Corporate Counsel Business Journal
September ▪ October 2018
ccbjournal.com

CCBJ

Cyber's Singular Nature: Spanning Industries, Boundaries and Precedent

▶ Akin Gump's Michelle Reed and Natasha Kohne stress the importance of knowing the myriad privacy obligations that affect a company, as well as the regulators that enforce them.

CCBJ: Let's start off with some background about you and your practices.

Natasha Kohne: Michelle and I co-lead the cybersecurity, data privacy and data protection practice at Akin Gump. We do everything from advising clients on managing data breaches and defending clients in related regulatory investigations and legal proceedings, to privacy and information security compliance, which includes work on privacy policies, tabletop trainings, incident response plans, vendor management processes and risk assessments.

We routinely lead clients through civil and criminal cyber cases involving the FBI, the Department of Justice, the Securities and Exchange Commission, the Federal Trade Commission and other government agencies. Our representation on these matters utilizes both our deep privacy and information security knowledge and regulatory experience as well as our firm's strong litigation practice, particularly our class-action defense work.

One thing that sets our firm apart from others in this space is our international expertise. We use that expertise, and our global presence, to help clients whose businesses and concerns span several countries and fall within different international privacy and information security regimes.

Michelle Reed is a partner at Akin Gump and co-leader of the firm's cybersecurity, privacy and data protection practice. She specializes in advising clients on data breach investigations, notifications and subsequent litigation. Reach her at mreed@akingump.com.

Michelle Reed: Cyber is one of those unique practices that spans multiple industries. We do interesting due diligence work on mergers and acquisitions, making sure that companies have thought through the privacy and information security implications.

We are particularly adept at working through breaches. We do tabletop scenarios to help our clients prepare on the front end and then work with them to efficiently remediate after a breach, helping them get through their notification obligations and meet state- and country-specific requirements. Depending on the type of breach, notifications are not just to consumers or employees but also to governments, both domestic and international.

The FTC has pursued a number of data security cases over the past 12 to 18 months. What are some of the core issues they are trying to address, and what should readers be doing to protect their companies?

Reed: The FTC has always been a lead regulator in the privacy and cybersecurity area. When you look at all of its enforcement actions, the FTC's main focus is really on whether companies are doing what they've said they'll do in terms of protecting privacy and securing data, and making sure they have the proper administrative, physical and technical

safeguards in place to meet their promises. The FTC is also asking, even if companies didn't make an affirmative representation, if the way they've handled data is so egregious that it is, by its very nature, an unfair practice.

To date, however, the FTC hasn't defined what fair cybersecurity or privacy practices are. They have simply said that you have to have practices that are not unfair and are not deceptive. In advising clients, we dissect the enforcement matters and, by implication, assess what the FTC deems to be unfair or deceptive.

Kohne: In short, the FTC continues to play its role as the data privacy and security guardian for consumers, and it continues to cast a broad net across many issues and industries. In addition to the issue of misrepresentations in privacy policies and affirmative representations to consumers, which continue to be an important theme in FTC enforcement actions, the FTC brought its first charges against companies relating to the EU-U.S. Privacy Shield framework for certain alleged misrepresentations regarding participation in that program. We expect the Commission to continue to pursue similar cases as the Privacy-Shield program faces increased pressure and as the EU continues to scrutinize international data transfers.

With the varying disclosure requirements, how do you advise clients on compliance if they suffer a breach? How might this differ on a state-by-state basis or for multinational companies?

Natasha G. Kohne is a partner at Akin Gump and co-leader of the firm's cybersecurity, privacy and data protection practice. Her practice also focuses on investigations, litigation and international arbitration, often involving complex multijurisdictional and international problems. Reach her at nkohne@akingump.com.

Reed: All 50 states have their own identity theft protection statutes. These statutes define personal data and the combination of data that requires notice differently. We have to drill down very quickly into what happened, what data was impacted and, typically, where those individuals whose data was impacted reside. Many state statutes are not based on where the corporation is located but where the individuals whose information was breached reside.

