Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Cybersecurity And Privacy Policies To Watch In 2018

By **Ben Kochman**

Law360, New York (January 1, 2018, 3:04 PM EST) -- Sweeping European data protection reforms that will echo around the globe, an opaque new cybersecurity law coming into force in China, and enforcement decisions made by a Republican-led Federal Trade Commission head policy watchers' list of cybersecurity and privacy regulations to keep an eye on in 2018.

In a world increasingly more connected by data, regulators around the world will continue racing to keep up with new technologies while addressing security concerns and privacy expectations, experts tell Law360.

"It's not coordinated, and it's not even always coherent, but there is an unmistakable trend toward more regulation in the space," said Robert Silvers, a former assistant secretary for cyber policy at the U.S. Department of Homeland Security under President Barack Obama and now a partner in Paul Hastings' white collar and cybersecurity and privacy practices.

Here are five data privacy and cybersecurity policies to watch in the coming year:

Dawn of a New Data Day in Europe

The last time the European Union adopted a member-state-wide law regulating data privacy, Sergey Brin and Larry Page were brainstorming the idea of a search engine that would help find specific sites on the World Wide Web — they later called this Google — from their Stanford dorm room. Mark Zuckerberg, the future founder of Facebook, was 11 years old.

It's a bit of an understatement to say that how the world interacts with data has evolved since the EU adopted its data protection directive in 1995. But it took over two decades for European legislators to agree on an update to that law: the General Data Protection Regulation, which will take effect on May 25.

The new law applies to any company that processes the personal data of people in the EU, including tech giants like Facebook, Apple, Google and Twitter, which each have millions of European consumers.

The GDPR creates a higher bar for customers to consent on how their data is stored and used. Companies will be required to post more prominent privacy notices and give consumers an option to opt out of certain data collections. The new law also requires potential victims of a data breach to alert local

authorities within 72 hours.

One of the legislation's aims is to harmonize what had been a splintered set of national data privacy laws within Europe. But the GDPR may end up causing companies aiming to comply with European law just as many headaches as before because it gives individual countries leeway to set their own rules on key issues, said Kristof Van Quathem, special counsel in Covington & Burling LLP's Brussels office.

One thorny issue for technology firms seeking access to Europe's lucrative market could be inconsistencies in the age when someone can consent to his or her data being collected. The GDPR sets that bar at 16 years old, but allows member states to lower the age of consent to 13 years old.

"If you provide the same services to people throughout the EU, it is going to be a challenge," said Van Quathem. "You almost have to adapt your service to the particular territory. That was not the spirit of the GDPR."

Germany and Austria have already passed their own data protection laws implementing the GDPR, and privacy watchers eagerly await other countries passing their own data security laws by May.

Then there's the question of enforcement.

The new law gives European regulators the chance to levy massive fines of up to 4 percent of a company's annual revenue, which could amount to hundreds of millions of dollars for the big Silicon Valley tech companies.

If fines are high enough, firms are likely to challenge the first enforcement actions in court, said Lothar Determann, a partner at Baker McKenzie who advises Silicon Valley companies on complying with global data privacy laws.

The inevitable court battles could help give European privacy laws, which have scarcely been enforced in the past, a much-needed "reality check," Determann said.

"There will be a lot of haggling and a lot of litigation, but it's far from clear who will pay these horrendous fines," he said.

Determann said he expects EU regulators to both target multinational tech giants and go after smaller European companies, which are less likely to comply with complex rules, with what he called "traffic ticket kind of enforcement" that could help fund the bigger cases.

Van Quathem agreed that companies are likely to fight the first GDPR enforcement actions — which he said could make regulators think twice before bringing a case.

"I expect them to be cautious and to be careful about how they use their new powers," he said. "Because the laws are new, I think it's more likely that those fines will be challenged in court. Regulators are well aware of that."

The Great Cybersecurity Firewall

China's new cybersecurity law took effect on June 1, 2017, but authorities are not required to put it fully into place until June 2018, said Yan Luo, Beijing-based special counsel at Covington & Burling.

The new law mandates what it calls "network operators" and "critical information infrastructure operators" to submit to government security reviews companies fear will involve turning over encryption keys to Beijing. Companies covered by the law are required to store data on local servers.

A recent poll of American corporations that do business in China found that four out of five firms feel "somewhat or very concerned" at how the data security regulations could impact their business in the world's second largest economy.

Businesses could get some clarity on the scope of the new law in the coming year, Luo said.

"In the first half of 2018, we expect to see important guidance issued by regulators regarding controversial issues such as the protection of critical information infrastructure and cross border data transfers," she wrote in an email.

But it is unlikely that the Chinese government will immediately enforce the new law, as Beijing is likely to offer companies a grace period to comply, Luo said.

China has defended the legislation as a way to stop hackers and keep citizens' data safe. But for now, a number of seemingly vague and broad definitions have left multinational corporations around the globe — and their lawyers — confused about how to comply.

