Date of Hearing: April 8, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1436 (Chau) – As Introduced February 19, 2021

SUBJECT: Information Practices Act of 1977

SUMMARY: This bill would refine the findings and declarations in the Information Practices Act (IPA) to state the that the use of *software* has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information (PI) and in order to protect the privacy of individuals, it is necessary that in addition to the maintenance and dissemination, the *collection* and *security* of PI should be subject to strict limits and *standards*.

EXISTING LAW:

1) Establishes the IPA, which regulates the use and security of PI, as defined, that is maintained by certain state public entities. The IPA makes certain findings, including that 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 PI. (Civ. Code Sec. 1798 et seq.)

2) Requires state agencies to 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 Sec. 1798.14.)

3) Requires state agencies to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with 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. (Civ. Code Sec. 1798.21.)

4) Provides that any agency that fails comply with any provision of the IPA may be enjoined by any court of competent jurisdiction. (Civ. Code Sec. 1798.47.)

5) Defines "PI" to mean any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, their 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 Sec. 1798.3(a).)

6) Defines "maintain" to include maintain, acquire, use, or disclose. (Civ. Code Sec. 1798.3(e).)

FISCAL EFFECT: None. This bill has been keyed nonfiscal by the Legislative Counsel.

COMMENTS:

1) **Purpose of this bill**: This bill seeks to enhance the protection of PI by requiring that government agencies take into account the collection, maintenance, and security of PI collected and held by government computers and software. This bill is author-sponsored.

2) **Author's statement**: According to the author:

> As a state, we have been diligently been working for decades to ensure that the personal information of California residents is protected. The Information Practices Act of 1977 safeguards privacy by providing limits on the maintenance and dissemination of personal information by state agencies. Despite these protections, the exploitation of security vulnerabilities continues to be a growing threat as new technologies and methods of cyberattack emerge, both of which require ongoing monitoring to avoid data breaches, phishing, and other targeted attacks on personal information.
>
> At the same time, in a tremendous collective effort to keep employees, consumers, and residents safe, businesses and governments around the world have begun offering their services online so individuals are not put at risk of infection. These new practices have led to increased reliance on the use of personal devices to connect with company servers, creating seemingly endless new targets for cybercriminals. As evidenced by the *SolarWinds* hack which used malware to target U.S. Federal agencies to hold personal information and other data hostage for ransom, many methods of cyberattack no longer rely on a physical connection and can instead by accomplished via software. These cyberattacks are projected to continue and increase with volatility.
>
> To protect the personal information of all residents, California should require state agencies to follow information technology practices that reflect the evolving nature of how information is collected, used, stored, and compromised.
>
> By updating the findings in the IPA to include the use of software and call attention to the collection and security standards employed by state agencies, this bill will change the lens through which the entire IPA is interpreted and place more of an emphasis on best technology practices to keep the personal information of Californians safe.

3) **Background on the Information Practices Act**: In 1972, the people of California amended the state Constitution to provide explicit language protecting the personal right of privacy. Five years later, the Legislature enacted the Information Practices Act of 1977 (IPA). (Civ. Code, Sec. 1798 et seq.) The IPA's introductory provision 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." (Civ. Code Sec. 1798.1.) That section goes on to provide that the right to privacy was being threatened by "the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies" and that 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." (Civ. Code Sec. 1798.1 (a) and (b).)

   To guard against those threats, the IPA places limits on "the maintenance and dissemination of personal information." (Civ. Code Sec. 1798.1(c).) "Personal information" is defined to include "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." (Civ. Code Sec. 1798.3 (a).)

Under the IPA, state agencies are required to limit the collection and retention of PI to that necessary to accomplish the agency's specific purpose. (Civ. Code Sec. 1798.14.) If an agency maintains such a record, individuals have the right to be notified of that fact. (Civ. Code Sec. 1798.32.) Further, individuals may request amendments to correct any inaccurate information (Civ. Code Secs.1798.35-1798.37.) Notably, all disclosures of PI are restricted, and an accounting of such disclosures must be made, including disclosures pursuant to subpoena or search warrant (Civ. Code Secs. 1798.24 and 1798.25.)

By including in the introductory purpose of the IPA that the Act is intended to address threats to privacy because of the increasing collection of PI by *software*, in addition to emphasizing the need to subject the *collection* and *security* of PI to strict limits and standards, this bill would recast the lens through which the IPA is interpreted, thereby updating the act to better align with Californians' reasonable expectation of privacy in light of new technologies and practices that have been developed since 1977.

4) **Changes in technology and cybercrime warrant updating of the purpose of the IPA**: Since the enactment of the IPA in 1977, numerous developments in technology and resulting changes in the public's understanding of the constitutional right to privacy have led to significant change in this State's privacy laws. For example, SB 1936 (Peace, Ch. 915, Stats. 2002) enacted the data breach notification law (DBNL) in California, which requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data including PI, to disclose any breach of the security of the data to California residents whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person.

