Bloomberg Law®

Privacy and Security Law Report®

Data Security

Looking Into the Murky Privacy and Data Security Crystal Ball–Predictions for 2018

Privacy and Data Security in 2018

The author writes about her top five privacy and data security predictions for 2018, including the on-set of the new European Union privacy regime, the privacy implications of the Federal Communication Commission's repeal of net neutrality rules, development of the injury standard that the Federal Trade Commission uses for data security enforcement, the proliferation of the internet of things, and the inevitable next major data breach.

By Adrienne Ehrhardt

With 2017 almost in our rearview mirrors, the Equifax Inc. data breach and the WannaCry ransomware cyberattack will become distant memories with new disquieting stories taking their place. Peering into the murky privacy and data security crystal ball, what can we expect to see in 2018? Keeping in mind the accuracy of antiquated crystal ball technology, these are some issues that may be on the horizon.

1. General Data Protection Regulation Unless you have been in a privacy black hole, you probably already know that the European Union's General Data Protection Regulation (GDPR) enforcement date will finally arrive on May 25, 2018. With as much anticipation as the release of a *Star Wars* movie and a preparation approach for many that resembles a college student in denial of an approaching final exam, we will find that May 25, 2018 will not be an Armageddon like day of reckoning, especially for most organizations in the U.S. Potential fines of the greater of 20 million euros ($23.58 million) or 4 percent of global annual turnover for noncompliance provide entities with motivation to comply with GDPR.

Adrienne Ehrhardt is the practice group chair of Michael Best LLP's privacy & data security group in Madison, Wis.

The practicality of immediate enforcement on all those for whom GDPR applies, however, will buy organizations some time. In addition, for many organizations who may be technically subject to the EU's extraterritorial reach even though they do not have establishments in the EU, it would seem unlikely that the EU's enforcement priority would be focused on them, unless the potential fines or number of affected data subjects are significant.

New to the EU are data breach notification requirements. Because of the publicity that data breaches generally receive, this may be an area that receives attention. Of interest will be how supervisory authorities assess whether a data breach is likely to result in a high risk to the rights of data subjects such that individual notification will be required. It is likely that individual notification will occur with respect to some data breach next year in the EU.

2. The Death of Net Neutrality The 2017 year ended with the death of net neutrality. With the Restoring Internet Freedom Order, the Federal Trade Commission's Acting Chairman Maureen Ohlhausen proclaimed that the Federal Communications Commission ''restored the FTC's ability to protect consumers and competition throughout the internet ecosystem.

The FTC is ready to resume its role as the police on the broadband beat, where it has vigorously protected the privacy and security of consumer data and challenged broadband providers who failed to live up to

 ISSN 1538-3423

their promises to consumers.'' While this issue even grabbed the attention of teenagers who may have even shed some tears because of the thought that their videos may not stream properly and others who decried that internet service providers can basically do whatever they want, the death of net neutrality will not equate to death of the internet.

The FTC was quick to remind people of its role as the privacy and data security police, providing hope to people that its general consumer protection role will further prompt it to act more broadly to regulate other unfair practices of internet service providers. In order to gain credibility in this role, look for the FTC to engage in some kind of enforcement action relating to the provision of internet service or at the very least release some guidelines targeted at Internet service providers.

3. What's the Harm? Acting Chairman Ohlhausen discussed the concept of informational injury in September 2017, summarizing the types of injury that has motivated the FTC to act in privacy and data security matters. Expect the FTC to require a more concrete demonstration of harm in order for it to bring an enforcement action relating to privacy and data security. Meanwhile the issue of harm will continue to play out in the courts with challenges to and differing applications of *Spokeo* (the U.S. Supreme Court's decision relating to whether an alleged violation of a statute alone as opposed to a showing of some concrete harm was necessary to have standing to bring a claim) that lead to inconsistent results.

Courts and regulators will continue to wrestle with balancing and determining the amount and nature of harm that will be acceptable to people in order to set standards for when individuals should be able to seek judicial intervention and when businesses should be given the benefit of not having the impossible task of protecting against all cybersecurity harm. This harm determination will be material in nurturing growth and innovation in technology and data use in a world where some may want the relative information security of a paper world.

4. IoT Companies will invest in greater security for their internet of things (IoT) devices in the face of no new regulation or guidelines relating to IoT in order to move their products beyond novelty use cases to ones consumers and businesses will trust and want. IoT and artificial intelligence capabilities will continue to grow even more rapidly in business-to-business applications that process commercial data and in traditional industries like manufacturing and agriculture where the power of data analytics provides valuable insights and brings less risk because of the absence of consumer data and interests.

5. The Next Big Breach There will be one. Having a world without data breaches is as idealistic and lofty as achieving world peace. It is something for which we should strive, but is ambitious for some of the reasons that threaten peace. We will see even more sophisticated cyberattacks using advances in artificial intelligence and machine learning. In addition to focusing on the human and technological levers to prevent and anticipate these attacks, there will be an increased effort on and demand for developing more options for business continuity and solutions for consumers to address issues in the event their data is breached. Consumers will clamor for more than just credit monitoring as the primary solution to when their personal information is accessed or stolen. The limited nature of this consumer relief was ironically demonstrated by the Equifax breach.

As we make our way through 2018, we will see how good crystal ball technology is, given that it lacks the benefit of big data, edge computing, and artificial intelligence. In the meantime, we wish you and yours a 2018 with no data breaches.

BY ADRIENNE EHRHARDT

To contact the editor responsible for this story: Donald Aplin at daplin@bloomberglaw.com

PVLR ISSN 1538-3423