Privacy Legislation And Regulation To Watch In 2016

By **Allison Grande**

Law360, New York (December 24, 2015, 8:38 PM ET) -- Privacy issues will grab the spotlight in both the U.S. and European Union in 2016, with attorneys keeping their eye on high-stakes negotiations to replace a popular trans-Atlantic data-transfer mechanism as well as legislation that will ramp up companies' data protection and cybersecurity obligations on both sides of the Atlantic.

The last weeks of 2015 were marked with several major developments on the privacy front, including EU officials finally reaching an agreement on a new general data protection regulation after nearly four years of debate and U.S. lawmakers squeezing cybersecurity information-sharing legislation into an omnibus spending bill.

Progress is only expected to continue in the new year, with a deadline looming to clean up the upheaval created by the EU high court's invalidation of the safe harbor scheme for trans-Atlantic data transfers and the Federal Trade Commission expected to be joined by the Federal Communications Commission and others as aggressive cops on the privacy and data security beat.

"The privacy and cybersecurity worlds are becoming increasingly closer, and policymaking is growing because companies and individuals are interested in both," Hogan Lovells partner Harriet Pearson said.

Here, attorneys share the top policy developments that will bear watching in 2016.

Safe Harbor 2.0

Since the European Court of Justice's **surprising invalidation of** the U.S.-EU safe harbor data transfer mechanism in October, the clock is ticking for the European Commission and U.S. Department of Commerce to reach an agreement on an alternative.

"One of the biggest issues looming out there is the safe harbor, given that over 4,000 U.S. companies have relied on safe harbor for the exchange of data from Europe since the mechanism was put in place 15 years ago," Akin Gump Strauss Hauer & Feld LLP cybersecurity, privacy and data protection co-leader David Turetsky said.

The commission and Commerce Department, which were working on updates to the safe harbor scheme for nearly two years before the court's ruling, have **signaled in recent weeks** that they

are close to reaching a deal to address the high court's concerns that the data transfer tool fails to adequately protect the privacy rights of EU citizens by allowing U.S. intelligence officials unfettered access to the transferred data.

A swift agreement is particularly important in light of the European data protection authorities' recent pronouncement that they would **hold off on enforcement actions** until the end of January, after which time they would take "all necessary and appropriate actions, which may include coordinated enforcement actions."

"Right now, we're at the point where leading U.S. companies that are transferring data from the EU to the U.S. have to ramp up their use of alternate mechanisms for compliance," Pryor Cashman LLP digital media practice group co-chair Robert deBrauwere said. "It will be important to watch how that is resolved, and whether there will be some mechanism in place to facilitate that transfer of information as opposed to the ad hoc situations that are existing now."

In order to address one of the biggest criticisms advanced by the EU high court — that EU citizens lack the ability to challenge government surveillance activities in U.S. courts — Congress is considering the Judicial Redress Act, which would extend to foreigners the same rights enjoyed by U.S. citizens under the Privacy Act of 1974.

The U.S. House of Representatives **passed the bill** in October, but the measure has been held up in the Senate, where the Judiciary Committee failed to vote on it during its last business meeting of 2015.

"Without this bill, it is unlikely that regulators can agree on a new safe harbor program, meaning that companies will not only face continued regulatory uncertainty with respect to international data transfers but will also need to implement more burdensome, cost-prohibitive mechanisms for validating EU to U.S. data transfers," said Mauricio Paez, who heads Jones Day's privacy and cybersecurity practice.

EU Data Protection Regulation

After nearly four years of negotiations, the European Commission, Parliament and Council on Dec. 15 finally **reached an agreement** on a new regulation that will overhaul the bloc's data protection regime by tightening restrictions on the use and the flow of data while empowering national privacy regulators to levy fines of up to 4 percent of companies' annual global revenue.

"This is a sea change," said Lisa Sotto, the head of Hunton & Williams LLP's global privacy and data security practice. "The final text of the general data protection regulation is the biggest thing to happen in the privacy arena in 20 years, and the regulation will affect every global company in every industry sector."

While the long-sought-after political agreement on the regulation's text was finalized in 2015, multinational companies will have plenty to do in the new year, given that the law won't go into effect until two years after the Parliament and Council formally adopt it, a step that is expected to happen in early 2016.

"The big issue is how Europe will take the regulation and make sense of it and apply it, and what the next steps will be for companies in implementing it," Pearson said. "Regardless of where they're sitting in Europe, the regulation is going to be the main privacy policy for any company that has a website that touches Europe."

Besides its ability to sweep up a broad range of multinational companies, the regulation — which replaces a directive enacted in 1995 with a uniform law that will be implemented in the same way across member states — also significantly ramps up the fines that regulators are authorized to assess for noncompliance.

"With the general data protection regulation, the stakes are much higher with respect to enforcement and penalties," Turetsky said.

The regulation for the first time additionally creates an obligation for companies to report data breaches within 72 hours of their discovery, a requirement that will not only make such incidents subject to heightened public and regulatory scrutiny but may also prove difficult for companies to achieve on a practical level.

"There's no out in the general data protection regulation for making sure that the problem is fixed before the company has to give notice," Morrison & Foerster LLP global privacy and data security group co-chair Miriam Wugmeister said. "That could end up making things much worse from a security perspective because if a company is still wide open when it gives notice, that risks even more data being exposed."

EU Cybersecurity Directive

Just a little over a week before EU officials nailed down the general data protection regulator's text, members of the Parliament and the Council on Dec. 7 **reached a separate** deal on another piece of policy that will bear monitoring in 2016: a directive creating the bloc's first cybersecurity rules.

