wiley

NEWSLETTER

What to Watch for in Privacy and Security in 2019

January 2019

Privacy in Focus®

We can expect an enormous amount of activity for privacy and security professionals in 2019. While 2018 may have been as big a year as we have ever had for new privacy and security developments, 2019 may be just as important.

Practice Areas

Privacy, Cyber & Data Governance

The Development of GDPR

While Europe has had significant privacy rules for more than 20 years, the EU General Data Protection Regulation (GDPR) caught everyone's attention to an unprecedented degree. Companies around the world raced the clock to get into compliance with the GDPR in May of 2018. We heard agitated reports (none of which should have been surprising) about the small percentage of companies that were in "full compliance" with the GDPR at this date – with these reports continuing today. Since that point (and continuing into 2019 and beyond), these companies (and the many others who were not aware of their obligations in May) will need to refine their GDPR compliance activities, paying close attention to ongoing official guidance, additional information about best practices and reported breaches or other problems. It is clear that GDPR compliance – like most privacy and security compliance – will be a long and winding road, and that there will be no obvious "end" to the compliance process. In fact, companies seeking to say "we're compliant and we are done" seem to be missing the main point.

The most critical issue to watch in 2019 will be enforcement. Some in the media have decried the lack of GDPR enforcement to date. That makes little sense to me – cases take time to investigate, and

government regulators generally do not try to jump the gun on privacy investigations. At the same time, enforcement has started, and we can expect to see it ramp up significantly in 2019. I will be watching for two key things – what kinds of enforcement and how big are the penalties. On the first, we will see what the various privacy regulators care about. One note of caution, however – what happens "first" may not be what they care about the most; these may simply be the cases that are resolved the most quickly, either because the practices clearly are problematic or the target does not resist to the death. We already are aware of large-scale investigations into some of the world's largest tech companies – but what kind of enforcement will a "normal" company face?

The penalty issue may be more significant (although, again, this may reflect ease of negotiation rather than substance). The GDPR caught people's attention because of the potential for large fines – fines of up to 4% of an entity's "global annual turnover" (essentially revenue) for the preceding fiscal year, or 20,000,000 euros, whichever is higher. These are real numbers – if used. At the same time, even these enormous numbers may not matter much to some of the larger companies – raising the question of what kinds of penalties and enforcement might be "enough" to generate better behavior. If the regulators – who have substantial flexibility under the GDPR – start pushing the envelope on these amounts, particularly for "normal" companies, then all bets are off.

California's Privacy Law (and will there be others)

In June, California passed the California Consumer Privacy Act. It is a broad, general privacy law (scheduled to go into effect in 2020) that protects all California consumers and will apply to a broad range of companies, both in and out of California. It provides consumers with many rights (of varying levels of detail and complexity) concerning their personal data, with substantial compliance challenges for covered companies. It may be less prescriptive than the GDPR – but the rights may be more challenging to implement. The law also is in flux – it was written quickly, and has both obvious ambiguities (including such threshold questions as whether personal data is included in employment and professional contexts) and various ongoing points of debate. We will be watching how the language of the law evolves and is explained and whether the industry is able to water it down. We will watch whether the deadlines get extended, and how – when the law finally does go into effect – enforcement will proceed.

Perhaps more significantly, we also will be watching whether other states follow California's lead – resulting in both a broader range of privacy law and the possibility of conflicts and tensions between the states. California's law is tough – and will create compliance challenges – but, much like the GDPR, companies likely will be able to navigate it. However, if we start getting other versions in other states – particularly with different provisions – then the compliance challenges magnify dramatically. California has an extensive history of privacy laws. Some of these laws exist in California and nowhere else. Some – even if they exist only in California (e.g., the law on privacy policies for websites) have a broader national impact. Some California laws (e.g., the SSN law) end up in many but not all states. The breach notification statute took more than a decade, but now exists in all states. Where will the newest California law land? It is highly unlikely that there will be 50 similar state laws – but it may only take three to five to tip the national debate in significant ways.

