A Potential Trend in the Making? Utah Becomes the Second State to Enact Data Breach Safe Harbor Law Incentivizing Companies to Maintain Robust Data Protection Programs

David J. Oberly
Blank Rome LLP

***David J. Oberly** is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Cybersecurity & Data Privacy, Biometric Privacy, and Privacy Class Action Defense groups. David's practice encompasses both counseling and advising clients on a wide range of privacy, biometric privacy, and data protection/cybersecurity matters, as well as defending clients in high-stakes, high-exposure privacy, biometric privacy, and data breach class action litigation. He can be reached at doberly@blankrome.com.*

Today, the question is no longer a matter of "if," but "*when*," a company will fall victim to a successful security incident. Over the years, lawmakers have struggled with devising effective methods and incentives for companies to enhance their data protection programs without mandating one-size-fits-all requirements that undercut effective data security management.

Earlier this year, Utah enacted a new data security statute—the Utah Cybersecurity Affirmative Defense Act ("CADA")—which accomplishes just that goal. With the CADA—the second law of its kind to be enacted in the United States—Utah businesses are now afforded a safe harbor against certain causes of action that commonly arise in data breach class action litigation where the entity maintains reasonable data protection measures to safeguard sensitive personal information at the time of the incident. From a broader perspective, the passage of the CADA may influence other states to follow Utah's lead and enact similar laws of their own.

Utah's Cybersecurity Affirmative Defense Act

To incentivize companies to adopt appropriate data protection safeguards, Utah enacted the CADA, which offers companies sizeable benefits in return for maintaining data protection and security practices. Specifically, the CADA provides companies that meet the law's written cybersecurity program requirements with an affirmative defense to claims that are brought under the laws of Utah or in Utah courts alleging a failure to: (1) implement reasonable security controls that resulted in a security incident; (2) appropriately respond to a security incident; or (3) appropriately notify individuals whose personal information was compromised in a security incident.

In order to qualify for the affirmative defense safe harbor, a company must implement a written cybersecurity program that "reasonably conforms" to one of several recognized cybersecurity frameworks, including any of the following: (1) NIST Special Publication 800-171; (2) NIST Special Publications 800-53 and 800-53a; (3) the Federal Risk and Authorization Management Program Security Assessment Framework; (4) the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or (5) the International Organization for Standardization/International Electrotechnical Commission 27000 Family – Information Security Management Systems.

Read more on page 42

A Potential... Continued from page 12

Alternatively, companies can satisfy this requirement by implementing a "reasonable security program," which is defined under the CADA as a program that, among other things: (1) designates an employee to oversee and facilitate the program; (2) utilizes practices and procedures to detect, prevent, and respond to security incidents; (3) provides training to employees on the company's data security practices; and (4) utilizes risk assessments to test and monitor its data security practices.

At the same time, companies that are subject to certain state or federally mandated sector-specific laws, such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or the Gramm-Leach-Bliley Act of 1999 ("GLBA"), may satisfy this requirement and rely on the affirmative defense if their cybersecurity program complies with the security requirements of those laws.

In addition, a company's cybersecurity program must be of an appropriate scale and scope in light of the following factors: (1) the size and complexity of the company; (2) the nature and scope of its activities; (3) the sensitivity of the information at issue; (4) the cost and availability of tools to enhance data security and reduce vulnerabilities; and (5) the resources available to the company.

Importantly, however, a company is *precluded* from claiming the affirmative defense if: (1) it had actual notice of a threat to the security of personal information; (2) did not act in a reasonable amount of time to remediate and neutralize the threat; and (3) the threat resulted in a security incident.

Takeaways

With the CADA, Utah becomes the second state to put in place legislation incentivizing businesses to implement certain privacy and data protection controls through the utilization of an affirmative defense to certain data breach causes of action. In 2018, Ohio became the first state to do so with its enactment of the Ohio Data Protection Act, which also uses an affirmative defense model with requirements that closely parallel those seen in its Utah counterpart.

While Utah is the second state to enact a data breach affirmative defense statute, it will almost certainly not be the last. Utah's new data protection law represents a potential trend evolving among state legislatures that are currently looking for ways to tighten up organization privacy and data protection practices. In fact, Connecticut has a copycat data breach safe harbor bill of its own—"An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses" (HB 6607)—currently pending at this time.