"It will be interesting to see how the rules are implemented," Paul Hastings LLP privacy and cybersecurity practice co-chair Behnam Dayanim said. "The EU is finally taking a broad-reaching position that certain steps are required when it comes to cybersecurity and that notice of breaches is required."

Under the network and information security directive, which was agreed to after more than two years of political wrangling and which member states have 21 months to implement into their national laws, critical infrastructure operators such as banks and health care providers as well as digital service providers such as Google Inc. and Amazon Inc. will for the first time be required to grapple with a set of security obligations.

Besides having to maintain appropriate security measures, covered entities will also be required to report all major security incidents to their relevant national authority, an obligation that will be broader than what is mandated by the data protection regulation, which covers only breaches of

personal data, and will be added on top of a patchwork of federal and state laws that multinational companies already need to contend with in the U.S.

"There are very mature breach notification and cyberincident understanding in the U.S., and that's not the case in Europe," Sotto said. "So this is really going to be sort of a watershed moment for cyberincidents."

Cybersecurity Information Sharing Act

Protecting networks from cyberattacks also promises to be a hot topic in the U.S. in 2016, especially after the Senate passed in the waning hours of its last session **a massive $1.15 trillion omnibus spending bill** that included a compromise version of a trio of competing cybersecurity information-sharing bills that had sailed through the Senate and House earlier in the year.

The Cybersecurity Act, which was quickly signed into law by President Barack Obama, is designed to encourage businesses to voluntarily share cyberthreat information among themselves and with the federal government by creating certain antitrust and legal liability protections and other incentives for companies that participate.

"In a world of risk and uncertainty, this legislation tips the cost-benefit analysis in favor of sharing and speaks to general counsel by saying that the company will have liability protections if it takes reasonable steps to share cyberthreat information that is stripped of personal information," Turetsky said. "It won't be a silver bullet, but hopefully it will be an effective tool in enhancing cybersecurity."

In the early part of 2016, retailers, banks and businesses across a broad range of sectors will be busy getting adjusted to the new law, and figuring out information-sharing arrangements that are most effective to protect their systems, attorneys say.

"It will be interesting to see what impact the law will have on the sharing of cyberthreat information between the public and private sector," Wugmeister said. "In order to fight the bad guy, there needs to be sharing between the sectors, so if this piece of legislation will have an impact on that will be something to watch."

FTC v. FCC: Data Security Friends or Foes?

There is no doubt that privacy enforcement will run hot in 2016; the primary question will be from which regulator companies are most likely to face the most heat.

"The FTC has for a long time been the lead regulator on the issue of privacy and data security, but I fully expect the FCC to continue to take a more active role in the space," Dayanim said.

The commission received a boost to its active enforcement agenda in August, when the Third Circuit ruled in a case involving Wyndham Worldwide Corp. that the **commission has the authority** to regulate private companies' data security under the unfairness prong of the FTC Act. The dispute settled in December, with the parties reaching a pact that helped **lend some**

insight into what the commission considers reasonable data security.

But the regulator was also **dealt a blow** in November, when its own administrative law judge tossed its data security case against LabMD Inc. due to a lack of harm, a decision that the agency has **asked its own commissioners** to review.

"The arguments in the LabMD case are not that much different from what we've seen trip up plaintiffs regarding harm in private class actions," Morrison & Foerster global privacy and data security group co-chair Andrew Serwin said. "So one thing to watch is how the LabMD decision impacts what cases they bring and where they go."

While predicted that the LabMD decision will be "more of a speed bump than a deterrent" for the FTC and have little impact on their aggressive enforcement style, the FCC is still looming large as the new privacy enforcer on the block.

The FCC boosted its profile in 2015 with **major data security actions** against AT&T Inc. and Cox Communications Inc., and with the enhanced power garnered from its recent Open Internet Order to regulate Internet service providers as "common carriers" exempt from the FTC's jurisdiction — which has **raised concerns for** at least one FTC commissioner — and its **hiring of prominent security researcher** Jonathan Mayer to serve as the chief technologist for its enforcement bureau, the new year promises to be no let down.

"The FCC seems to relish the higher profile and increased enforcement activity," Dayanim said. "But at the same time, I don't see the FTC relinquishing its role as lead regulator."

Encryption Wars

In 2015, law enforcement aggressively **pushed back at** moves by companies such as Apple and Google to outfit the latest versions of their products with default encryption settings that would prevent law enforcement from unlocking and retrieving data off them, even in response to valid search warrants.

The debate seemed to die down late in the year, when the Obama administration said that it would not push Congress for legislation that would require service providers to set up backdoors to allow law enforcement access to user data, but recent terrorist attacks in Paris and San Bernardino, California, has thrust the fight back into the spotlight.

"This is a really complicated debate that raises serious issues having to do with safety and privacy rights, so I think it's going to continue to be an important subject of discussion in the coming year," Turetsky said.

With the number of companies offering products with encryption that even they can't break on the rise, a legislative or policy move that would mandate them to provide a key to decipher the data would not only potentially undermine their security by allowing hackers to intercept the key, but could also result in backlash from consumers.

"Hopefully there will be healthy debate and exploration of alternatives that will not compromise the privacy and security of individuals, while providing a meaningful way for access to encrypted data to aid cybercrime, terrorism, and other criminal investigations," Paez said. "This will be significant issue in the overall privacy versus security debate for 2016."

--Editing by Katherine Rautenberg and Patricia K. Cole.