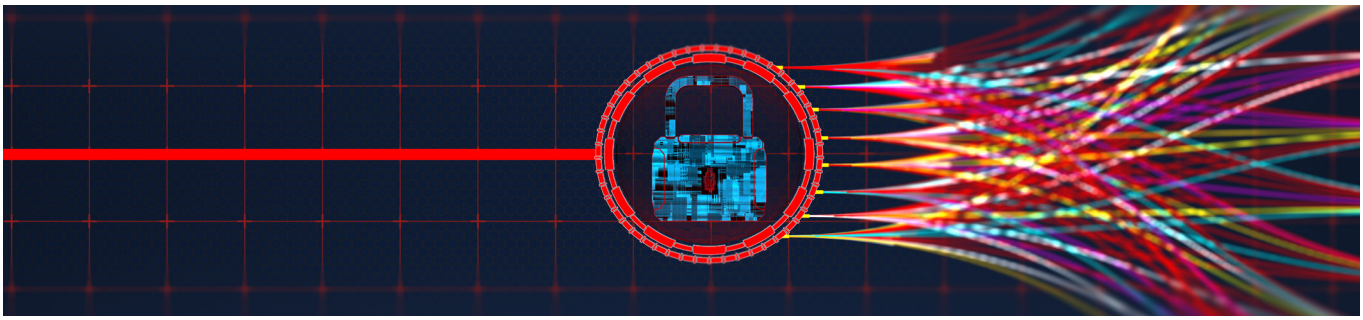
Breached data impacts consumers of many states, often all 50, as well as other countries. In those instances, we take the highest standard and meet those notice requirements for all. It can impact how long you do credit monitoring or how quickly disclosures go out. Many disclosure requirements involve contacting authorities before you give notice, but others involve contacting the authorities after consumer notice is given. With some states, you contact the state police or FBI; some others, you don't. The response depends greatly upon what happened and what data was impacted.

Kohne: We've developed our own proprietary matrix that tracks the specific requirements of all 50 states' data breach laws that allows us to efficiently input information related to a breach and turn it into advice in a very short time frame. Notification obligations often depend on the number of individuals affected who live in a particular state, what type of data is affected, and other incident-specific details. We use our internal matrix to quickly build a breach response timeline and to track state-specific notification requirements. A reliable notification timeline is the first step in the breach response process.

Internationally, notification obligations have taken on increased importance, given the GDPR's general 72-hour breach notification requirements for certain incidents. Other countries are also moving to adopt similarly strict notification obligations. We track these as well and work on U.S. and international notifications simultaneously.

There are so many government agencies involved in data security issues. How are you advising clients on how to navigate them all?

Kohne: We advise each of our clients, especially those operating in the multinational environment, to identify what data sets are critical to their functioning. This serves as a means of better understanding what regulators may oversee their work – state, federal or



international. With this information, we help companies craft policies and procedures that are tailored to their specific situations.

We also recommend that clients work their regulatory response and outreach efforts into their incident response plans. We advise clients to have the contact information of their relevant regulators and local law enforcement offices available and to reach out and speak to them before any incident occurs. Having strong relationships with your local regulators can really ease any incident response process.

Reed: Many companies don't even realize who regulates them. We've had numerous merger and acquisition due diligence instances where the company on the other side missed an entire slew of regulations that they didn't even know they were subject to. We can usually hunt through that pretty quickly and get clients a clean answer of who is going to be regulating them here in the United States.

Privacy is at the core of many cyber and data security issues. What are some best practices to ensure that companies are compliant with privacy regulations?

Reed: Know your data flows. If you don't know what your data is, where it's coming from and how you use it, there's no way to protect it.

Second, make sure that you have fundamental protections in place to assess privacy. The FTC put out a great publication called "Start with Security," and it gives you some data security basics. If you want to make sure you're protecting privacy, you need to have strong password protections and address access controls, so that only people who need the data to do their work have access to it.

GDPR codifies privacy by design. Designing practices to maximize data protection and privacy, and adopting data minimization policies, is key to protecting data. Even if you're not subject to GDPR, incorporating privacy into everything you do can actually decrease the cost of a breach in the future because, when you have a breach, you typically have less data or data in fewer places.