"I know some companies assuming that the law will apply to them, and taking steps based on that, and I know other companies assuming that the law won't apply to them, and taking steps based on that," Miriam Wugmeister, co-chair of Morrison & Foerster LLP's global privacy and data security group, told Law360 earlier this month. "Both are acting reasonably."

No matter how stringent the law winds up being, it will be difficult for companies to turn their backs on China's massive market. Apple and Amazon have already announced plans to build data storage centers in China in efforts to comply with the new rules.

What Simons Says on Section 5

In America, the agency to watch will be the Federal Trade Commission, which has pursued companies it says failed to reasonably protect consumers' data by using the unfair and deceptive practices prong of Section 5 of the FTC Act.

The Senate is expected to confirm the Trump administration's nominations for the three vacant spots on the five-member FTC commission in the coming year, including Trump's choice for FTC chair, antitrust attorney Joseph Simons of Paul Weiss Rifkind Wharton & Garrison LLP.

Simons' background, which includes a stint as director of the FTC's Bureau of Competition from June 2001 to August 2003, gives some clues as to his approach on antitrust matters. His view on cybersecurity and privacy issues is less clear.

Acting FTC Chairman Maureen Ohlhausen has repeatedly stressed that she favors "regulatory humility," and has directed her staff to focus on concrete privacy and data security harms, not speculative ones.

Where a Simons-led commission draws the line for what is actionable under Section 5 in data breach

cases could have wide-reaching effects on how regulators nationwide act on information security, attorneys say.

"The FTC is far and away the thought leader in the United States when it comes to privacy and cybersecurity," said Doug Meal, a partner at Ropes & Gray LLP currently fighting, in a closely watched case in the Eleventh Circuit, the Obama-era FTC commission's ruling that small medical provider LabMD harmed consumers by failing to protect sensitive medical data.

"Whatever direction the FTC goes in from an enforcement standpoint will have a significant influence on what direction other state and federal regulators go," he said.

To round out the Republican-led commission, the Trump administration has said it will nominate Noah Phillips, chief counsel for Republican Sen. John Cornyn of Texas at the Senate Judiciary Committee, and Democrat Rohit Chopra of the Consumer Federation of America.

The Senate's approval of the nominations would resolve what has been a tricky situation on the commission, which has three vacancies for the first time in its more than 100-year history. The current setup makes it difficult to take action in any matter, since the agency requires a majority vote of commissioners to do so.

Empire State of Mind-ful Cybersecurity

It remains to be seen whether credit reporting giant Equifax's recent admission that sensitive data on more than 145 million Americans was compromised in a data breach will spark action to pass a federal cybersecurity law.

Legislative action on the issue for now is expected to largely continue to happen on the state level, including in New York, where any financial institution regulated by the New York Department of Financial Services — a group that includes some of the world's biggest banks — will be required to meet key deadlines in the coming year showing they have set out detailed plans for handling data breaches, increased their monitoring of how third-party vendors handle and secure customer data, and appointed a chief information security officer, among other requirements.

Avi Gesser, a partner in Davis Polk & Wardwell LLP's litigation department who represents clients in white collar criminal defense and cybersecurity matters, called the new financial services law a "game-changer."

"The DFS has created the most robust cyber regulatory framework out there, which is likely to have a lasting impact on cybersecurity regulations and expectations in general," he wrote in an email.

Regulators in Albany may also consider a post-Equifax data security law proposed by State Attorney General Eric Schneiderman. The Stop Hacks and Improve Electronic Data Security Act, or SHIELD Act, would expand the kinds of data breaches that trigger automatic reporting to authorities, such as username and password combinations, biometric data and HIPAA-covered health information, the attorney general's office says.

72 Hours: The New Normal?

Much of the public outcry over Uber's recent admission that hackers stole sensitive data on 57 million

rider and driver accounts has focused on the ride-sharing giant's disclosure that it waited over a year to tell customers about the breach. Equifax has been grilled in Congress over waiting six weeks to tell the public about its breach that compromised data like Social Security numbers that could have allowed consumers to be victimized without their knowledge.

Both the GDPR and New York State's new regulations address these concerns by requiring covered businesses to alert authorities of a data breach in the same timeframe: 72 hours.

In the absence of a U.S. federal law unifying the patchwork of 47 state data breach notification laws, the three-day deadline imposed by the European and New York laws could end up becoming the new normal for companies scrambling to get to the bottom of a possible breach, policy watchers say.

Tighter deadlines will put a heavy premium on having organized planning in place to respond to potential cyber incidents, said Silvers, the Paul Hastings partner and former DHS assistant secretary.

"It's very difficult for a company to get its arms around the scope of a data breach within 72 hours," he said, adding: "You need to be well oiled at the starting gun."

--Additional reporting by Evan Weinberger, Matthew Perlman, Christopher Crosby and Allison Grande. Editing by Benjamin Guilfoy and Catherine Sum.
