Date of Hearing: April 19, 2022

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Jesse Gabriel, Chair
AB 1711 (Seyarto) – As Amended March 23, 2022

SUBJECT: Privacy: breach

SUMMARY: This bill would require that, when a person or business operating a system of records on behalf of a state or local agency is required to disclose a data breach pursuant to existing law, the state or local agency also disclose the breach by conspicuously posting the notice provided by the person or business pursuant to existing law on the agency's website, if the agency maintains one, for a minimum of 30 days. Specifically, **this bill would**:

1) Require an agency, when a person or business operating a system on behalf of the agency is required to disclose a breach of that system pursuant to an existing data breach notification law (DBNL), to also disclose the breach by conspicuously posting, for a minimum of 30 days, the notice provided by the person or business pursuant to the DBNL on the agency's website, if the agency maintains one.

2) Specify that, for purposes of the bill, conspicuously posting on the agency's internet website means providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

EXISTING LAW:

1) 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, as defined, to any California resident whose unencrypted PI, or encrypted PI along with an encryption key or security credential, 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).)

2) If an agency demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the agency doesn't have sufficient contact information, permits the agency to provide substitute notice, which consists of, among other things, conspicuous posting, for a minimum of 30 days, of the notice on the agency's internet website page, if the agency maintains one; and defines conspicuous posting, for the purposes of this notice, to mean providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link. (Civ. Code Sec. 1798.29(i)(3)(B).)

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) Requires any agency, person, or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system pursuant to 1), above, to electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. (Civ. Code Secs. 1798.29(e) and 1798.82(f).)

5) Defines "agency," for the purposes of 1) - 4), above, to include a local agency; and further defines local agency, pursuant to subdivision (a) of Section 6252 of the Government Code, to include a county; city, whether general law or chartered; city and county; school district; municipal corporation; district; political subdivision; or any board, commission or agency thereof; other local public agency; or entities that are legislative bodies of a local agency, as specified. (Civ. Code Sec. 1798.29(k); Gov. Code Sec. 6252(a).)

6) Defines "breach of the security of the system," for purposes of 1) – 4), above, to mean unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the agency, and excludes from that definition the good faith acquisition of PI by an employee or agent of the agency, person, or business for the purposes of the agency, person, or business, provided that PI is not used or subject to further unauthorized disclosure. (Civ. Code Secs. 1798.29(f); 1798.82(g).)

7) Defines "PI," for purposes of 1) - 4), above, 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; health insurance information; unique biometric data generated from measurements or technical analysis of human body characteristics used to authenticate a specific individual; or information or data collected through the use or operation of an automated license plate recognition system. "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).)

8) Provides, in the Information Practices Act of 1977 (IPA), that each state 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 Sec. 1798.14.)

9) Requires each state 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 injury. (Civ. Code Sec. 1798.21.)

10) 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.)

11) Requires a business that owns, licenses, or maintains PI about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PI from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code Sec. 1798.81.5.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: This bill seeks to ensure that a California resident whose PI is compromised by a data breach of a contractor operating a system of records on behalf of an agency can adequately discern the responsible agency in order to better identify mitigating actions that can be taken in response. To accomplish this, the bill requires that, in addition to the breach notification required under existing law, the agency post the data breach notification on its agency website. This bill is author sponsored.

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

> AB 1711 seeks to provide greater transparency for Californian residents whose personal information, collected by a state agency, is compromised during a data breach. The purpose of providing a data breach notification is to allow individuals a chance to mitigate risks that stem from that data breach. However, consumers may not recognize a notification submitted by a business operating an IT system on behalf of a state agency. As a result, data breach notifications become less meaningful if the notice comes from an entity that may not be readily recognized. AB 1711 adds value to data breach notifications submitted on behalf of the agency by connecting the state agency, the entity residents can identify, to the notification. The intent is not to blame but to make the notification more meaningful without creating additional compliance obligations for business.

