Date of Hearing: March 26, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1130 (Levine) – As Introduced February 21, 2019

SUBJECT: Personal information: data breaches

SUMMARY: This bill would include the following in the definition of personal information in California's Data Breach Notification Law as it applies to both public agencies and businesses: (1) government-issued identification numbers; and, (2) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data. The bill would also make other corresponding and technical changes.

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.)

1) Sets forth, in the Information Practices Act, the right of an individual who is the subject of information maintained in state or local agency records to have access to that information. (Civ. Code Sec. 1798 et seq.)

2) Requires any agency, person, or business that owns or licenses computerized data that includes personal information (PI) to disclose a breach of the security of the system to any California resident whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as specified. (Civ. Code Secs. 1798.29(a) and (c); 1798.82(a) and (c).)

3) Requires any agency, person, or business that maintains computerized data that includes PI that the agency, person, or business does not own to notify the owner or licensee of the information of any security breach immediately following discovery if the PI was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code Secs. 1798.29(b), 1798.82(b).)

4) Defines "PI," for purposes of the data breach notification statute, to include either a user name or email address, in combination with a password or security question and answer that would permit access to an online account, or the individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted: social security number; driver's license number or California identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; or health insurance information. "PI" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code Secs. 1798.29(g) and (h); 1798.82(h) and (i).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to better protect the personal information of California residents by adding government-issued identification numbers and biometric data to the definition of PI under the Data Breach Notification Law. This bill is sponsored by the California Attorney General.

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

> AB 1130 requires businesses to notify individuals whenever their passport number or biometric information has been compromised in a data breach and to maintain security measures to protect these types of personal information.
>
> More specifically, this bill would expand the definition of "personal information" in our breach notification statute to include government-issued identification numbers and a person's biometric information. In the case of the former, the bill would effectively cover the breach of not only U.S. passport numbers, but the identification numbers on non-U.S. passports, passport cards, and permanent resident cards, to help California residents who are not necessarily U.S. citizens. In the case of the latter, we employ a working definition of biometric information to mean: "unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data."
>
> Finally, to ensure consistency, the bill would also require businesses to reasonably secure these data points by amending Section 1798.81.5 in a corresponding fashion.

3) **Background**: SB 1936 (Peace, Ch. 915, Stats. 2002) enacted the data breach notification law (DBNL) in California that requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes PI, to disclose any breach of the security of the data to California's residents whose unencrypted personal information 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, and 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.

   In 2017, Equifax, one of the three major consumer credit reporting agencies, suffered a cybersecurity breach that gave criminals access to information including consumer names, social security numbers, birth dates, addresses, and in some instances, driver's license numbers. Credit card numbers were accessed for approximately 209,000 U.S. consumers, as were documents with personal identifying information for approximately 182,000 U.S. consumers. The Equifax breach, which affected nearly 50 percent of the total U.S. population of 323 million people, was not an isolated or limited incident. According to news reports, at

the time of its occurrence, the Equifax breach was only the fifth largest data breach impacting U.S. consumers. (Wise, USA Today *Equifax breach: Is it the biggest data breach?* (Sept. 2017) < https://www.usatoday.com /story/tech/ 2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001/> [as of Mar. 15, 2019].)

While no federal data breach laws exist, all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws requiring private or governmental entities to notify individuals of security breaches involving personally identifiable information. (National Conference on State Legislatures, *Security Breach Notification Laws*, Updated Feb. 22, 2019 <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> [as of Mar. 15, 2019].)

4) **Government-issued identification numbers**: PI is defined for the purposes of the DBNL to include either a user name or email address, in combination with a password or security question and answer that would permit access to an online account, or the individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted: social security number; driver's license number or California identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; or health insurance information. PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Civ. Code Secs. 1798.29(g) and (h); 1798.82(h) and (i).)

