Corporate Counsel Business Journal
Online
CCBJournal.com

CCBJ

New Data Privacy and Security Laws Put U.S. Companies On the Defensive

▶Michelle Reed and Natasha Kohne, co-leaders of Akin Gump's Cybersecurity, Privacy and Data Protection practice, discuss the effects of new data regulations in California and other states, and what companies can do to protect themselves.

CCBJ: There has been a lot of activity in the cybersecurity and data privacy spacelately. What general trends and issues are you seeing in your practice?

Michelle Reed: Many of the issues we're seeing on the cybersecurity front involve various kinds of fraud: business email compromise scams, wire transfer fraud, cyber breaches that involved some sort of intellectual property–gathering efforts. It's very common to see breaches in the payment card industry, both e-commerce and retail-facing. But some of the most significant activity is actually more complex than Social Security numbers or credit card numbers being stolen – it involves other confidential data and the data integrity itself. There are always new and creative attempts by criminals to exploit defenses and breach companies.

On the privacy side, it is an entirely new world. We saw the transformation the EU first, with the General Data Protection Regulation (GDPR), and now we're seeing it in the United States as well, with the advent of the California Consumer Privacy Act (CCPA). Many other states are creating legislation similar to the CCPA, and privacy has become a major discussion point in most boardrooms. There are new data disclosure requirements, limitations on how you can sell data, requirements on contractual arrangements for vendors in order to share data. And there are rules making sure that individuals have the access to their data, as well as about the portability of their data and the right to have their data deleted. These are new rights that didn't previously exist in the United States. That means that in some case our clients are having to change the way they do business. Until now, in the United States, data has been a commodity that was used and exchanged at no price, because there was no comprehensive privacy regime in the United States. With the introduction of the CCPA, and with similar legislation pending in other states, companies are having to conduct new analyses.

Natasha Kohne: We are definitely seeing more prescriptive cybersecurity requirements. For example, regulators are emphasizing that companies must implement specific measures such as privacy by design, as well as identify the employees within their organizations who are in charge of security and privacy, and update information security plans when there is a change in circumstances. These points were always best practices, but they were not necessarily spelled out in most U.S. statutes, and now the clear trend is that laws are becoming more specific. You can see this, for example, in the New York SHIELD Act that was passed in July and the NYDFS Cybersecurity Regulation. Simultaneously, we have seen a proliferation of privacy statutes being passed or proposed that emphasize rules and controls around the collection, use and disclosure of personal information. You see the impact on our federal government, which is trying to grapple with this growing trend and the threat of more U.S. states coming out with their own sets of privacy rules. We are tracking at least 17 states with privacy statute activity, and we expect a number of other states to release proposed privacy bills again in 2020.

What recent developments should our readers be aware of within the regulatory landscape?

Reed: From a basic standpoint, regulators are becoming more active in making sure that privacy and security are

in play, and that people are notified about what companies are doing with their data. If you dig down into the separate industries, you see that they're becoming more prescriptive in their approach. For example, on the government contract side, the Department of Defense (DOD) is now planning to require its contractors and subcontractors to obtain third-party audits, assessments, and certifications about their cybersecurity capabilities and controls. They're calling this new approach the Cybersecurity Maturity Model Certification. The DOD has always been on the forefront of making sure that people are using secure systems when they're dealing with defense-type secrets, but they're becoming more prescriptive about it now by requiring this analysis and audit to be done through third parties.

On the healthcare side, you see a lot more activity in terms of enforcement actions, and for higher settlement amounts. Obviously HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act) have been in place and have been enforced for a long time, but what you see now are increasing penalties associated with these laws. In financial services, there is more regulation as well, in response to the proliferation of wire transfer fraud and banking fraud. The regulations themselves have not significantly changed, but you see a lot more cooperation with regulators in terms of trying to track down criminals and protect companies that are suffering from these risks.

Michelle Reed is a partner with Akin Gump Strauss Hauer & Feld LLP. She is the co-leader of the firm's cybersecurity, privacy and data protection practice. Reed represents clients in a variety of complex civil litigation matters, including securities class actions, derivative suits and consumer class actions. Reach her at mreed@akingump.com.

Kohne: Michelle mentioned the CCPA, and that's really the biggest change, in my opinion. California is the fifth-largest economy in the world, so this law impacts nearly all businesses, and it has extraterritorial reach as well. Businesses have to assess risk not only from a privacy perspective but also from a cyber perspective. For example, the CCPA maintains a private right of action that allows certain individuals to sue businesses when their personal information is compromised due to a business's failure to maintain reasonable security. We could see a sea change in data breach legal activity as a result of this private right of action. Also, because the CCPA is so different from the GDPR, many businesses have had to rethink critical issues around vendor contracting, practices of sharing of personal information, verification of consumer requests for California residents, and even some rewards programs. Then most recently, it appears that an entirely new set of proposed rules, the CCPA 2.0, has been released and may go to the California ballot for voters to vote on in 2020. We are seeing this shifting landscape continue well into the future.

How do you expect the SHIELD Act, CCPA, and other new or developing U.S. regulations to be enforced?