3) **Data breach notification laws**: Over the past decade, the frequency and variety of data breaches, which are characterized by the unauthorized acquisition of PI, have increased dramatically as computing power and the public's reliance on digital information technology grow. According to the Identity Theft Resource Center's 2021 Data Breach Report, 2021 marked the highest number of reported data breaches in a single year on record, increasing 68% over the 2020 total, and 23% over the previous all-time high set in 2017.[1] While no federal data breach laws exist, all 50 states, the District of Columbia, Guam, Puerto Rico and

[1] "2021 in review: Data Breach Annual Report" *Identity Theft Resource Center*, Jan. 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ [as of Apr. 12, 2022].

the Virgin Islands have enacted laws requiring private or governmental entities to notify individuals of security breaches involving personally identifiable information.[2]

In 2002, this Legislature passed AB 700 (Simitian, Ch. 1054, Stats. 2002) and SB 1386 (Peace, Ch. 915, Stats. 2002) which created the DBNL to require a state agency, person, or business that conducts business in California, that owns or licenses computerized data including PI, to disclose any breach of the security of that data to California residents whose unencrypted PI was, or is reasonably believed to have been, acquired by an unauthorized person. The DBNL is divided into two independent code sections within the Civil Code, one of which applies to information held by persons or businesses (i.e. private entities; Civ. Code Sec. 1798.82), and the other of which is located within the IPA and applies to information held by public agencies. (Civ. Code Sec. 1798.29.) While the IPA generally exempts local agencies from its requirements, in 2013, this Legislature passed AB 1149 (Campos, Ch. 395, Stats. 2013), which, among other things, explicitly applied the DBNL provisions of the IPA to local agencies, stating that "[n]otwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, 'agency' includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code." (Civ. Code Sec. 1798.29(k).)

Since its establishment, 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) and AB 825 (Levine, Ch. 527, Stats. 2021) added government-issued identification numbers and unique biometric data, and genetic data, respectively, to the DBNL definition of PI.

Both the public and private DBNLs provide detailed specifications concerning required notifications disclosing when an agency, person, or business that owns or licenses computerized data that includes PI has suffered a "breach of the security of the system," and define "breach of the security of the system" to mean "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency." (Civ. Code Secs. 1798.29(f) and 1798.82(g); emphasis added.) In the event of such a breach, the DBNLs require that the breach be disclosed to any resident whose PI was, or is reasonably believed to have been, acquired by an unauthorized person (Civ. Code Secs. 1798.29(a) and 1798.82(a)), and, if the agency, person, or business is required to issue a breach notification to more than 500 California residents as a result of a single breach, they must also submit a sample copy of the breach notification to the Attorney General. (Civ. Code Secs. 1798.29(e) and 1798.82(f).)

---

[2] National Conference on State Legislatures, *Security Breach Notification Laws*, Updated Jul. 17, 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, [as of Mar. 18, 2021].

This bill would further require that, if the breached entity is a person or business operating a system of records on behalf of an agency and must disclose a breach of that system under either DBNL, the agency must post the breached entity's required disclosure of the incident on the agency's website.

4) **Agencies often fail to disclose data breaches of contractors managing their information technology (IT) systems**: Recent events have brought to light the significant cybersecurity risks assumed when government agencies outsource IT services to third-party private contractors. In early 2021, a private cybersecurity company, FireEye, determined that hackers associated with Russian intelligence successfully compromised a commonly-used network management software package offered by the company SolarWinds, jeopardizing the information security of more than 250 federal agencies and businesses, including the Centers for Disease Control and Prevention, the State Department, the Justice Department, parts of the Pentagon and a number of utility companies.[3] The unprecedented scope of this cyberattack has, for many governments and businesses, prompted a re-evaluation of procedures for detecting, reporting, and mitigating compromised IT systems managed by third-parties.

   In California, PI managed on behalf of several state and local agencies has been subject to breaches through third-party contractors on several occasions. For instance, in late 2019, Automatic Funds Transfer Services, a vendor contracted to verify vehicle registration addresses behalf of the California Department of Motor Vehicles (DMV), suffered a ransomware attack that allegedly may have compromised up to 20 months of California vehicle registration records, including names, addresses, license plate numbers, and vehicle identification numbers.[4] The breach potentially compromised approximately 38 million records, according to a spokeswoman for the DMV.[5] Nonetheless, the Attorney General's public database of submitted sample data breach notifications contains no entries from the contractor or the DMV for this incident.

