CONCURRENCE IN SENATE AMENDMENTS
AB 1711 (Seyarto)
As Amended August 8, 2022
Majority vote

SUMMARY

This bill requires 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.

Senate Amendments
Provide chaptering-out amendments to take effect in the event that both this bill and AB 2958 (Judiciary Committee) of the current legislative session are enacted.

COMMENTS

In 2002, this Legislature passed AB 700 (Simitian), Chapter 1054, Statutes of 2002, and SB 1386 (Peace), Chapter 915, Statutes of 2002, which created the data breach notification law (DBNL) to require a state agency, person, or business that conducts business in California, that owns or licenses computerized data including personal information (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; Civil Code Section (CC) 1798.82), and the other of which is located within the Information Practices Act (IPA) and applies to information held by public agencies. (CC 1798.29.) While the IPA generally exempts local agencies from its requirements, in 2013, this Legislature passed AB 1149 (Campos), Chapter 395, Statutes of 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." (CC 1798.29(k).)

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." (CC 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 (CC 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. (CC 1798.29(e) and 1798.82(f).)

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. (CC 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.

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. It is thus 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.

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.

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.

Arguments in Support

Oakland Privacy argues:

> 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 includes 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 decisions for themselves. […] After a brief consultation with the author's office regarding the intent of the bill, we recognize that the bill is not intended to reduce any obligations on the part of a business contractor to send individualized notices, but simply adds a requirement for the relevant state agency to post a web notification . We have no objection to that proposal and would express support for it.

Arguments in Opposition
The California Association of School Business Officials (CASBO), the California Special Districts Association, and the Association of School Administrators, who oppose the bill unless amended, argue:

> We believe the proposed online posting requirements could create further confusion and alarm rather than provide helpful information**,** at the expense of staff time and resources. Parties whose data was not affected could flood the school district with inquiries to determine if their data was exposed. Schools, local government, and other public agencies already place a significant amount of information on their homepages, which is critical to their operations and allows services to be provided in a timely and efficient manner. Adding further required website content, particularly on homepages or first significant webpages, may distract from the core service functions of public agencies. It may also underplay other critical information shared. AB 1711's prescriptive language and lack of flexibility as to what constitutes conspicuously posting a link to a notice may also raise potential website accessibility concerns now or in the future. Requiring that a link to the vendor's or contractor's notice be posted on the public agency's website may also alert bad actors to system vulnerabilities and the opportunity to exploit them.

FISCAL COMMENTS

According to the Assembly Appropriations Committee, "[l]ikely minor and absorbable costs to a public agency to post a security breach notification on its website when a business operating a data system on behalf of a public agency suffers a data breach."

VOTES:

ASM PRIVACY AND CONSUMER PROTECTION: 10-0-1
YES: Gabriel, Kiley, Bauer-Kahan, Bennett, Berman, Cunningham, Mike Fong, Irwin, Valladares, Wilson
ABS, ABST OR NV: Wicks

ASM APPROPRIATIONS: 14-0-2
YES: Holden, Bigelow, Bryan, Calderon, Carrillo, Megan Dahle, Davies, Mike Fong, Seyarto, Levine, Quirk, Robert Rivas, Akilah Weber, Wilson
ABS, ABST OR NV: Gabriel, Eduardo Garcia

ASSEMBLY FLOOR: 65-0-13
YES: Aguiar-Curry, Arambula, Bauer-Kahan, Bennett, Berman, Bigelow, Bloom, Mia Bonta, Calderon, Carrillo, Cervantes, Chen, Choi, Cooley, Cooper, Megan Dahle, Daly, Flora, Mike Fong, Fong, Friedman, Gabriel, Gallagher, Cristina Garcia, Eduardo Garcia, Gipson, Haney, Holden, Irwin, Jones-Sawyer, Kalra, Levine, Low, Maienschein, Mathis, Mayes, McCarty, Medina, Mullin, Muratsuchi, Nazarian, Nguyen, O'Donnell, Patterson, Petrie-Norris, Quirk, Ramos, Reyes, Luz Rivas, Robert Rivas, Rodriguez, Salas, Santiago, Seyarto, Smith, Stone, Ting, Villapudua, Voepel, Waldron, Akilah Weber, Wicks, Wilson, Wood, Rendon
ABS, ABST OR NV: Boerner Horvath, Bryan, Cunningham, Davies, Gray, Grayson, Kiley, Lackey, Lee, Quirk-Silva, Blanca Rubio, Valladares, Ward

SENATE FLOOR: 26-2-12
YES: Archuleta, Atkins, Bates, Becker, Borgeas, Bradford, Cortese, Dahle, Dodd, Grove, Hertzberg, Hueso, Hurtado, Jones, Leyva, McGuire, Melendez, Min, Newman, Ochoa Bogh, Portantino, Roth, Rubio, Umberg, Wiener, Wilk
NO: Durazo, Nielsen
ABS, ABST OR NV: Allen, Caballero, Eggman, Glazer, Gonzalez, Kamlager, Laird, Limón, Pan, Skinner, Stern, Wieckowski

UPDATED

VERSION: August 8, 2022

CONSULTANT: Landon Klein / P. & C.P. / (916) 319-2200 FN: 0004044