in any record maintained; and to submit a request in writing to amend a record containing PI pertaining to them maintained by an agency. (Civ. Code § 1798.30, et seq.)

13) Provides that an agency that fails to comply with any provisions of the IPA may be enjoined by any court of competent jurisdiction, and, as specified, the agency may be liable to the individual in an amount equal to the sum of actual damages sustained by the individual, including damages for mental suffering, and the costs of the action together with reasonable attorney's fees as determined by the court. (Civ. Code §§ 1798.46-1798.48.)

14) Provides that the intentional violation of any provision of the IPA, or any rules or regulations adopted thereunder, by an officer or employee of an agency shall constitute a cause for discipline, including termination of employment; and further specifies that the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the IPA is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains. (Civ. Code §§ 1798.55, 1798.57.)

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

16) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the CCPA and creates the California Privacy Protection Agency (PPA), which is charged with implementing these privacy laws, promulgating regulations, and

carrying out enforcement actions. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)

17) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers of specified information. (Civ. Code § 1798.100(a).)

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

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

This bill:

1) Updates the definition of "personal information" to include any information that is maintained by an agency that is reasonably capable of identifying or describing an individual, including, but not limited to, the individual's name, social security number, physical description, genetic information, address, telephone number, IP address, online browsing history, location information, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

2) Removes the term "system of records" and simplifies the definition of "record" to include any file or grouping of personal information that is maintained by an agency.

3) Requires the notice accompanying data collection to include all purposes within the agency for which the collected PI is to be used.

4) Requires the rules of conduct to be consistent with the State Administrative Manual and the State Information Management Manual.

5) Prohibits an agency from using records containing PI for any purpose or purposes other than those for which that PI was collected, except as required by federal law, or as authorized or required by state law.

6) Tightens the bases for disclosure of PI that could link it to an individual. This includes removing disclosure to a law enforcement or regulatory agency when required for an investigation of unlawful activity or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law.

7) Requires the notification DMV is required to make to be provided to the person to whom the PI relates.

8) Requires retention of accounting for at least three years.

9) Extends the basis for discipline to negligent violations of the IPA.

10) Removes the condition that in order to be held liable for intentional disclosure of specified medical records there must be resultant economic harm or personal injury.

## COMMENTS

1. The IPA and Californians' privacy

Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Privacy is therefore not just a policy goal, it is a constitutional right of every Californian. However, it has been under increasing assault.

The phrase "and privacy" was added to the California Constitution as a result of Proposition 11 in 1972; it was known as the "Privacy Initiative." The arguments in favor of the amendment were written by Assemblymember Kenneth Cory and Senator George Moscone. The ballot pamphlet stated in relevant part:

> 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 . . . 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. . . . The proliferation of government and business records over which we have no control limits our ability to control our personal lives. . . . Even more dangerous is the loss of control over the accuracy of government and business records on individuals. . . . Even if the existence of this information is known, few government agencies or private businesses permit individuals to review their files and correct errors. . . . Each time we apply for a

> credit card or a life insurance policy, file a tax return, interview for a job[,] or get a drivers' license, a dossier is opened and an informational profile is sketched.[1]

In 1977, the Legislature reaffirmed through the IPA that the right of privacy is a "personal and fundamental right" and that "all individuals have a right of privacy in information pertaining to them."[2] The Legislature further stated the following findings:

- "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."
- "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."
- "In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."

Modeled after the Federal Privacy Act of 1974, the IPA governs the collection, maintenance, and disclosure of personal information by state agencies, specifically excluding local agencies. The IPA places guidelines and restrictions on the collection, maintenance, and disclosure of Californians' PI, including a prohibition on the disclosure of an individual's PI that can be used to identify them without the individual's consent except under one of a list of specified circumstances. State agencies are required to provide notice to individuals of their rights with respect to their PI, the purposes for which the PI will be used, and any foreseeable disclosures of that PI.

The IPA also provides individuals with certain rights to be informed of what PI an agency holds relating to that individual, to access and inspect that PI, and to request corrections to that PI, subject to specified exceptions. In addition, when state agencies contract with private entities for services, the contractors are typically governed by the IPA.

2. Updating the existing framework for the digital age

In response to growing concerns about the privacy and safety of consumers' data, proponents of the CCPA, a statewide ballot initiative, began collecting signatures in order to qualify it for the November 2018 election. The goal was to empower consumers to find out what information businesses were collecting on them and give them the choice to tell businesses to stop selling their personal information. In response to the pending initiative, which was subsequently withdrawn, AB 375 (Chau, Ch. 55,

---

[1] *Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 17, quoting the official ballot pamphlet for the Privacy Initiative.
[2] Civ. Code § 1798.1.