   In August 2021, Seneca Family of Agencies (Seneca), which contracts with 17 California counties to provide mental health, counseling, and family engagement services to county human services, health services, and probation departments, discovered a breach of their system containing records managed on behalf of those departments.[6] While Seneca subsequently issued eight data breach notifications to the Attorney General and provided notice to all clients with PI maintained on their system, the counties contracting with Seneca largely failed to provide notice, or acknowledge the breach, in a timely manner. In fact, of

---

[3] Sanger DE, Perlroth N, & Barnes JE, "As Understanding of Russian Hacking Grows, So Does Alarm," *New York Times*, Jan. 2, 2021, updated: May 28, 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html [as of Apr. 12, 2022].

[4] "Personal information of California drivers potentially compromised in ransomware attack of DMV contractor," *ABC30*, Feb. 18, 2021, https://abc30.com/dmv-personal-info-leaked-california-data-breach-leak-hack/10348979/ [as of Apr. 12, 2022].

[5] Joshua Bote, "California DMV hit by data breach, exposing millions of drivers' personal information to hackers," *SFGATE*, Feb. 18, 2021, https://www.sfgate.com/bayarea/article/California-DMV-hit-data-breach-ransomware-attack-15959944.php [as of Apr. 12, 2022].

[6] Angelica Cabral, "4,000 Monterey County residents may have been impacted by data breach," *The Californian*, https://www.thecalifornian.com/story/news/2021/11/05/4-000-monterey-county-resident-may-have-been-impacted-data-breach/6301536001/ [as of Apr. 12, 2022]; "Family services agency suffered data breach," *Sonoma Index-Tribune*, Nov. 30, 2021, https://www.sonomanews.com/article/news/family-services-agency-suffered-data-breach/ [as of Apr. 12, 2022].

the 17 counties with which Seneca contracts, only Monterey County submitted a data breach notification to the Attorney General. Notably, only some of Seneca's sample notices, which are printed on SENECA letterhead with Seneca's logo, explicitly indicate possible partnerships with other entities ("Seneca Family of Agencies ("Seneca") works with its partners, including <<Entity Name>> to provide services to families in our communities and writes to notify you of an incident that may affect the privacy of your information."), and none of the notices specify the partnering organization more than a single time or with any design element to draw attention to that detail.

In 2021, Telmate, LLC, which contracts with the Department of General Services (DGS) to operate the Inmate/Ward Telephone System on behalf of the California Department of Corrections and Rehabilitation (CDCR), submitted a sample breach notification to the Attorney General detailing a breach exposing personal information of Telmate account holders the previous year. The notification did not contain any reference to either state agency, and neither DGS nor CDCR submitted a notification.

Recognizing the importance of adequate and consistent data breach notification, Oakland Privacy, which now supports the bill (*see* Comment 6), points out:

> While some governmental data breaches are widely publicized, many are not. If an impacted person doesn't know a data breach has occurred, they are unable to take actions to protect themselves, if such actions are needed. Actions people impacted by data breaches can take include changing passwords, initiating two-step authentication, requesting a credit freeze, signing up for a monitoring service, or replacing financial cards. Certain actions may or may not be necessary for a particular data breach scenario, but impacted persons should always have the choice to be fully informed and to make the best decisions for themselves.

This bill seeks to create a mechanism to ensure that breaches of entities operating systems of records on behalf of agencies are publicized by that agency, with which the affected parties are likely to be more familiar.

5) **Protocol for reporting data breaches of persons or businesses contracting with state and local agencies is not clear under existing law**: The DBNL requires that an agency, person, or business that is breached report that breach to individuals whose PI may have been compromised, and, in specified circumstances, to the Attorney General. (Civ. Code Secs. 1798.29(a) and 1798.82(a).) The DBNL also requires that an agency, person, or business that maintains PI that the agency, person, or business does not own notify the owner or licensee of the information of any breach of the data immediately following discovery. (Civ. Code Secs. 1798.29(b) and 1798.82(b)). Accordingly, a person or business contracting with an agency for the operation of a system of records that suffers a breach potentially compromising PI would be required to report that breach to the agency. However, in those circumstances, statute does not make clear whether the contractor or the agency is responsible for notifying affected parties, and, if applicable, the Attorney General, in these circumstances.

