Bloomberg Law News Dec 18, 2018

By Kirk J. Nahra Dec 18, 2018

Privacy law is hot and shows no signs of slowing in 2019.

We probably saw more significant privacy and data security developments in 2018 than in any previous year, including the compliance date for the EU's General Data Protection Regulation, the passage of California's groundbreaking privacy law, tech company scandals aplenty and substantial security breaches on essentially a weekly basis.

These issues will continue to play out in 2019. Here are the top five privacy and security issues I'll be watching given their potential impact on consumers and businesses alike.

The Evolution and Enforcement of GDPR

Companies around the world raced the clock to get into compliance with the General Data Protection Regulation (GDPR) in May 2018. There were widespread reports (none of which should have been surprising) about the small percentage of companies that were in "full compliance" with GDPR at this date.

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.

The most critical issue to watch 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.

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 percent 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 the regulators—who have substantial flexibility under GDPR—start pushing the envelope on these amounts, then all bets are off.

California's Privacy Law (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.

The law also is in flux—it was written quickly, and has both obvious ambiguities and 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. 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.

U.S. National Privacy Legislation

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.

The Federal Trade Commission

The 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) 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. 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.

The Next Big Security Breach or Privacy Scandal

Last, 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) would tip the vote towards national legislation on data security. We've been wrong each time.

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.

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., and chair of the firm's Privacy Practice. He teaches privacy law at the Washington College of Law at American University. You can contact him at knahra@wileyrein.com, and follow him on Twitter @kirkjnahrawork.