   This bill would add government-issued identification numbers to the definition of PI in the data breach notification law. This addition is arguably consistent with the current definition of PI which already includes driver's license numbers and California identification numbers. Including government-issued identification numbers in the definition would also capture identification numbers issued by other states or countries, such as state-issued identification card numbers and passport numbers.

   The sensitivity of passport numbers gained mainstream attention late last year when Starwood Hotels (recently acquired by Marriott) announced a data breach affecting the records of up to 500 million customers. For approximately 327 million of these guests, the information included some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. Meanwhile, for some, the information also included payment card numbers and payment card expiration dates. The company reported that the payment information was encrypted but the company could not rule out the possibility that the elements needed to break the encryption were also taken in the breach. (O'Flaherty, *Marriott Breach - What Happened, How Serious Is It And Who Is Impacted?* Forbes (Nov. 30, 2018).)

   Customers whose name and driver's license number that were accessed in that breach are clearly covered under this state's DBNL. However, customers whose name and passport number were accessed might not be covered under those same laws and thereby not be entitled to the same notices and remedies. Passport numbers are unique, government-issued, static identifiers of a person—all characteristics which make them valuable to criminals seeking to create or build fake profiles and engage in sophisticated identity theft and fraud.

By adding "government-issued identification card" to the definition of PI, this bill would effectively cover the breach of not only U.S. passport numbers, but the identification numbers on non-U.S. passports, passport cards, and permanent resident cards, to help California residents who are not necessarily U.S. citizens.

In opposition, a coalition of businesses, including the California Chamber of Commerce argues that "government-issued identification cards" is too broad of a term. "[It] would include government-issued identification numbers from any level of government that pose no risk of harm in the event of a data breach, such as fishing license and professional license numbers. However, we do not oppose the addition of passports to the list of government identification numbers for which notification is required."

Indeed, there are a substantial number of government-issued identification numbers, that carry with them a high risk of identity theft. State-issued identification cards, passport numbers, military identification cards, SENTRI identity cards, and other types of numbers that prove identity, should receive protection under the DBNL. The author and sponsor have expressed a willingness to continue working with the opposition to ensure that the language is narrowly tailored to cover government-issued documents that create risk of identity theft.

That being said, the current version of the bill would cover passport numbers, which are exactly the type of government-issued identification that, if in the wrong hands, creates a risk of identity theft. On this point, the author writes, "[t]he Starwood Hotels' breach highlights the need for California to close this important loophole in existing law, which does not require businesses to notify consumers of data breaches that compromise passport numbers. But for the size of the Starwood breach and other states' laws requiring notice for breach of passport numbers, affected Californians would likely not have learned that this personal data had been compromised."

5) **Unique biometric data**: This bill would also add unique biometric data to the definition of PI for the purposes of the DBNL. The bill would define unique biometric data as "data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data."

   Biometric data is generally described as the measurement and statistical analysis of an individual's physical and behavioral characteristics. (Margaret Rouse, *Biometrics*, <https://www.searchsecurity.techtarget.com/definition/biometrics> [as of Mar. 15, 2019].) Typically, there are two main classes of biometrics: physiological characteristics and behavioral characteristics. Physiological characteristics concern the shape or composition of the body while behavioral characteristics concern the behavior of an individual. Physiological biometrics includes facial recognition, fingerprint scanning, hand geometry, iris scanning, and DNA. Behavioral biometrics include an individual's keystroke, signature, and voice recognition. The use of biometrics in business is widespread, and the types of usage are constantly evolving. With new technological developments and the technology itself becoming more readily available, industries of all sizes and kinds are turning to biometric data collection to enhance their time management, security access, safety, and employer-provided health plans.