The Statewide Information Management Manual (SIMM), which contains standards, instructions, forms, and templates that State agencies must use to comply with IT policy does provide some guidance on this situation, but that guidance is similarly opaque. In the

SIMM's "Requirements to Respond to Incidents Involving a Breach of Personal Information" (SIMM 5340-C; Feb. 2020), the Manual instructs as follows:

> *There may be some instances in which notice of a breach may appropriately come from an entity other than the actual agency that suffered the loss. For example, when the breach involves a contractor operating a system of records on behalf of the agency* or public-private partnership. The roles, responsibilities, and relationships with contractors or partners for complying with notification procedures should be established in writing with the contractor or partner prior to entering the business relationship, and must be reflected in the agency's breach response plan and in the contractual agreements with those entities.
>
> Whenever practical, to avoid creating confusion and anxiety for recipients of the notice, the notice should come from the entity that the affected individuals are more likely to perceive as the entity with which they have a relationship. *In all instances, when the breach involves a contractor or a public-private partnership operating a system on behalf of the agency, the agency is responsible for providing any required or necessary notification, and for taking appropriate corrective actions.* (SIMM 5340-C (D), p.11; emphasis added.)

This guidance seems to suggest that any contract between an agency and a contractor should explicitly specify who is responsible for disseminating notifications in what circumstances. The guidance also suggests that although in some non-mandatory circumstances it may be appropriate for the data breach notification to come from the contractor, if the notification is required by law, as would be the case for notifications pursuant to the DBNL, the notification must be provided by the agency. Still, the language arguably could more clearly delineate these circumstances, as it seems to imply that there are some circumstances in which it would be inappropriate and create confusion and anxiety for recipients for the notification to come from the agency, but that the agency must nonetheless provide it.

Further complicating this assignment of responsibility is that the SIMM does not explicitly require the compliance of local agencies, though local agencies are bound by the DBNL. Despite the explicit inclusion of local agencies in the DBNL, it is also not entirely clear how the DBNL applies to persons or businesses that contract with local agencies. Subdivision (k) of Section 1798.29 of the Civil Code, which applies the DBNL to local agencies, reads as follows:

> Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, *for purposes of this section*, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code. (Civ. Code Sec. 1798.29(k); emphasis added.)

The referenced paragraph of Section 1798.3, which the provision is notwithstanding, specifies that for the whole of the IPA (i.e. "[a]s used in this chapter"), the term "agency" shall *not* include "[a] local agency, as defined in subdivision (a) of Section 6252 of the Government Code." (Civ. Code Sec. 1798.3(b)(4).) Generally speaking, a person or business contracting with a state agency is bound by the provisions of the IPA pursuant to Section 1798.19 of the Civil Code, which specifies:

> Each agency when it provides by contract for the operation or maintenance of records containing personal information to accomplish an agency function, shall cause, consistent with its authority, the requirements of this chapter to be applied to those records. […] (Civ. Code Sec 1798.19.)

That said, because the definition of "agency" includes local agencies only for the section of the IPA that contains the DBNL, it is unclear whether this provision governing contractors applies to those who contract with local agencies. Typically, the practical effect of this possible exclusion would be inconsequential, since the DBNL that applies to persons and businesses is substantially similar to the DBNL for agencies, and would subject the contractor to virtually identical requirements regardless of whether they are considered an agency, a person, or a business. In cases like this bill that seek to amend only one of the DBNLs in a manner affecting the local agency-contractor relationship, however, it is consequently material to the necessary language which statute applies.

By requiring an agency to post the data breach notice on their website under the specified circumstances regardless of who is responsible for distributing the notice and applying the bill to persons or businesses contracting with an agency that must provide notice under *either* of the DBNLs, this bill prudently addresses these ambiguities.