U.S. National Privacy Legislation

The GDPR and the new California law also have pushed privacy to the top of the national agenda. For the first time in recent memory, there is a significant debate about a national privacy law. Stakeholders are setting out their positions and principles, hearings are being held, and legislative language is being drafted. Preemption of state law, a private cause of action, and how to handle otherwise regulated sectors are on the core list of critical topics for debate (and there is no current consensus on any of these points). While there clearly is interest, on both sides of the political aisle, in some kind of national law, we are still a long way away from any meaningful consensus on the large or small points of such a law. But the activity on this potential national legislation during 2019 is likely to be frenetic.

Aside from these broad issues, I'm also watching carefully how existing laws will be factored into the national debate, particularly for the health care industry. We've always known that the Health Insurance Portability and Accountability Act (HIPAA) rules have meaningful gaps. At the same time – where it applies – HIPAA creates some important policy choices that have worked well for the health care industry and patients, and may prove useful as models for the national debate. Will the new law override HIPAA? Will it simply apply in addition to HIPAA? Or will heath care companies be carved out from the broader national law? The California law generally carves out HIPAA covered entities and business associates from coverage (although not without generating meaningful confusion). Many of the federal proposals are directed primarily at "unregulated" activities – and therefore also leave out HIPAA entities from new regulation. Will that approach continue? Does it make sense, given HIPAA's scope limits? If there is meaningful preemption of state law, will health care companies want to be subject to the new law, to benefit from preemption? There are lots of moving parts on this legislation, but the health care industry needs to make sure it is participating aggressively and thoughtfully in this ongoing debate.

The Federal Trade Commission

The Federal Trade Commission (FTC) is the default national privacy regulator, independent of specific industries. They have developed an aggressive approach to data security enforcement, based on more than 50 cases in recent years. At the same time, their authority on data security is under attack (including a highly confusing court result in 2018 as part of the extensive LabMD proceedings), and FTC leadership is looking at focusing its enforcement only on situations where there is clear individual harm. In addition, the FTC has been less assertive in developing "privacy standards" – what is appropriate for consumers in connection with privacy – beyond deceptive practices. The FTC is under pressure from EU regulators to be active in enforcing Privacy Shield and privacy and data security in general. There are extensive debates that are ongoing about whether the FTC can be trusted to be the regulator if there is a national law. Other countries also look to the FTC for America's "position" on privacy issues. I'll be watching whether the FTC moves in new enforcement directions (which might reduce the need for a new privacy law), or whether it backs away on these issues or stays silent. I will be watching whether the recent challenges to data security enforcement make the FTC back away from its history. I will also be looking for whether the FTC has teeth in concluding some of its larger ingoing investigations – where both U.S. industry and international regulators will be watching whether the FTC can truly be the nation's privacy regulator.

The Next Big Security Breach or Privacy Scandal

We keep waiting for a privacy and security tipping point. Many of us have thought that the latest and greatest security breach (going back almost annually for a decade, whether it was Target, Sony, OPM, Anthem, Equifax, or other enormous breaches) would tip the vote towards national legislation on data security. We've been wrong each time – and now the debate is largely being driven by other events. We've seen recent tech company privacy scandals - almost too numerous to mention – shape the privacy debate. I will be watching whether the next problem, an enormous or risky security breach or a particularly juicy privacy scandal, will actually make any difference in how the federal government addresses privacy and data security issues. We all – consumers and companies alike – need to be paying close attention to this debate.

Hot Topics for the Health Care Industry

The core principles for privacy and data security in the health care industry are set out in the HIPAA Privacy and Security Rules. These rules – initially established early in the 21st century – have undergone one large modification (the HITECH statute and implementing regulations) and a small handful of otherwise modest changes.

I will be watching whether a current initiative – a "Request for Information" (RFI) from The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) – will result in significant modifications to the HIPAA Rules. The concept behind this RFI is two-fold. First there are various holdover issues still remaining (nine years later) from the HITECH statute – like the controversial HIPAA Accounting Rule. More broadly, the RFI looks at whether HIPAA creates impediments to "coordinated care" and other areas where a broader flow of patient information should be encouraged (think opioid crisis). While only the first step in what could be a lengthy regulatory process, we may see meaningful change to some of the core provisions of the HIPAA Rules (even in a context where it isn't clear any changes are necessary).