   Since that time, California has added numerous provisions to the DBNL to protect residents as data breaches become more commonplace. For example, in 2004, AB 1950 (Wiggins, Ch. 877, Stats. 2004) required a business that owns or licenses PI about a California resident to implement and maintain reasonable security procedures and practices to protect PI from unauthorized access, destruction, use, modification, or disclosure. AB 1710 (Dickinson, Ch. 855, Stats. 2014) required the source of the breach to offer appropriate identity theft prevention and mitigation services to consumers at no cost, AB 2828 (Chau, Ch. 337, Stats. 2016) required notification of breaches of encrypted PI if an encryption key or security credential that could render the PI readable was also compromised in the breach, and AB 1130 (Levine, Ch. 750, Stats. 2019) added government-issued identification numbers and unique biometric data to the DBNL definition of PI.

   More recently, in 2018, the Legislature enacted the California Consumer Protection Act (CCPA) (AB 375, Chau, Ch. 55, Stats. 2018), which gives consumers certain rights regarding their personal information (PI), such as: (1) the right to know what PI that is collected and sold about them; (2) the right to request the categories and specific pieces of PI the business collects about them; and (3) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age. The CCPA was the byproduct of compromises made between business interests on one side, and consumer and privacy interests on the other, to provide a legislative alternative to a ballot initiative on the same subject.

   Last year, California voters passed Proposition 24, which, in addition to establishing certain new rights, renames the CCPA as the California Privacy Rights Act (CPRA). Importantly, to protect Californians from any future legislative efforts to weaken statutory protections in

the CPRA, Proposition 24 provided that the CPRA's contents may be amended by a majority vote of the Legislature only if the amendments are consistent with and further the purpose and intent of the CPRA, which is to further protect consumers' rights, including the constitutional right of privacy. (Ballot Pamp., Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74.)

Directly relevant to this bill are the changes the Legislature has made to the IPA since 1977, including AB 1751 (Low, Ch. 478, Stats. 2018) which made certain necessary changes to terminology for the purposes of the statute (e.g., "natural parent" to "biological parent") and also authorized sharing of PI under the IPA for the "sole purpose of participation in the interstate California Uniform Controlled Substances Act so long as disclosure is lonely limited to the prescription drug monitoring program information. In addition, AB 1130 (Levine, Ch. 750, Stats. 2019) further clarified the definition of PI for the purposes of the DBNL to include government-issued IDs and biometric data.

Despite changes to the IPA itself, the intent and purpose of the act has never been updated, which could arguably lead to applications of recently updated provisions in the IPA that are inconsistent with the intent of the Legislature in passing those various laws. In other words, when interpreting a statute and applying it to the facts of a specific case, attorneys and courts often turn to the statute's legislative history to understand the Legislature's intent and public policy behind the law. For courts, the best legislative history tends "to be that which represents a large body of legislators, not just the bill's author or one side of the public policy debate." (Micheli, *Statutory Construction Guidelines for Bill Drafting in California*, (2021). 52 U. Pac L. Rev 457, p.468.) Many bills contain legislative intent that is uncodified, which is likely not as persuasive as language in the code itself. The IPA, however, has a detailed, codified legislative purpose that was approved by a majority of the Legislature, which makes it an important tool in interpreting the IPA.

By way of example, in *Bates v. Franchise Tax Bd.* 124 Cal.App.4th 367 (2004), plaintiff taxpayers sued defendants, the Franchise Tax Board, the Board of Equalization, and state employees, under the IPA. Plaintiffs alleged use of nonpersonal information in determining individual tax liabilities and failure to provide access to records maintained about them. The Superior Court dismissed the action and the taxpayers appealed. As to the allegation that defendants used nonpersonal information to determine tax liabilities, the court found that this claim was not actionable under the IPA. However, the taxpayers did state claims under the IPA to the extent that they alleged that information used to assess taxes was not handled in compliance with the IPA. In reaching these conclusions, the court looked to the express purpose of the IPA found in Civil Code Section 1798.1, which this bill would amend, and used that purpose to interpret specific provisions of the IPA which plaintiffs alleged had been violated. (*Bates* at 376-77.)

As described above, the changes to this State's privacy laws in recent years show the public's and the Legislature's continued interest in ensuring that the constitutional right to privacy continues to be effective and robust despite technological developments that could arguably dilute the effectiveness of existing statutory protections. By acknowledging in the purpose of the IPA increased threats to personal privacy because of the widespread use of software, in addition to emphasizing strict standards in the collection and security of PI, this bill would broaden how specific provisions in the IPA should be interpreted, which should increase protections for the personal privacy of the residents of this State.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

Analysis Prepared by: Nichole Rocha / P. & C.P. / (916) 319-2200