Reed: Let me start with the SHIELD Act, which applies to New York businesses, and businesses dealing with New York data. One key aspect of it is the notification component, and the other is the reasonable security component. There are a lot of outs in the sense that if you are regulated by another statutory or regulatory regime, and you're compliant with it, SHIELD is not as applicable. But with respect to the notice requirements,

there's no federal notification standard that's generalized across industries, so most companies will end up being subject to the New York notification requirements. And the New York notification requirement has some interesting new elements – in particular the access-only standard, which means it doesn't require that data actually be taken from a system in order for there to be a notification of a breach. Notification is required even on an access-only basis, if personal information as defined by the statute is impacted. That is a game changer, because there are a lot of breaches, particularly in the context of wire fraud or ransomware, where you didn't previously have notification obligations because nothing was actually taken – but now, depending what the actual breach situation is, what was accessed, companies may have to provide notice. I think you will see enforcement actions there, in the event that companies aren't properly notifying or applying that standard.

About CCPA: Enforcement doesn't go into place until six months after the regulators come out with the regulatory framework, which should be around July 1, 2020. But once it starts, we anticipate that you will see enforcement, and that regulators are going to be very specific about the cases they take. They're going to be looking for clear violations, cases that they can win, to show that the CCPA has teeth. The attorney general is empowered to seek penalties of up to $2,500 for general violations and $7,500 for intentional violations. On top of that, the consumers themselves have a right to enforce the act, and the CCPA creates a new private right of action for consumers that permits cases against businesses who fail to provide reasonable data security.

Kohne: I expect enforcement for SHIELD and CCPA and other privacy statutes that are passed in the U.S. to be consistent but not overly robust. The attorney general's office in California, for example, has already publicly noted that it has limited resources to enforce the CCPA. Even though it has reportedly expanded the number of staff in its privacy office, they still do not necessarily have the bandwidth to bring dozens of privacy cases per year. This is one of the purported reasons that California's attorney general sponsored an amendment to the CCPA to expand the privacy right of action beyond the data breach context. He did not believe that his office could take on sole enforcement responsibilities of these CCPA violations.

How are you advising clients on multistate or global breach issues and potential litigation, and how is class-action litigation playing out?

Reed: Multistate and international breaches are complex and require a legal team that is very familiar with the company and with cybersecurity laws. It's crucial to understand whether the data that was impacted actually rises to the level of notification – and if it does, what notification is required and how it's rolled out. Then, of course, dealing with the ensuing litigation is important. There's been an uptick in litigation in this space, as the courts are finding standing where they didn't find it before.

Natasha Kohne is a partner with Akin Gump Strauss Hauer & Feld LLP. She is a co-leader of the firm's cybersecurity, privacy and data protection practice. Kohn advises on privacy-and security-related compliance investigations and enforcement actions. She represents companies cross-corder litigations, arbitration and investigations. Reach her at nkohne@akingump.com.

Kohne: We treat every breach as though it is going to litigation. In reality, only

a small percentage of publicly reported breaches result in class-action litigation in the U.S. This may change with the CCPA and the private right of action it grants consumers, so we do expect many more data breach litigations to be filed when that happens. Smaller companies may be targets for lawsuits more often. Regardless of the anticipated litigation landscape, it's critical that companies run data breach investigations through outside counsel, who must retain all third parties, and for all parties to work at the direction of outside counsel. We spend a lot of time ensuring that companies implement and maintain strict communication protocols during data breach investigations, due to the threat of litigation and in particular discovery. Also, it's very important to be privy to the requirements, notification deadlines, and specific nuances of different jurisdictions across the world – and the ways privacy and cyber laws often conflict with one another. Decisions surrounding how to reconcile these laws are essential for legal, regulatory and reputational reasons.

Within the context of cybersecurity, what are some of the key issues you are seeing related to privilege?

Reed: Privilege can be a sticky wicket in cybersecurity investigations. The case law has been fairly good for instances where the forensics provider was retained by the outside law firm in order to assist the firm with its investigation. You see pretty consistent enforcement of attorney-client privilege in that instance. But it sometimes becomes problematic if the company itself is the one retaining the forensic investigator. There are instances where that work has been found not to be privileged because it wasn't at the behest of an attorney specifically to assist with an attorney's investigation.

Another instance where privilege can be challenging is on the retail side with payment card breaches,

With a top-tier, AI-driven predictive analytics solution in place, law departments can expect to see a host of improvements.

because they're governed by the Payment Card Industry Security Standards (PCI DSS) Council. Many times you're required to retain what's called a PCI Forensics Investigator (PFI), and that PFI is going to share their report with the credit card brands. So there's a pretty clear argument that plaintiff lawyers will make that, given the sharing of that report with the credit card brands in connection with the PCI work, there is no privilege attached to it.

Kohne: Case law regarding attorney-client privilege continues to evolve. Courts have generally respected the attorney work-product doctrine in the context of a data breach investigation. However, companies should be on notice that forensic reports, risk assessments and other security-related documents must be prepared under the umbrella of attorney-client privilege, where all parties are working at the direction of outside counsel, and that there are certain practical steps companies should take to protect attorney-client privilege. Since cybersecurity is an area where technical reports are often produced, thinking through how to structure data breach investigations will be critical to maximize a company's likelihood of maintaining that privilege. In addition, companies should be aware that in cases of multijurisdictional breaches, the laws around privilege can vary greatly from jurisdiction to jurisdiction. These various laws should dictate a company's actions and communication practices during the breach. ■