Kohne: Michelle is right that one of the first steps is internal data mapping. This is critical to ensuring you understand what privacy and information security frameworks are applicable to your business. Another key area of focus is starting up a robust third-party vendor management program to minimize risk against third parties that routinely receive your data or access your systems. To help manage all of this and prepare for the inevitable security incident, we work with clients to develop and test incident response plans. Running risk assessments to prioritize threats and tailoring compliance programs to address business priorities and highest risks are also recommended best practices.

What trends are you seeing in data breach litigation?

Kohne: In the *Lab MD* case, the FTC brought claims against the company for violation of Section 5 of the FTC Act, by, among other things, failing to have reasonable security measures in place to protect patient information. After a long and sordid history, the Eleventh Circuit recently found in Lab MD's favor. Most interestingly, the Eleventh Circuit noted that the FTC must specifically provide a company with the actions that the Commission believes violate the law, and the FTC must tailor a corrective action plan to those particular violations, rather than simply asserting a blanket order to implement "reasonable security." This has been an ongoing criticism of the FTC, and the

decision is significant because it's a successful challenge against an FTC enforcement action and scrutinizes the FTC's approach to regulation by consent decree.

One of the threshold issues in any data breach litigation is a plaintiff's ability to establish standing to bring a case, and it usually hinges on establishing harm. Post-*Spokeo*, courts have continued to adopt divergent views on whether the risks of identity theft are enough to meet the standing requirements when no allegations of actual harm exist. A lack of clarity among circuit courts continues.

Reed: The *Carpenter* case was a surprise to many people. Privacy advocates are saying it's a huge victory. In *Carpenter,* the Supreme Court said that there is a constitutional Fourth Amendment problem with providing cell phone location information without a warrant. Geolocation data tells about who we are, where we go, what we do and, often derivatively, what we believe.

When you look at the *Carpenter* decision, which is a very complex 5-4 decision with multiple dissents, you can see that the Supreme Court is recognizing that as technology changes, so too does the interpretation of what a Fourth Amendment right looks like and what our expectations of privacy are. Things have been less likely to be litigated previously because plaintiffs have not had receptive courts, but I think we are going to find a greater reception as technology changes.

Now let's be clear, I'm on the defense side, and I think we have really strong defenses as to why certain privacy protections don't necessarily apply in various instances. But as technology grows and changes, I definitely think we're going to see a changing of the law to serve these new facts.

What should readers know about the California Consumer Privacy Act (CCPA)?

Kohne: This is certainly one of the most significant pieces of privacy legislation in the United States that was just passed in June 2018. Consumers have a right to know what information is being collected about them, the purposes for which the data is used and whether it's being sold and to whom, or at least the category of third party to whom it's being sold. They also have the right to access the personal information that companies have collected about them, to request that their data be deleted in certain circumstances and to opt out of their data being sold to third parties. Each of these rights has certain exceptions, and the CCPA does not go into force until January 2020.

There is broad concern among those of us who regularly defend companies in California that the act will touch off a wave of consumer class actions.

But the key issues, from a defense perspective, are the potential for plaintiffs to argue that the CCPA's definition of "personal information" is expansive and the new private right of action for consumers.

> **Have the contact information of relevant regulators and local law enforcement offices readily available and reach out to them before any incident occurs.**
>
> —NATASHA KOHNE

Consumers will be able to seek the greater of their actual damages or statutory damages ranging from $100 to $750 per consumer per incident. If you think about class actions, the potential effect is significant. The California Attorney General's Office will also have the ability to pursue enforcement actions and seek fines of up to $2,500 for general violations and $7,500 for intentional violations. There has already been talk of trying to reform certain aspects of the CCPA before it goes into force.

Reed: The California Consumer Privacy Act is estimated to impact over 500,000 U.S. companies, and the impact of this legislation is going to be very broadly felt throughout the United States, since most large companies do business in California.

There are two ways to look at the CCPA: you can look at it as a pretty significant burden that passed very quickly to avoid a referendum, or you can view it as a way, potentially, for U.S. businesses to have an improved relationship with Europe. There have been many complaints that we have not had sufficient privacy protections in the United States, and I think this California legislation takes a step, hopefully, in building a bridge with the EU. ■