In considering legislation this year that would regulate, to a degree, biometric data, California joins a handful of other states including Massachusetts, New York, Delaware, Alaska, and Michigan. Illinois was a pioneer in recognizing the sensitive nature of biometric data and enacted the Biometric Information Privacy Act (BIPA) in 2008, one of the first state laws to address business' collection of biometric data. (740 ILCS 14 et seq.) BIPA set forth a comprehensive set of rules for companies collecting biometric data of state residents, and has five key features. Specifically, BIPA: (1) requires informed consent prior to collection; (2) permits a limited right to disclosure; (3) mandates protection obligations and retention guidelines; (4) prohibits profiting from biometric data; and, (5) creates a private right of action for individuals harmed by BIPA violations.

BIPA was largely ignored after enactment in 2008, until 2015 when a series of five class action lawsuits were brought against businesses alleging the unlawful collection and use of biometric data of Illinois residents. Several other similar customer-based class actions are currently in motion. However, early this year the Illinois Supreme Court unanimously ruled that when companies collect biometric data without informed opt-in consent, they can be sued, and users do not need to prove an injury or harm to prevail. (Lynch and Schwartz, *Victory! Illinois Supreme Court Protects Biometric Privacy* Electric Frontier Foundation (Jan. 25, 2019) <https://www.eff.org/ deeplinks/2019/01/victory-illinois-supreme-court-protects-biometric-privacy> [as of March 15, 2019].)

In contrast to the breadth of BIPA, this bill requires companies who collect biometric information to take steps to secure that information, and notify customers if that information has been subject to a data breach, as required under the DBNL. These requirements should help ensure that Californians have a better ability to respond when their sensitive biometric information has been subject to a data breach, and should also help ensure that companies who collect this information properly safeguard its security.

6) **Interaction with other state privacy laws**: On June 28, 2018, the California Legislature unanimously passed, and the Governor signed AB 375 (Chau, Ch. 55, Stats. 2018), a significant expansion of data privacy protections for Californians. That new law, the California Consumer Privacy Act (CCPA), guarantees consumers certain rights and protections with respect to the collection and sale of their PI. These rights and protections include the following:

- The right of a consumer to access their PI. (Civ. Code Sec. 1798.100.)
- The right to know what PI is collected about a consumer by a business. (Civ. Code Sec. 1798.110.)
- The right to know whether PI is sold or disclosed by a business. (Civ. Code Sec. 1798.115.)
- The right to delete the PI that a business collected from a consumer. (Civ. Code Sec. 1798.105.)
- The right to opt out of the sale of PI, or opt in, in the case of minors. (Civ. Code Sec. 1798.120.)

- The right to equal service and price in goods and services, despite a consumer exercising any of the rights listed above. (Civ. Code Sec. 1798.125.)

As enacted by AB 375, the CCPA represents a legislative effort to reach an agreement on issues relating to the collection and sale of consumers' PI by businesses, both online and otherwise. Those same issues were also the subject of initiative measure, which would have been placed on the November 2018 ballot for Californian voters' consideration in the absence of a legislative solution by June 28, 2018—the deadline to remove an initiative from the November ballot. Immediately after the passage of the CCPA, the original authors of AB 375 sought to correct numerous drafting errors, make non-controversial clarifying amendments, and address several policy suggestions made by the Attorney General in a preliminary clean-up bill at the end of the 2017-2018 legislative session, SB 1121 (Dodd, Ch. 735, Stats. 2018). That bill was signed by Governor Brown on September 23, 2018.

Of particular relevance to this bill, SB 1121 specifically ensured that a private right of action in that bill applied only to the CCPA's section on data breach and not to any other section of the CCPA, as specified. (*See* Civ. Code Sec. 1798.150.) Adding biometric data and passport numbers to the definition of PI in the DBNL is arguably consistent with SB 1121 in that it does not extend the availability of the private right of action beyond the requirements to maintain appropriate security procedures and practices for information subject to the DBNL.

