Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 2677 (Gabriel) – As Introduced February 18, 2022

SUBJECT: Information Practices Act of 1977

SUMMARY: This bill would make several changes to the Information Practices Act of 1977 (IPA), including expanding the definition of personal information (PI) to include information that is reasonably capable of identifying an individual, prohibiting an agency from using records containing PI for any purposes other than those for which the PI was collected, except as specified, adjusting penalties for violations of the law to include discipline for negligent violations by agency employees and to eliminate injury-in-fact requirements for intentional disclosures of sensitive information, and applying the IPA to local agencies. Specifically, **this bill would**:

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

2) Remove the requirement that a wrongful disclosure must result in economic loss or personal injury to the individual to whom the information pertains in order for the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the IPA to be punishable as a misdemeanor.

3) Provide that a negligent violation of any provision of the IPA or of any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment.

4) Remove the exemption permitting disclosure of PI without consent to a law enforcement or regulatory agency when required for an investigation of unlawful activity or for licensing, certification, or regulatory purposes; and make conforming changes.

5) Require that each agency retain the accounting of disclosures made pursuant to the IPA for at least three years after the disclosure for which the accounting is made, rather than for at least three years or *until the record is destroyed, whichever is shorter*.

6) Amend the definition of "personal information" as it applies to the IPA to mean 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.

7) Amend the definition of "agency" as it applies to the IPA to include local offices, officers, departments, divisions, bureaus, boards, commissions, or other local agencies; and make conforming changes.

8) Amend the definition of "record" as it applies to the IPA to mean any file grouping of PI that is maintained by an agency, removing the requirement that the PI be maintained by reference to an identifying particular of the individual in order to be considered a record.

9) Require that the rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing PI established by each agency be consistent with applicable provisions of the State Administrative Manual (SAM) and the Statewide Information Management Manual (SIMM).

10) Require that each agency provide on or with any form used to collect PI from individuals a notice including the purpose or purposes within the agency for which the information is to be used, rather than only the *principal* purpose or purposes.

11) Specify that an agency shall not disclose any personal information in a manner that *could*, rather than *would*, link the information disclosed to the individual to whom it pertains, except as specified.

12) Specify that, to permit a disclosure of PI to officers, employees, attorneys, agents, or volunteers of the agency that has custody of the information if the disclosure is relevant and necessary in the ordinary course of the performance of their official duties, the disclosure must *further*, rather than be *related to*, the purpose for which the information was acquired; and specify that, to permit a disclosure of PI to a person, or to another agency if the transfer is necessary for the transferee agency to perform its constitutional or statutory duties, the use must *further*, rather than be *compatible with*, the purpose for which the information was collected.

13) Require that, to permit a disclosure to a person who has provided the agency with advance, adequate written assurance that the information will be used solely for statistical research or reporting purposes, the information must be disclosed in a form that *cannot*, rather than *will not*, identify any individual; and further require that the written assurance includes a statement that the person will not attempt to reidentify the information.

14) Specify that procedures established by the Department of Motor Vehicles regarding the sale of information concerning the registration of any vehicle or from the files of drivers' licenses shall provide for notification to the person to whom the information relates, rather than the person to whom the information *primarily* relates, as to what information was provided and to whom it was provided.

15) Strike from the IPA the terms "system of records" and "governmental entity," and replace uses of the term "governmental entity" throughout the IPA with the term "branch of the federal government".

16) Replace all references within the IPA to the Department of Business Oversight with references to the Department of Financial Protection and Innovation.

17) Make several technical and conforming changes to the IPA.

EXISTING LAW:

1) Provides, under 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 IPA, which generally enumerates the requirements applicable to state agencies that collect, maintain, and disclose PI from California residents, including limitations on permissible disclosure, the rights of residents to know and access that PI, and required accounting of disclosures of PI. (Civ. Code Sec. 1798, et seq.)

3) 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 Secs. 1798.14 and 1798.18.)

4) 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 Secs. 1798.15 and 1798.16.)

5) 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 Sec. 1798.17.)

6) Requires each agency to establish rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing PI and 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 any injury.

7) 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, among many other circumstances:

    - With the recent prior written voluntary consent of the individual to whom the PI pertains.

    - To officers, employees, attorneys, agents, or volunteers of the agency that has custody of the PI if the disclosure is relevant and necessary in the ordinary course of the performance of their official duties and is related to the purpose for which the information was acquired.

- 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, including, with respect to law enforcement or regulatory agencies, an investigation of unlawful activity under the jurisdiction of the requesting agency.