These efforts, however, also are highlighting some of the concerns with other aspects of health care privacy beyond HIPAA. For example, many of the concerns in the RFI about data sharing for "coordinated care" and the opioid crisis actually seem rooted in other federal law (mainly the Part 2 rules on substance abuse information) and the enormous range of state laws that make data sharing harder in many contexts.

In addition, while the HIPAA Rules provide a baseline for the traditional health care industry, HIPAA has never been an overall health information privacy law. Limited by statute, the Privacy Rule applies only to "covered entities," mainly health care providers and health insurers. The RFI can't "fix" this limitation in any meaningful way. Over the past decade, we have seen an explosion of new kinds of health data being gathered, accessed, and analyzed by entities not subject to the HIPAA Rules, primarily (but not exclusively) in the direct-to-consumer context. The RFI cannot address these gaps – HHS cannot extend its regulations without congressional action outside of the set of covered entities – so currently there is a significant gap in regulatory obligations for this "non-HIPAA health data." For consumers, these gaps create privacy risks and confusion and potentially risks of discrimination and otherwise. For the entities gathering this highly sensitive data, there is an important challenge to act thoughtfully and responsibly even in the absence of firm governing principles.

I will be watching how this issue evolves in 2019, and whether companies will appropriately safeguard this important information.

We also are seeing an enormous change in who is actually part of the health care industry. Some of this involves GDPR more than HIPAA – pharmaceutical companies, for example, have little direct concern under HIPAA (as they typically are not covered entities or business associates) but have meaningful compliance challenges under GDPR. In addition, one critical element of this "non-HIPAA" data involves the accelerating role of technology companies into the health care field. We are seeing aggressive moves into the health care industry – on almost a daily basis – by Amazon, Apple, and others, both to address perceived failures in the current industry and to make heath information more available to consumers through a variety of additional channels. Many of these consumer-driven activities will fall outside of the HIPAA rules. Some – particularly where technology companies may be moving directly into traditional health care industry activities – may subject these companies to new regulatory obligations. So, while the health care industry awaits the impact of these companies entering health care from a competitive direction, from a privacy perspective, we will need to see how consumer interests, loosely regulated environments, and health care disruption all combine to protect (or not protect) individual privacy interests – particularly for companies whose traditional use of personal data has not been driven by health care industry laws or ethics.

State Enforcement

We also are going to be watching whether the states become more involved in privacy and security enforcement in 2019. We are seeing some drop-offs in enforcement at the federal level (for example, the HHS Office for Civil Rights (OCR) generally has been quiet since the new Administration took office – but recently has shown more signs of life through a series of meaningful enforcement actions). Will the states step in to beef up the overall enforcement threat? We are starting to see three important kinds of state enforcement from state attorneys general: (1) enforcement in the regulatory gaps (primarily but not exclusively in New York); (2) through concerted state activity to take action under the HIPAA Rules (where state AGs have formal enforcement authority in addition to OCR); and (3) concerted action on broad national privacy issues (e.g., the recent national settlement involving Uber). Much like the FTC, the state AGs have authority to pursue a broad range of privacy and security cases – but they have not historically done much with this authority. We are seeing some modest changes in this area – but it will be important to see if this growth in state enforcement continues.

Conclusions

As a privacy lawyer, my need to learn and participate in new activities grows every day. For companies – with an ever-growing range of data available and new opportunities for analytics and other data crunching activities – the challenges for privacy and security are now a core corporate priority across virtually every industry. For consumers, the confusion and complexity has never been greater. We are seeing the privacy debate grow louder on a regular basis – but we are nowhere closer to any reasonable "solution." I expect 2019 to be a year of discussion, debate, enforcement, risks, and other challenges. I think we will make progress toward a U.S. national law – but we are unlikely to see that debate reach any meaningful

conclusions. At the same time, through the growing Internet of Things and other broad uses of data, an increasing range of companies now need to be paying close attention to these issues – many of them companies that have not historically had large amounts of personal data, including car companies, refrigerator and thermostat makers, toy companies, and the growing number of companies that make personal data use a part of their business model. This leaves companies with an increased need to think about privacy and security strategically, and to learn as much as they can about both their own data needs and the evolving regulatory and enforcement regimes related to the overall use and disclosure of personal information.