January 19, 2017

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.com
An ALM Publication

What to Expect in California Data Security and Privacy in 2017

By Natasha Kohne and Crystal Roberts

Natasha Kohne and Crystal Roberts of Akin Gump Strauss Hauer & Feld

With 2017 underway and the entrance of a new Republican administration and Congress, whether robust regulatory oversight will remain a federal priority is more than uncertain and the area of data privacy and security is no different. The data privacy and security action, however, may continue at the state level where already-active state legislatures and regulators see these areas as a focus. Reviewing recent developments in California over the past year may shed light on key issues and trends that we can expect to see in the coming months.

California has, in many respects, led state efforts nationwide to protect privacy and data security. In 2003, California became the first state in the nation to impose data breach notifications, at the time requiring California businesses "that own[] or license[] computerized data" to notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person (Cal. Civ. Code section 1798.82). California has continued to trailblaze in the privacy and data security arena, enacting a number of privacy and data security requirements since.

As the primary regulator of these requirements, the California attorney general has brought numerous investigations and enforcement actions involving data privacy and security. However, despite its historical leadership in this space, approximately three years have passed since the California Attorney General's Office announced its last data breach-related settlement. Since then, the attorney general has engaged in other investigations, but has not formally announced any data security enforcement actions.

The lack of recent settlements in data security enforcement has not prevented the attorney general from continuing to announce "recommendations," issue formal guidance for businesses in various industries, and institute cybersecurity initiatives, signaling a continued focus on enhancing data security and privacy for California businesses and residents. The California legislature has also made efforts to amend data security laws, and with cybersecurity continuing to be a major threat, we will likely see further developments in 2017.

California Attorney General Activities and Initiatives

One major 2016 development included California's attempt to define the elusive "reasonableness

standard." By way of background, California, like many other states, requires that businesses "maintain reasonable security procedures and practices" to protect their customers' "personal information." (See Cal. Civ. Code section 1798.81.5.) But the technologically-neutral term "reasonable security," meant to reflect the "reasonableness" standard of tort law, is not defined.

With the release of its 2016 Data Breach Report in February 2016, the Attorney General's Office identified a list of safeguards that it views as constituting a reasonable level of information security. While this report is not a law or regulation, the report is an effort to regulate data security of businesses operating in California and demonstrates the attorney general's expectations. Indeed, the report stated that the 20 Critical Security Controls defined by the Center for Internet Security constitute "a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all controls that apply to an organization's environment constitutes a lack of reasonable security."

Evidencing further prioritization of data privacy and security, in October 2016, the attorney general released an online tool for reporting violations of the California Online Protection Practices Act (CalOPPA). CalOPPA, enacted over a decade ago, requires operators of commercial websites and online services that collect personally identifiable information about California residents to conspicuously post a privacy policy on its website and to comply with the terms of the policy.

The attorney general's new online tool consists of a CalOPPA Complaint Form and allows consumers to report any allegations of noncompliance in the following areas: privacy policy missing or inapplicable; privacy policy difficult to locate; privacy policy incomplete; privacy policy violated; failure to provide notice of a material change. The attorney general has claimed that this tool "exponentially increase[es] the California Department of Justice's ability to identify and notify those in violation of CalOPPA." The attorney general is also partnering with the Usable Privacy Policy Project at Carnegie Mellon University to develop a tool that will identify mobile apps that may be in violation of CalOPPA.

The following month, the attorney general released guidance for the education technology industry: "Ready For School: Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data." In her introduction, Attorney General Kamala Harris states that "organizations that make use of student data must take every step possible to be transparent with parents and schools and to protect student privacy." The guidance provides recommendations including minimizing data collection and retention, using information only for educational purposes, and vendor management, among other recommendations. Harris also refers to the 2016 Data Breach Report for a "good starting point for high-priority security controls."

Other State Measures

The state legislature also took efforts in 2016 to enhance data privacy and security requirements by attempting to expand the scope of what constitutes "personal information" under Section 1798.81.5 of the California Civil Code, to add biometric and geolocation data to the definition of personal information. However, the bill (AB 83) failed to pass the Senate Judiciary Committee. California did, however, amend its data breach notification law, which until now had required notification of a breach when unencrypted personal information was comprised. As of Jan. 1, the amended law refined this specific notification requirement by requiring notification when (a) an unauthorized acquisition of both encrypted personal information and the encryption key or security credential occurs, and (b) the business has a reasonable belief that the encryption key or security credential could render such personal information readable or useable.

At least two additional privacy-related bills are pending this year regarding the use of surveillance technology by law enforcement agencies (SB 21) and the disclosure of religious affiliation information to the federal government (SB 31).

Companies that do business in California, or otherwise collect information about California residents, should take heed of the latest guidance, recommendations, and legislative initiatives, as business requirements, expectations of regulators and investigations are likely to increase in 2017.

Natasha Kohne *is a partner in the San Francisco and Abu Dhabi offices of Akin Gump Strauss Hauer & Feld and co-head of its cybersecurity, privacy and data protection practice.* ***Crystal Roberts*** *is a staff attorney in the firm's San Francisco office.*