- To a governmental entity if required by state or federal law.

- Pursuant to the California Public Records Act. (Gov. Code Sec. 6250, et seq.)

- Pursuant to a determination by the agency that maintains the PI that compelling circumstances exist that affect the health or safety of an individual, if notice is transmitted to the individual's last known address.

- Pursuant to a subpoena, court order, search warrant, or other compulsory legal process with notification to the individual, unless notification is prohibited by law.

- For statistical and research purposes, as specified.

- To a committee of the Legislature or a Member of the Legislature, or the member's staff if authorized in writing, if the member has permission to obtain the PI from the individual, or with reasonable assurance that the member is acting on behalf of the individual. (Civ. Code Sec. 1798.24.)

8) 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 Secs. 1798.25 and 1798.27.)

9) 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 PI 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 PI pertaining to them maintained by an agency. (Civ. Code Sec. 1798.30, et seq.)

10) 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 Secs. 1798.46-1798.48.)

11) Permits an individual to bring a civil action against an agency if: the agency refuses to comply with a lawful request to inspect records pursuant to 9), above; the agency's failure to maintain any record concerning the individual with such accuracy, relevancy, timeliness, and completeness as necessary to assure fairness in any determination made on the basis of the record, and the resulting determination is adverse to the individual; or the agency fails to comply with any other provision of the IPA in a way that has an adverse effect on an individual. (Civ. Code Sec. 1798.45.)

12) 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 Secs. 1798.55 and 1798.57.)

13) Requires each state agency, when it provides by contract for the operation or maintenance of records containing PI 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 Sec. 1798.19.)

14) Defines "personal information", for the purposes of the IPA, to mean any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history, including statements made by, or attributed to, the individual. (Civ. Code Sec. 1798.3(a).)

15) 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 Sec. 1798.3(b); Gov. Code Sec. 6252(a).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to clarify, simplify, and modernize the provisions of the IPA in order to better protect Californians' PI that is collected, stored, and shared by government agencies. This bill is author sponsored.

2) **Author's statement**: 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.

3) **The Information Practices Act of 1977**: The Information Practices Act of 1977 (IPA; Civ. Code Sec. 1798, et seq.), modeled after the Federal Privacy Act of 1974, is the primary privacy scheme governing the collection, maintenance, and disclosure of personal information by state agencies. 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 PI by government agencies as follows:

> The Legislature 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. The Legislature further makes the following 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.
>
> (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 Sec. 1798.1.)

Generally, the IPA places several conditions and restrictions on the collection, maintenance, and disclosure of the PI of Californians held by state agencies, including a prohibition on the disclosure of an individual's PI without the individual's consent except under one of several specified circumstances, and a requirement that along with any form requesting PI from an individual, an agency must provide notice of information pertaining to the individual's 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, with few additional privacy protections generally stipulated in the contracts themselves. For a more detailed description of the major provisions of the IPA, see the "Existing Law" section of this analysis.

This bill would amend the IPA in several ways to clarify, update, and strengthen many of these protections.

4) **Some provisions of the IPA are arguably outdated or insufficient**: The findings and declarations included in the IPA remain strikingly relevant to the modern information ecosystem, but advances in technology have monumentally shifted the scope and diversity of

PI collected and maintained by government agencies, likely far beyond the circumstances envisioned when the IPA was first conceived. For example, the State's Employment Development Department (EDD) has recently adopted identity verification and fraud detection tools that rely on opaque, artificial intelligence-based technology to flag claims of interest for further investigation. One such tool, the Thomson Reuters ID Risk Analytics framework, "combines a database of comprehensive public and proprietary records to verify identities. That data is then run through Pondera Solutions, which utilizes refined pattern-detection, program-specific models, and criminal network detection algorithms to identify more sophisticated schemes." In order to function, these tools rely on the accumulation of massive amounts of PI from public and private sources, increasing the risk that sensitive data concerning California's most vulnerable residents may be compromised or inappropriately disclosed. The specific data inputs and outputs relied on by these tools are also highly sophisticated, baring less resemblance to the types of straightforward "personal information" contemplated in 1977 when the IPA was first enacted (e.g. name, SSN, home address, etc.). As a result, the data amassed and examined by such technology fall less clearly within the boundaries of the existing, arguably outdated definition of "personal information," which the IPA protects against inappropriate collection and sharing.