Stats. 2018) was introduced, quickly shepherded through the legislative process, and signed into law. The outcome was the CCPA.

The CCPA, later amended by the CPRA, grants a set of rights to consumers with regard to their personal information, including enhanced notice and disclosure rights regarding information collection and use practices, access to the information collected, the right to delete certain information, the right to restrict the sale of information, and protection from discrimination for exercising these rights.

The CCPA defines "personal information" as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including biometric information, geolocation data, and "sensitive personal information."

However, the modernized protections of the CCPA only apply to businesses. The IPA on the other hand has not been updated in decades, leaving its framework vulnerable. The Legislature at the time could not conceive of the digital information revolution that was to come. This bill seeks to bring the IPA into this new era and bolster the protections for Californians' PI that is collected, used, and retained by state agencies.

3. A new and improved IPA

According to the author:

> Despite epochal advances in information technology, the Information Practices Act (IPA), which governs the collection, use, and disclosure of Californian's personal information by state agencies, has not been meaningfully updated since its passage in 1977. As the technology employed by the state to better serve the people has become increasingly sophisticated, the definitions and protections provided by the IPA have fallen out of step with the types of information with which we entrust our government. An update to the IPA to better reflect our changing relationship with information in the 21st Century is long overdue.
>
> In 1977, the passage of the IPA was a landmark moment in this State's commitment to the right to privacy guaranteed by the California Constitution. AB 2677 would renew California's leadership in recognizing the immense importance of privacy rights to the liberty of its people.

This bill makes a number of changes to the IPA to ensure its scope and protections are meaningful, especially in light of increased data insecurity issues at various state agencies.

First, the bill refines the definition of "personal information," recognizing the enhanced ability to reidentify what previously was anonymous data. The current definition is "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. It includes statements made by, or attributed to, the individual." This antiquated definition leaves a variety of forms of PI out and can be narrowly read to only apply to information that is maintained in a form that it can be actively associated with a specific individual.

Conversely, the definition of PI in the CCPA appreciates that in combination with other sources of data an otherwise non-identifying data set can be connected to a specific person. This bill borrows from that definition to update the definition currently in the IPA. It defines PI as any information that is maintained by an agency that is reasonably capable of identifying or describing an individual, including, but not limited to, the individual's name, social security number, physical description, genetic information, address, telephone number, IP address, online browsing history, location information, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

The bill also incorporates critical data minimization principles into the IPA. It prohibits agencies from using records containing PI for any purpose or purposes other than the purpose or purposes for which that personal information was collected, except as required by federal law, or as authorized or required by state law. To ensure individuals are properly informed about what is being done with their PI, the bill also requires notification, on the form used to collect PI, of all purposes for which the information is to be used, rather than solely the *principal* purpose as now required.

The bill also tightens up a number of the conditions under which an agency is authorized to disclose PI in a manner that could link the information disclosed to the individual to whom it pertains. For instance, disclosure to a person or to another agency is authorized if the transfer is necessary for the transferee agency to perform its constitutional or statutory duties and the use *furthers* the purpose for which the PI was collected. Currently it must only be "compatible with" that purpose. However, the second sentence of that provision also includes reference to compatibility. To ensure consistency, the author has agreed to an amendment that fixes that inconsistency.

In addition, the bill removes authorized disclosure to a law enforcement or regulatory agency when required for an investigation of unlawful activity or for licensing, certification, or regulatory purposes, unless the disclosure is otherwise prohibited by law. However, the provision discussed in the preceding paragraph still allows for sharing when necessary to further the duties of the state agency.

The bill also increases the accountability of state agencies and their employees. Currently, only intentional violations of the IPA by an officer or employee of any agency constitute a cause for discipline. The bill extends this to negligent violations to ensure due care is afforded to the collection and handling of this sensitive PI.

In addition, current law provides the unlawful and intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the IPA is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains. Therefore, there is a requirement to establish certain damages before a person who intentionally disclosed sensitive information in violation of the law faces these consequences. This bill removes the requirement that the disclosure must result in economic loss or personal injury to the individual to whom the PI pertains.