A coalition of businesses, including the California Chamber of Commerce oppose the bill because it expands liability under the CCPA. The coalition writes:

> While we support adding passport and precisely defined biometric data elements to the breach notification laws, we strongly oppose adding them to Section 1798.81.5 because this would create significant class action litigation risk for breaches without any consideration of harm. Further, biometric data is a safer way to authenticate identity than a social security number. Unlike social security numbers, biometric data is not a one-size-fits-all identifier. There are many kinds of biometric data - not one – and, therefore, the breach of one particular type of that data does not create a significant risk of identity theft or fraud. However, adding it to the list of statutory damage data elements in Section 1798.81.5 would strongly discourage the use of this effective, pro-privacy security measure.
>
> […]
>
> Finally, the language defining biometric data in AB 1130 is also overly broad and confusing. The reference to any "unique physical representation or digital representation of biometric data," could be interpreted too broadly to include photos or behavioral data. It could include shoe size or clothing size plus a name or it might include video showing your gait. This definition is too vague to provide guidance to agencies or businesses regarding what biometric data requires notice.

Staff additionally notes that the definitions of biometric data in the CCPA and this bill (which would add biometric data to the definition of PI under the DBNL) are not consistent. The definition is potentially broader under the CCPA in that the CCPA clearly encompasses an individual's physical characteristics *and* behavior, whereas the definition under this bill would potentially only capture physical characteristics depending on how a court may

interpret this bill's definition with respect to what is captured under "other unique physical representation or digital representation of biometric data." While this might not cover all behavioral biometric data, it could include some forms such as voice recognition or signatures. Given these differences, the author may wish to consider whether and how to better align these definitions so that Californians affected by a data breach involving their biometric information could potentially seek remedies under both laws, assuming they are provided proper notice under the DBNL.

7) **Related legislation**: AB 1035 (Mayes, 2019) would require a person or business that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system within 72 hours following discovery or notification of the breach, subject to the legitimate needs of law enforcement

8) **Prior legislation**: AB 2678 (Irwin, 2018) would have required the notification provided to a person affected by a breach to include, among other things, notice that the affected person may elect to place a security freeze on his or her credit report and an explanation of how a security freeze differs from identity theft prevention and mitigation services. This bill was placed on the Senate inactive file.

   AB 241 (Dababneh, 2017) would have required a public agency that is the source of a data breach, and is required to provide affected persons with notice of the breach, to provide at least 12 months of appropriate identity theft prevention and mitigation services at no cost to the affected persons. This bill died in the Assembly Appropriations Committee.

   AB 2828 (Chau, Ch. 337, Stats. 2016) S*ee* Comment 3.

   SB 570 (Jackson, Ch. 543, Stats. 2015) required, in the event of a data breach, agencies and persons conducting business in California to provide affected individuals with a notice entitled "Notice of Data Breach," in which required content is presented under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."

   AB 1710 (Dickinson, Ch. 855, Stats. 2014) *See* Comment 3.

   SB 46 (Corbett, Ch. 396, Stats. 2013) revised certain data elements included within the definition of personal information under the DBNL, by adding certain information that would permit access to an online account and imposed additional requirements on the disclosure of a breach of the security of the system or data in situations where the breach involves personal information that would permit access to an online or email account.

   SB 24 (Simitian, Ch. 197, Stats. 2011) required any agency, person, or business that is required to issue a security breach notification pursuant to existing law to fulfill certain additional requirements pertaining to the security breach notification, and required any agency, person, or business that is required to issue a security breach notification to more than 500 California residents to electronically submit a single sample copy of that security breach notification to the Attorney General.

   AB 1950 (Wiggins, Ch. 877, Stats. 2004) *See* Comment 3.

   SB 1936 (Peace, Ch. 915, Stats. 2002) *See* Comment 3.

REGISTERED SUPPORT / OPPOSITION:

Support

Attorney General of California Xavier Becerra (sponsor)

Opposition

Advanced Medical Technology Association
California Business Properties Association
California Chamber of Commerce
California Communications Association
California Land Title Association
California Retailers Association
CompTIA
Email Sender & Provider Coalition
Feld Entertainment
Internet Association
Insights Association
Investment Company Institute
National Payroll Reporting Consortium
Software and Information Industry Association
TechNet

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