While the IPA provides several fundamental privacy protections, many of its provisions seem increasingly outdated. More than ever, state agencies are contracting with sophisticated technology services with the means to extract commercially valuable insight from the government data with which they are entrusted, many of whom notoriously traffic in the aggregation and sale of such insights. Though the IPA nominally protects PI of California residents held by the government from misuse and wanton disclosure, several shortcomings limit the effectiveness of these protections. For instance, the definition of "personal information" is quite narrow and does not seem to incorporate information that could be used, either through processing or in combination with other information, to identify an individual. The IPA defines PI to mean "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history." (Civ. Code Sec. 1798.3(a).) Under this definition, information that has been deidentified (i.e. divorced from the individual's name), but is still readily reidentifiable, arguably would not be covered. This could include information such as device geolocation data, income information, and even medical data. Because the IPA applies to contractors as well as state agencies (Civ. Code Sec. 1798.19), technologically advanced companies such as Google, Amazon, and Facebook could potentially obtain deidentified information through a state contract, without any immediately evident prohibition against reidentifying that information via integration with existing data held by the company.

The IPA's enforcement structure has also been criticized for failing to incentivize due care with respect to the PI of individuals by government agencies. While the intentional violation of the IPA by an officer or employee of an agency constitutes cause for discipline under the law, the statute is silent with respect to negligent violations. Even for intentional violations in which an individual's highly sensitive medical, psychiatric, or psychological information is wrongly disclosed, the prescribed misdemeanor penalty is only applicable "if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains." It is notoriously difficult under existing legal precedent to establish, and especially to quantify, economic loss or personal injury for violation of personal privacy,

making it nearly impossible for such a penalty to apply. Additionally, the IPA does not apply to local governments, leaving any sensitive data collected by local agencies virtually unprotected by existing statutory frameworks.

This bill seeks to bring the IPA's protections in line with the role the collection and transfer of PI plays in modern life. To do so, the bill would make several updates to definitions and substantive provisions of the IPA, including expanding the definition of PI to include information that is reasonably capable of identifying an individual, prohibiting an agency from using records containing PI for any purposes other than those for which the PI was collected, except as specified, adjusting penalties for violations of the law to include discipline for negligent violations by agency employees and to eliminate injury-in-fact requirements for intentional disclosures of sensitive information, and applying the IPA to local agencies.

5) **Definition of PI**: Because the IPA primarily serves to regulate the handling of PI by government agencies, the adequacy of the protections it provides necessarily hinges on the way PI is defined. The IPA currently defines "personal information" to mean "any information that is maintained by an agency that *identifies or describes an individual*, including, but not limited to, his or her 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." In addition to neglecting to explicitly include several more modern forms of PI, drawing into question whether these less "traditional" types of PI are intended to be included, this definition also seems to imply that the information must actively identify or describe a particular individual in order to qualify as PI. In other words, even if, through processing or integration with other information, that information can ultimately identify a person, so long as the information is not maintained in a manner directly associated with an individual, it may not qualify as PI under the current definition.

   This bill would amend the definition of "personal information" upon which the IPA relies to contemplate information that is not presently identifiable but could be reidentified, and expressly includes types of information resulting from technology that was far less common when the IPA was originally enacted. Specifically, the bill would define "personal information" to mean "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." In support of the bill, Oakland Privacy argues that "[t]his change is more consistent with current privacy laws and recognizes that digital data that may fall short of absolute identification may still under certain circumstances be capable of identifying specific individuals. […] [The added examples of covered PI] are responsive to changes in technology since 1977 and the kinds of personal information generally in circulation and broadly held by governmental agencies."

6) **Data minimization**: Existing law, pursuant to the IPA, 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. (Civ. Code Secs. 1798.14.) Existing law, pursuant to the IPA, also

requires each agency to provide with any form used to collect PI from individuals a notice containing specified information including 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; and any known or foreseeable disclosures that may be made of the information. (Civ. Code Sec. 1798.17.) While these provisions provide some information to Californians with respect to permissible government uses for their information, they are neither abundantly clear, nor particularly limiting. So long as principle purpose for which the PI will be used is disclosed to the individual, that information can be used for any number of secondary purposes that may fall within the agency's authority but are wholly unrelated to the reason that information was initially provided.