4. Stakeholder positions

Writing in support, a coalition of privacy and civil liberties groups, including ACLU California Action, Privacy Rights Clearinghouse, and the Electronic Frontier Foundation explain their support and their desire that it go further to include local agencies:

> AB 2677 makes some common-sense changes to the IPA that reflect more recent thinking around the best practices for data management. These changes are in step with recent developments in privacy law. For one, it adds a data minimization requirement that guards against the overcollection of data. This ensures that all state entities will carefully think through what information they need to achieve their policy goals without erring into overcollection that can undermine trust in those initiatives.
>
> The bill updates the definition of personal information to include types of data that are either now commonly collected or are headed that way, including: genetic information, IP addresses, online browsing history, and location information. These types of data each have the potential to reveal intimate information about a person's habits, their racial identity, their political identity, their gender identity, and myriad other sensitive data inferences that should be protected under this law.
>
> AB 2677 also recognizes the latest thinking about best practices for addressing privacy harms. It removes the requirement that a person suffer "economic loss or personal injury" in order for an intentional disclosure of "medical, psychiatric, or psychological information" to have consequences for the person intentionally sharing this sensitive information. This change rightly acknowledges that harms are not simply monetary or bodily, but

> that improper disclosure itself can meaningfully and negatively affect a person's life.
>
> Unfortunately, AB 2677 no longer applies the IPA to local entities, despite laudable intent language calling for a comprehensive privacy law to govern personal information held by local entities that is congruent with the privacy law that governs personal information held by state entities. Because of amendments removing the application of the IPA to local entities, state entities will continue to be governed by one set of rules, the IPA, while the local entities they often interact with will instead be subject to a patchwork of policies that may differ from the requirements of the IPA. This difference will sow confusion about how entities can work together while respecting their own regulations around data sharing and collection and continues to leave personal information held by local governments at risk while the identical information held by state entities is protected under the IPA.

The League of Women Voters writes in support:

> AB 2677 is an update to the nature of personal information protected by the Information Practices Act of 1977 (IPA). It also strengthens the rules of conduct of individuals involved in managing these records. These are timely changes, introduced when records including individual information proliferate and privacy is at risk. The prior version of the bill would have applied these provisions to local governmental entities, and we encourage you to pursue those expanded protections next year.

**SUPPORT**

ACLU California Action
Electronic Frontier Foundation
The League of Women Voters
Privacy Rights Clearinghouse

**OPPOSITION**

None known

**RELATED LEGISLATION**

Pending Legislation:

AB 2135 (Irwin, 2022) requires state agencies that do not fall under the direct authority of the Governor to adopt and implement certain information security and privacy

policies, standards, and procedures meeting specified federally-established criteria, and requires those agencies to perform a comprehensive independent security assessment every two years for which they may contract with the Military Department or a qualified responsible vendor. This bill is currently in the Senate Appropriations Committee.

AB 2190 (Irwin, 2022) requires that the chief of the Office of Information Security submit an annual statewide information security status report including specified information to the Assembly Committee on Privacy and Consumer Protection beginning no later than January 2023. This bill is currently in the Senate Appropriations Committee.

AB 1711 (Seyarto, 2022) requires agencies to report data breaches on their website when a person or business operating a system on behalf of an agency is required to disclose a breach of that system. This bill is currently in the Senate Appropriations Committee.

Prior Legislation:

AB 825 (Levine, Ch. 527, Stats. 2021) added "genetic information" to the definition of personal information for purposes of the laws requiring certain businesses to implement and maintain reasonable security procedures and practices to protect personal information they own, license, or maintain. It required businesses and agencies that maintain personal information to disclose a breach of genetic information.

AB 660 (Levine, 2020) would have prohibited the use of any data collected, received, or prepared for purposes of contact tracing from being used, maintained, or disclosed for any purpose other than facilitating contact tracing efforts, and would have required any such data to be deleted within 60 days, except as specified. This bill died in the Senate Appropriations Committee.

AB 3223 (Gallagher, 2020) would have prohibited an agency from selling, renting, or exchanging for commercial purposes the PI an agency holds without the consent of the person to whom that information applies. It would have held an agency liable for all damages resulting from a negligent or intentional violation of the IPA. This bill died at the Assembly Desk.

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

AB 928 (Olsen, Ch. 851, Stats. 2014) required each state department and state agency to conspicuously post its privacy policy, including specified information, on its website.

**PRIOR VOTES:**

Assembly Floor (Ayes 73, Noes 0)
Assembly Appropriations Committee (Ayes 12, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 10, Noes 0)

**********