6) **Notification via the agency website would improve public awareness of the incident, but may not be the most efficient means of informing affected parties**: This bill would require that when a person or business operating a system on behalf of an agency is required to disclose a breach of that system pursuant to the DBNL, the agency also disclose the breach by conspicuously posting the notice provided by the person or business pursuant to the DBNL on the agency's website, if the agency maintains one, for a minimum of 30 days. The bill would also specify that for these purposes, conspicuously posting on the agency's website means providing a link to the notice on the home page or first significant page after entering the website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

   In effect, the bill would apply one of the notification media required in the DBNL's "substitute notice" mechanism (i.e. "conspicuous posting, for a minimum of 30 days, of the notice on the agency's internet website page") to circumstances identified by SIMM 5340-C as appropriate for notice to come from an entity other than the actual agency that suffered the loss. Although the SIMM seems to suggest that the agency is responsible for distributing notice in the mandatory circumstances contemplated by this bill, that requirement is not included in statute, and in practice, it appears that data breach notifications tend to be provided by the contractor rather than the responsible agency. By maintaining existing requirements while additionally requiring the publication of the notice on the agency's website (i.e. "the agency shall *also* disclose the breach by conspicuously posting […]"), the bill would provide an opportunity for those potentially affected by the breach to encounter the notice through a medium with which they are likely more familiar (i.e. the agency with which they have shared their information) in addition to the notice that may be sent by the contractor with whom they are not familiar. Compliance with the requirement of this bill does not seem particularly onerous for the agency, and it would expand awareness of data breaches beyond existing law.

That said, if the author's intent is to ensure that those potentially affected by data breaches of government contractors receive notice that is meaningful and actionable, rather than from a contractor with whom they are not even aware how they've shared information, there may be more effective mechanisms to accomplish this end. While some PI is provided to government agencies in transactions for public services that recur regularly, providing an opportunity to view a notice on the website, this is the case in only a small set of circumstances. In an opposition[*] letter submitted by Oakland Privacy based on a previous version of the bill, Oakland Privacy points out some of the inefficiencies associated with the bill's approach:

> While certainly representing a reduction in administrative burden, we are confident that governmental agency websites receive a limited amount of recreational browsing activity and that such notices are guaranteed not to reach each and every impacted person. […] It is also important to state that impacted persons may or may not have consistent or robust Internet access, and for those without, an Internet website disclosure is tantamount to no disclosure at all. They will never see it, unlike a notice mailed to them.

Indeed, it is not clear how much exposure to the general public a post on an agency website will receive. Rather, the objective of clarifying the responsible agency when a contractor is breached could arguably be more effectively achieved through other means, such as specifying in statute that the notice must come from the agency or that if the notice comes from the contractor, it must conspicuously include the agency on behalf of which the contractor is operating the system. As the Association of School Administrators, which opposes the bill unless amended, argues:

> We believe the proposed online posting requirements could create further confusion and alarm rather than provide helpful information. Parties whose data was not affected could flood the school district with inquiries to determine if their data was exposed. We also generally oppose prescriptive requirements for mandatory information to be placed on website home pages or first landing pages, since it can make them more difficult to navigate as each new required piece of information is added.
>
> [W]e request that AB 1711 be amended to remove the online posting requirement for the agency and instead, add to the required information that is to be provided directly to the impacted individuals. Specifically, the vendor's notice to impacted parties shall include the name of the public agency in association with the data breach, where applicable. This would allow additional information to be shared through an established, existing workstream. The modified approach speaks to the intent of AB 1711 with greater precision and reduced demands on school resources.

---

[*] Oakland Privacy initially adopted an "oppose unless amended" position on this bill due to a lack of clarity in the language of a previous version that could have been read to supplant existing data breach notification mechanisms with posting on the agency's website. The author has since amended the bill to clarify the intent, i.e. that the posting of the notice is *in addition to* rather than *in place of* existing notification requirements, by specifying that the agency "shall *also* disclose the breach by conspicuously posting" the notice. In response to this amendment, Oakland Privacy has switched to a "support" position for the bill in print.