Seeking to provide Californians with more complete information regarding the permissible uses of PI they entrust to the government, this bill imposes a data minimization requirement by prohibiting an agency from using records containing PI for any purpose or purposes other than the purpose or purposes for which that PI was collected, except as required by federal law, or as authorized or required by state law. The latter qualification seemingly provides adequate flexibility to accommodate other state laws granting specific authority for uses of PI collected by particular agencies. Additionally, the bill would require that the notice provided with any form used to collect PI specify the purpose or purposes for which the information is to used, rather than only requiring disclosure of the *principal* purpose or purposes. As Oakland Privacy explains in support of the bill, "[d]ata minimization or data use confined by collection purpose is a fundamental building block of privacy regulation. It is long overdue for California's state and local governments to commit themselves to privacy-protective actions by default."

7) **Penalties for negligent violations and intentional disclosures of sensitive PI**: Existing law specifies that the *intentional* violation of any provision of the IPA, or of any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment. (Civ. Code Sec. 1798.55; emphasis added.) However, existing law does not impose penalties for negligent violations of the provisions of the IPA, meaning the negligent disclosure of an individual's PI by an at-fault employee does not entail any statutory punishment. Arguably, this lack of available penalties to deter carelessness in the handling of PI does not sufficiently encourage due care in the handling of PI. Additionally, demonstrating intent for a given action can be particularly difficult, further complicating enforcement of the IPA's provisions. To better incentivize care and compliance with the provisions of the IPA, AB 2677 would amend the penalty provisions of the IPA to specify that both intentional and negligent violations of the provisions of the IPA by an employee of an agency constitute causes for discipline. As Oakland Privacy argues in support of the bill:

> Addition of negligent behavior to an enforceable violation […] correctly assesses that some disastrous data mishandling that results in privacy harm may be negligent rather than intentional on the part of governmental agencies, but the lack of intention doesn't eliminate the harm experienced and the need for governmental agencies to take corrective action, including and up to termination, to ensure that the negligence does not recur.

Existing law also specifies that, except for disclosures otherwise required or permitted by law, 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 Sec. 1798.57; emphasis added.) With respect to privacy violations, however, demonstrable harm (i.e. economic loss or personal injury) is particularly difficult to prove, let alone quantify. As Danielle Keats Citron and Daniel J. Solove explain in a publication in Boston University's Law Review:

> The requirement of harm has significantly impeded the enforcement of privacy law. In most tort and contract cases, plaintiffs must establish that they have suffered harm. […] Caselaw is an inconsistent, incoherent jumble, with no guiding principles. Countless privacy violations are not remedied or addressed on the grounds that there has been no cognizable harm.
>
> Courts struggle with privacy harms because they often involve future uses of personal data that vary widely. When privacy violations result in negative consequences, the effects are often small – frustration, aggravation, anxiety, inconvenience – and dispersed among a large number of people. When these minor harms are suffered at a vast scale, they produce significant harm to individuals, groups, and society. But these harms do not fit well with existing cramped judicial understanding of harm.[1]

This bill would remove the requirement that an intentional wrongful disclosure of medical, psychiatric, or psychological information must result in economic loss or personal injury to the individual to whom the information pertains in order to qualify for prosecution as a misdemeanor offense. The existing requirement is arguably inappropriate in the context of wrongful disclosure, and may be insufficient to properly incentivize compliance. As the Electronic Frontier Foundation argues in support of the bill:

> A.B. 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 intentional disclosure of "medical, psychiatric, or psychological information" to be considered a misdemeanor. This rightly acknowledges that harms are not simply monetary or bodily, but that improper disclosure itself can meaningfully and negatively affect a person's life.

Together, these updates to the penalty provisions of the IPA seem to align more appropriately with the objectives of the IPA, namely to incentivize due care and disincentivize wrongful disclosure of the PI maintained by government agencies.

8) **Bill would apply the IPA to local agencies**: Since its passage in 1977, the IPA has exempted local governments from its provisions. In 2013, acknowledging the increasing corpus of PI maintained by local agencies and the risks arising from unauthorized disclosure, this Legislature passed AB 1149 (Campos, Ch. 395, Stats. 2013), which, among other things, explicitly applied the data breach notification requirements of the IPA to local agencies. Noting the numerous cyberattacks impacting local agencies across the country, cybersecurity experts have indicated that the IT systems of local governments are particularly vulnerable to compromise, making the inclusion of local governments in the IPA's data breach notification requirements a critical improvement. As an August 2021 Washington Post article points out,

---

[1] Solove DJ & Keats Citron D, "Privacy Harms," 102 B.U. L. Rev. __ (2022).