The CADA is a welcome opening for Utah companies seeking to limit their liability in the face of an ever-growing threat of security incidents, as the law provides clear steps that companies can take to qualify for the statute's safe harbor.

With that said, companies must keep in mind that qualifying for this new defense to liability is not automatic. Rather, a company will bear the burden of establishing both that its program satisfies all of the criteria to fall under the safe harbor *and* that the company was adhering to its program at the time a security event took place. At the same time, the CADA will only insulate breach victims from some—but not all—types of claims asserted in the wake of a security incident.

As such, with the limited scope of the safe harbor and corresponding challenges that companies will face in establishing their eligibility for the affirmative defense, companies must still focus their efforts on ensuring that the risk of security breaches is minimized to the greatest possible extent, as entities will still face potentially substantial liability exposure in the event of a breach, even if they are able to leverage the CADA's affirmative defense in litigation.

Conclusion

As the number and severity of breach events continues to climb today with no foreseeable end in sight, now more than ever companies must be proactive in implementing effective safeguards to shield sensitive personal information from unauthorized access, disclosure, or acquisition. At the same time, companies must ensure that their cybersecurity programs comport with the requirements of the CADA and similar safe harbor affirmative defense laws, as doing so will allow them to defeat certain claims asserted in data breach class action litigation in the event the company falls victim to security incident.

Through the implementation of a robust privacy and data protection risk management program, companies can effectively minimize the risk of falling victim to a catastrophic data breach, while at the same time putting themselves in the best position to assert the CADA's safe harbor if they find themselves on the receiving end of a class action lawsuit stemming from the compromise of sensitive personal information.

David J. Oberly is an attorney in the Cincinnati office of Blank Rome LLP and is a member of the firm's Biometric Privacy, Privacy Class Action Defense, and Privacy & Data Protection groups. David's practice encompasses both defending clients in high-stakes, high-exposure biometric privacy, privacy, and data breach class action litigation, as well as counseling and advising clients on a wide range of biometric privacy, privacy, and data protection/cybersecurity matters.

Kamala... Continued from page 13

solely on prosecuting violators of California and federal privacy laws.[3] Another notable achievement was her successful expansion of the 2002 California Online Privacy Protection Act (CalOPPA) to include mobile applications. CalOPPA requires website operators and online services to "conspicuously post" their privacy policies. In a 2012 agreement that Harris negotiated directly with major tech companies, including Apple, Amazon, Microsoft, Google, and Facebook, they agreed to abide by the terms of CalOPPA by posting the privacy policies of every mobile application offered on their respective platforms.[4]

If Vice President Harris were to play a role in developing federal privacy policy, some insight into her positions, particularly on the issue of a federal privacy law, may be found in a 2016 report produced by her office, called simply the *California Data Breach Report*. As its title suggests, the Report's primary focus is on data breaches; it provided an analysis of all known data breaches effecting Californians from 2012 to 2015, along with recommendations for combating data breaches and mitigating their harm. However, the Report also contained discussion of the problems posed by a system in which privacy laws varied from state to state, as well as issues raised by a potential federal privacy law, particularly as they pertained to California's laws and concomitant privacy rights.

Although the Report addressed these issues through the lens of data breach notification laws, the same reasoning is applicable to privacy laws in general. In the Report, Harris argues that the calls for uniform federal privacy legislation were the result of the "proliferation" of state data breach notification laws, which differed from one another on such basic issues as what constituted a "minimum standard of care."[5]

While acknowledging the benefits of a single, national privacy standard, the Report expressed the concern noted above, that federal legislation was likely to leave Californians with *fewer* privacy protections. Moreover, residents of other states would also be negatively affected because, the Report asserted, when organizations respond to large-scale data breaches that impact multiple states, they tend to follow the "highest-common-denominator approach," thus effectively providing "California-level protections to residents of all states."[6]

Instead of a federal privacy law, Harris advocated increased cooperation between policymakers of the various states to attempt to reduce the differences between their respective state privacy laws.[7] She also noted the usefulness of federal regulatory guidelines issued by agencies such as the Federal Trade Commission (FTC).[8]

The importance of such guidance is exemplified by the fact that the Data Breach Report was itself used for guidance in implementing no less a law than the CCPA.