Nonetheless, there is arguably little harm in requiring an additional mechanism of notice beyond existing practice, and posting on the website does have the potential to reach and inform some otherwise confused or uninformed individuals. Though cluttering website landing pages can present problems for accessibility of other services provided on those websites, the a significant impact of the required posting on website operations seems unlikely, since it is only required to be posted for a limited period of time and consists of only a conspicuous link to the notice, rather than the particular details of the breach. Accordingly, the bill seems to improve the status quo with respect to data breach notifications provided in the event a person or business operating a system of records on behalf of an agency is breached.

7) **Author's amendment**: The DBNL specifies that its required disclosures "shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided [], or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." (Civ. Code Secs. 1798.29(a) and 1798.82(a).) This provision defines a fairly vague timeline for disclosure, but allows for circumstantial assessment of timing in order to prevent the possibility of the disclosure interfering with a legal investigation of the incident or the disclosure introducing additional vulnerability to an affected system that has yet to be fully secured. The SIMM provides some additional guidance on how to comply with this provision, adding:

> To the extent possible, notification should be made within ten (10) business days from the date the agency has determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person. The following are examples which may warrant the delay of notification beyond the 10 days following discovery:
>
> - Legitimate needs of law enforcement, when notification would impede or compromise a criminal investigation, or pose other security concerns [Civil Code Section 1798.29 (c)].
>
> - Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system, so the harm of the initial incident is not compounded by premature announcement. For example, if a data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident. [Civil Code Section 1798.29 (a).].
>
> Any decision to delay notification should be made by the agency head, or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf, and any delay should not exacerbate the risk of harm to any affected individual(s). (SIMM 5340-C (C); p. 10.)

In a letter expressing concern with the bill, the California Special Districts Association argues that posting the notice on the agency website too hastily could endanger the cybersecurity of the agency, writing:

> [W]e believe that AB 1711 may have the opposite of its intended effect by increasing security risks. Requiring that a link to the vendor's or contractor's notice be posted on

the public agency's website in all instances may increase the opportunities for bad actors to become aware of and to attempt to exploit the vulnerability.

While this bill specifies "*When* a person or business operating a system on behalf of an agency is required to disclose a preach of that system […]," it is not entirely clear whether this implies that the same timeline for disclosure, which contemplates this scenario, is applicable. Without additional clarity, this ambiguity could arguably risk a notice posted on a website interfering with an investigation or further exposing a vulnerable system. To avoid this possible risk, the author has agreed to amend the bill to include the same timing provision within the text of the bill's provision.

Author's amendment:

On page 2, line 31, before the word "For" insert: "***The disclosure shall be posted in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.***"

8) **Related legislation**: AB 2135 (Irwin) would require 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 would require those agencies to perform a comprehensive independent security assessment (ISA) every two years for which they may contract with the Military Department or a qualified responsible vendor.

AB 2190 (Irwin) would enact a recommendation from the State Auditor's 2022 report (*see* Comment 7) to require that the Department of Technology (CDT) confidentially submit an annual statewide information security status report, including specified information, to the Chair of the Assembly Committee on Privacy & Consumer Protection no later than January 2023.

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 2677 (Gabriel) would amend several provisions of the IPA to, among other things, expand and modernize definitions of "personal information" and "record"; require agencies to provide notice of purposes for which PI will be used and prohibit agencies from using PI for any other purpose, except as specified; specify that negligent violations by agency employees constitute a cause for discipline; specify that intentional violations disclosing certain sensitive information are punishable by a misdemeanor whether or not the disclosure results in injury; and apply the IPA to PI collected, stored, and shared by local agencies.

Prior legislation: AB 825 (Levine, Ch. 527, Stats. 2021) *See* Comment 3.

AB 1130 (Levine, Ch. 750, Stats. 2019) *See* Comment 3

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.

AB 700 (Simitian, Ch. 1054, Stats. 2002) *See* Comment 3.

SB 1386 (Peace, Ch. 915, Stats. 2002) *See* Comment 3.

REGISTERED SUPPORT / OPPOSITION:

Support

Oakland Privacy

Opposition

Association of California School Administrators (unless amended)

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