"Often strapped with small IT departments, aging computer systems and limited budgets to allocate to cybersecurity, local governments across the country make for ill-equipped and easy targets for criminals."[2]

Still, under existing law, local agencies in California are not governed by any comprehensive privacy law protecting PI pertaining to individuals. As result, the data privacy and security practices of local agencies are made up of a patchwork of opaque policies that differ between entities and lack a required baseline level of protection. This situation arguably makes it more difficult for individuals to understand their rights with respect to PI collected by local governments, and complicates interactions between agencies when necessary. As the Electronic Frontier Foundation and Privacy Rights Clearinghouse describe in support of the bill:

> From an operational standpoint, the Information Practices Act of 1977 has needed an update for some time to deal effectively with the way information flows and is shared today. As written today, the IPA has many exemptions and exceptions, which make it difficult to understand how different entities can work together. This has become even more clear in the wake of the state's response to the COVID-19 pandemic. As the state undertook a massive data collection effort to deploy response efforts to the pandemic and evaluate the effectiveness of those efforts, it became clear that the system the IPA creates – in which each local entity creates its own privacy policies and rules – sows confusion about how entities can work together while also respecting their own regulations around data collection and sharing.

Significantly, this bill would remove the exemption for local agencies in the IPA's definition of "agency," applying the Act's provisions to local agencies wholesale. Consequently, AB 2677 would provide the State's first comprehensive framework to govern the PI collected, used, and disclosed by local agencies. In support of the bill, ACLU California Action argues:

> AB 2677 would require local governments to comply with the same standards as state entities. Local entities are responsible for administering many services to Californians, such as municipal services including trash and utility management, as well as COVID testing and vaccine administration. A single, privacy-protective standard allows for more efficient interactions across the state and a stronger guarantee that information is being processed in a respectful way.

Opponents of the bill, which consist of a coalition of groups representing local governments, contend that the imposition of the requirements of the IPA would be too onerous for local governments to comply with using existing resources, especially for smaller local agencies that operate on extremely small budgets. The coalition argues:

> The bill in its current form does not appear to contemplate the vast technical effort that would be required for thousands of agencies to immediately 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

---

[2] Karina Elwood, "Ransomware poses threat to vulnerable local governments," *Washington Post*, Aug. 22, 2021, https://www.washingtonpost.com/local/local-government-ransomware-dc/2021/08/05/048051cc-efc6-11eb-81d2-ffae0f931b8f_story.html [as of Apr. 13, 2022].

> personnel changes, including hiring new specialized staff and widespread training, especially important given the statutorily required penalties in the Act, up to and including termination, for errors made in negligence. This requirement for new staff would come at a time local agencies are experience workforce shortages, high vacancy rates and are struggling to fill existing positions.
>
> Application of the Act to local agencies would not only require time and staff capacity, it would also require significant financial resources that are not provided in the bill. […] Application of the Act to local agencies must be accompanied by sustainable and sufficient resources.

Arguably, the provisions of the IPA, and the bill in print, in many ways reflect foundational best practices for the protection of PI, in which case the additional burden imposed on local agencies that already boast sufficiently protective policies and procedures for protecting PI should be minimal, consisting of minor tweaks to existing protocols. For local agencies who currently lack policies consistent in any way with the provisions of the IPA, the impositions of the IPA seem to be necessary to ensure sufficient protection of the PI of constituents. Committee staff notes that, according to the Assembly Committee on Local Government's Analysis of AB 1149 (Campos, Ch. 395, Stats. 2013), a nearly identical coalition of organizations representing local agencies raised substantively similar concerns with the application of the IPA's data breach notification requirements to local governments, arguing that bill would impose "potentially costly new responsibilities on local agencies at a time when we are challenged to deliver core public services given difficult fiscal conditions." Notably, since the passage of that bill, local agencies have effectively maintained compliance with its provisions despite these concerns, allowing constituents to respond to data breaches affecting their PI held by local agencies in a manner that better protects their information and identities.

Nonetheless, for these agencies, the time necessary to attain compliance with the IPA's requirements may exceed the time before AB 2677 would come into effect, and therefore be enforceable, if passed (January 1, 2023). The changes to the existing provisions of the IPA should not require a major overhaul of the internal information management policies and procedures for state agencies that must already comply with the IPA as it currently reads, but establishing policies and procedures to accommodate all provisions of the IPA may indeed be a lengthier process. Accordingly, the author has offered an amendment to delay the implementation of the bill as it pertains to local agencies by one year.