Among the CCPA's requirements are that organizations implement "reasonable security" measures and procedures to protect private information. However neither the text of the 2018 statute, the version as amended by the 2020 CPRA, nor the guidelines issued by the California Attorney General in 2021, contain a definition of this vital term. As a consequence, many organizations turned to the most recent guidance available on the matter, namely the 2016 Data Breach Report. For its definition, the Report pointed to a set of twenty "Critical Security Controls" developed by the Center for Internet Security (CIS)[9], a non-profit organization that promotes best practices for cyber-security readiness and response. The CIS Critical Security Controls included recommendations on protecting email and web-browsing systems, defending against malware attacks, proper authentication procedures, as well as incident response and data recovery. The Report stated that to meet the "reasonable security" standard, an organization must implement all twenty of the Security Controls.[10] Consequently, when it came time for organizations to update their security protocols to come into compliance with the CCPA, they took their cue from the Report, and began to implement the twenty Security Controls.

The continued absence of a federal privacy law magnifies the importance of federal guidance, particularly by the agency most often involved in privacy matters, the FTC. Interestingly, Harris' connection to the FTC dates back to her college years, when she interned at the agency college years, while attending Howard University.[11]

As an agency of the executive branch, the FTC will promote the policies of the Biden-Harris administration. In its appointment of Lina Khan, a prominent critic of Big Tech, as Chairman of the FTC in June 2021,[12] the administration has signaled that its policies include an effort to reign in Big Tech. This policy will substantially impact on privacy issues as, with the possible exception of the government, the major tech companies are the largest collectors and disseminators of protected personal information.

Khan's appointment also increases the likelihood that the agency will issue new guidance in many areas, perhaps including privacy. This inference is based on an FTC Comment that Khan assisted in drafting while an aide to former Commissioner Rohit Chopra, which stressed that the primary purpose for the creation of the FTC was to provide guidance, including through its rule-making powers.[13]

Just as the 2016 Report influenced the interpretation of the CCPA, FTC guidance would influence state laws. Efforts to comply with FTC guidelines, particularly if they came in the form of rules, could spur states to develop stronger privacy laws, or at least impact the interpretations of their existing laws. Since the states would

be following the same set of privacy guidelines, their new laws and interpretations would establish a greater degree of consistency in the privacy rights and protections afforded by each state, thus creating a de facto national standard, without the need for federal legislation. Such an outcome would be in keeping with the position Vice President Harris advocated in her 2016 Report, all the more so if the use of a de facto national standard eventually enabled residents of all states to enjoy "California-level" privacy rights.

Endnotes

1 Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision, U.S. Dept. of Commerce (July 16, 2020), https://www.commerce.gov/about/letter-deputy-assistant-secretary-james-sullivan-schrems-ii-decision.

2 At the time of this writing, there are 220 Democrats in the House of Representatives, 42 of whom represent California districts. https://pressgallery.house.gov/member-data/party-breakdown

3 Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit, Office of the Attorney General (July 19, 2012), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-creation-ecrime-unit-targeting.

4 Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, Office of the Attorney General (Feb. 22, 2012), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy. Facebook signed on to the agreement in June 2012, four months after the other companies.

5 Kamala D. Harris, *California Data Breach Report*, Office of the Attorney General (Feb. 2016), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf, p. 38.

6 Id., p. 5.

7 Id., p. 38.

8 Id., p. 28.

9 The CIS Critical Security Controls for Effective Cyber Defense, Version 6.0, The Center for Internet Security (Oct. 15, 2015), https://www.uio.no/studier/emner/matnat/ifi/INF3510/v16/docs/csc-6.pdf. The CIS periodically updates its Critical Security Controls; the most recent version, Version 8.0, was released in May 2021.

10 Harris, p. 30.

11 Mike Swift, Claude Marx and Max Fillion, "VP Pick Harris has Long Regulatory History with Big Tech on Privacy," *MLex: FTC Watch*, (Aug. 24, 2020), https://www.mlexwatch.com/articles/9021/print?section=ftcwatch.

12 David McCabe and Cecilia Kang, "Biden Names Lina Khan, a Big-Tech Critic, as F.T.C. Chair," *The New York Times* (June 15, 2021), https://www.nytimes.com/2021/06/15/technology/lina-khan-ftc.html.

13 Comment of Federal Trade Commissioner Rohit Chopra, Hearing #1 on Competition and Consumer Protection in the 21st Century (Sept. 6, 2018), https://www.ftc.gov/system/files/documents/public_statements/1408196/chopra_-_comment_to_hearing_1_9-6-18.pdf.