> Author's amendment:
>
> *Delay implementation of provisions of the bill requiring local agencies to comply with the IPA by one year; and make conforming changes.*

The coalition representing local governments further argues that because the IPA was not conceived with local agencies in mind, its provisions, and the provisions of this bill, are not appropriate to apply to local agencies and do not make sense in that context. According to the coalition:

> The Act 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 2677 would amend the law, agencies under the IPA would be required to comply with the State

> Administrative Manual and the State Information Management Manual, highly detailed documents that are clearly prepared for state agencies and departments. […] 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.

Committee staff notes that the bill in print does not require local agencies to *comply* with all provisions of the SAM and the SIMM, but rather that the rules of conduct for persons involved in the design, development, operation, disclosure, or maintenance of records containing PI be *consistent with applicable provisions of* the SAM and the SIMM. Because the SAM and SIMM are developed as applicable to state agencies only, this provision is unlikely to require local agencies to comply with any policies and procedures laid out in the SAM and the SIMM, let alone those clearly applicable only to state agencies. Even if the bill were read to require local agencies to develop rules of conduct for persons involved in functions related to PI that are consistent with the SAM and the SIMM, which does not appear to be the case, the bill would nonetheless only require *consistency* with those provisions, rather than compliance. As such, a legal interpretation of this provision to require wholesale compliance by state agencies with all provisions of the SAM and the SIMM seems highly unlikely.

PI held by local agencies does not differ qualitatively from PI held by state agencies, and considering the types of services orchestrated by local agencies, may even be more sensitive and more extensive. Whether such information is inappropriately disclosed by a state agency or a local agency, the potential risks and infringements on privacy rights are identical. Though upon its passage, the IPA elected to exclude local agencies, the capacity for local governments to amass large troves of PI and to apply that information in different ways has resulted in a far more involved role for local governments in the information ecosystem than was the case in 1977. Efforts to enact evidence-based policies relying on data from individuals can provide significant benefits to the general public, but the sophisticated analyses conducted in order to do so generally involve large quantities of PI that must be appropriately managed. Considering the ways California's information economy has evolved over the past 45 years, requiring the compliance of local agencies with the provisions of the IPA is arguably overdue.

9) **Related legislation**: AB 1711 (Seyarto) would require a person or business operating an information system on behalf of an agency that is required to disclose a breach of that system pursuant to existing law, to also disclose the breach by conspicuously posting the requisite notice on the agency's website, if the agency maintains one.

AB 1917 (Levine) would prohibit a correctional officer or an officer, deputy, employee, or agent of a law enforcement agency from conducting contact tracing, as defined.

AB 2308 (Kiley) would amend the definition of "commercial purpose" in the IPA to mean any purpose that has financial gain as *an* objective, rather than as *a major* objective.

AB 2355 (Salas) would require a local educational agency (LEA), as defined, to report any cyberattack, as defined, that impacts more than 500 pupils and personnel to Cal-CSIC; AB 2355 would further require that Cal-CSIC establish a database that tracks reports of cyberattacks submitted by LEAs, and that Cal-CSIC annually report to the Governor and the

relevant policy committees of the Legislature specified information concerning cyberattacks affecting LEAs.

AB 2488 (Irwin) would require a public agency that collects precise geolocation data, as defined, to receive and maintain consent for the collection of precise geolocation data; and further require that a public agency that collects precise geolocation data maintain reasonable security procedures and practices to protect that data from unauthorized access, destruction, use, modification, or disclosure and implement a usage and privacy policy, as specified.

10) Prior legislation: 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. AB 660 would have also enacted provisions substantially similar to AB 1917. This bill died on suspense in the Senate Committee on Appropriations.

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. This bill died at the Assembly Desk.
AB 928 (Olsen, Ch. 851, Stats. 2014) requires each state department and state agency to conspicuously post its privacy policy, including specified information, on its website.

AB 2147 (Melendez, 2014) would have required a state agency that uses a website to obtain information by means of an electronic form and shares that information with another state agency or private party to provide a disclosure notice that the information may be shared in accordance with the IPA as specified. This bill died on suspense in the Assembly Committee on Appropriations.

AB 1149 (Campos, Ch. 395, Stats. 2013) *See* Comment 8.

AB 2455 (Campos, 2012) was substantially similar to AB 1149. This bill died on suspense in the Assembly Committee on Appropriations.

REGISTERED SUPPORT / OPPOSITION:

Support

ACLU California Action
California Association of Licensed Investigators
Electronic Frontier Foundation
Oakland Privacy
Privacy Rights Clearinghouse

Opposition

Association of California School Administrators
Association of California Healthcare Districts
California State Association of Counties
League of California Cities

Rural County Representatives of California
Urban Counties of California

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200