Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Privacy Legislation And Regulation To Watch In 2015

By **Allison Grande**

Law360, New York (January 02, 2015, 5:08 PM ET) -- Following a year marked by several headline-grabbing data breaches, privacy attorneys expect federal lawmakers in 2015 to step up efforts to push through uniform data security standards and cyberthreat information-sharing legislation and the European Union to finally deliver on a proposal to overhaul and strengthen the bloc's data protection regime.

Besides the legislative efforts, 2015 is also poised to bring with it increased regulatory scrutiny of companies' privacy practices by both established players as well as relatively new entrants such as the Federal Communications Commission, and an increased focus by policymakers on the security risks posed by emerging technologies such as Internet-connected devices, attorneys say.

“The outlook in 2015 is that we'll have more breaches, but I think we'll also continue to have more conversations as people get used to breaches as a way of life about what we expect to be kept private, and how we want to confront that,” Colin Zick, co-chair of the privacy and data security practice at Foley Hoag LLP, said.

Here are some of the policy moves that attorneys will be watching in 2015.

Data Security, Breach Notification Bills

While several bills to bolster private- and public-sector data security were floated in 2014 in response to high-profile intrusions at entities ranging from Home Depot Inc. and Sony Corp. to the U.S. Postal Service and the White House, no significant measures were able to cross the finish line. But with a Republican-controlled Congress set to take over, privacy attorneys are optimistic that calls to enact clearer data security standards will finally come to fruition.

“There have been efforts throughout the last several years to enact legislation, but I think Republicans taking control of the Senate really increases the prospects for having legislation pass both houses and being sent to the president's desk,” Mayer Brown LLP partner Howard Waltzman said. "Having Republicans in control means there's likely to be not only more agreement, but greater enthusiasm for it.”

The legislative proposals that have been put forth in past sessions and are likely to be reignited in the new term push for the creation of new standards for both data breach reporting and general data

security, which supporters say are necessary to eliminate confusion caused by a lack of clear data security standards and a patchwork of 47 state breach notification laws that impose conflicting reporting obligations.

“There's a growing recognition in Congress that having 47 different reporting standards does not make sense and that, given the number of breaches that have occurred recently, that it makes sense to instead have a clear set of standards not just for notification but for information security as well,” Waltzman said.

However, the path to getting data breach and security legislation, such as the trio of bills floated by various senators in January 2014, is unlikely to be a smooth one, attorneys noted.

A major sticking point will likely be the question of what to do with the existing state breach notification and security laws on the books, and whether a federal law should preempt more stringent requirements currently enforced by some states.

“The states together have more enforcement power, many oppose preempting state laws in this area, and there is no consensus over certain important issues, like whether civil remedies should be provided or what role the government should play in enforcing the law,” said Al Saikali, the co-chair of Shook Hardy & Bacon LLP’s data security and privacy group.

Efforts may also be stymied over how specific the data security standards that lawmakers draw up should be, with requirements that are too granular running the risk of being difficult for all companies to adopt and unable to adjust to hackers' rapidly evolving tactics.

“Part of the challenge is that you want to have a degree of flexibility for companies to be able to adopt security standards based on the nature of the information, its use of the data and the size of the organization,” Waltzman said.

With the challenges that are likely to pop up at the federal level, attorneys say they will also be keeping a close eye on states' activity. In 2014, states including California and Florida made changes to their breach notification laws that expanded the definition of personal information to include login credentials and to require breached entities to furnish credit monitoring services, and attorneys will be interested to see if other states follow suit.

“Because hackers are becoming more sophisticated, now data not covered by past regulations such as email addresses are of huge value to hackers, so it wouldn't be surprising to see state laws tweaked going forward to be even more restrictive in terms of what type of information is considered private,” Fran Goins, head of the data security practice at Ulmer & Berne LLP, said.

Cybersecurity Legislation

Legislation to tackle mounting cybersecurity threats — which impact not only consumer data but also corporate data like the type lifted from Sony Corp. in a recent cyberattack — has faced a similar fate to efforts to tighten data security protections in recent years.

Efforts to craft a framework that would make it easier for companies and the government to exchange data on cybersecurity threats appear to have the most momentum in Congress. The House in April 2013 passed a cybersecurity bill designed to encourage the government and private companies to share

information about cyberthreats, but a similar bill that garnered bipartisan support in the Senate — S. 2588, the Cybersecurity Information Sharing Act — failed to emerge from the chamber.

“There were some concerns over the privacy implications of a voluntary information-sharing regime, but it seemed as though Congress was very close to a deal, so I think that a deal is extremely doable in the next Congress,” Waltzman said.

While industries such as the banking sector have had information-sharing arrangements in place for years and retailers recently launched their own initiative to boost coordination following the recent spate of attacks that have tarted their businesses, a federal standard would allow for more cross-sector sharing of data, which could help companies more quickly identify threats and catch up with hackers.

“Because the attacks are becoming increasingly difficult to prevent, how fast a company is able to respond and shut down an attack is key, because that means the hackers are doing a lot of work but not getting a lot back,” Zick said.

However, while there is broad consensus on the need for better information-sharing procedures, disagreements are likely to persist over how to ensure that extraneous personal information is not being shared and how far lawmakers should go to shield companies from liability, a point that attorneys and their clients will be closely tracking.

“Companies are very concerned that information-sharing will open them up to a lot of lawsuits,” said Gerald Ferguson, a co-leader of the national privacy and data protection team at BakerHostetler. “A large number of lawsuits have been generated by the self-reporting obligation for companies under breach notification laws, so it's foreseeable that companies that share information on cyberthreats could expose themselves to litigation risks if there is no liability shield.”

EU Data Protection Reform

While the European Union has been mulling a proposal to replace the bloc's current data protection with a uniform and more stringent regulation for nearly three years, attorneys say that 2015 looks as though it will be the year that policymakers finally reach an agreement on the sweeping overhaul.

“Although it is difficult to predict, there are chances that the general data protection regulation, which has been on the table since 2012, will be finally confirmed,” Undine von Diemar, a Munich-based partner at Jones Day, said. “And if this happens, it will change the privacy regulations for companies significantly.”

As currently drafted, the new regulation would not only tighten restrictions on the use and flow of data held by companies in the EU and abroad that serve the bloc's residents, but also subject these businesses to fines of up to 5 percent of their annual revenue.

“The EU data protection legislative reform is a major development of global implications, [as] the new framework is set to provide the most stringent and sophisticated set of comprehensive rules ever adopted,” said Hogan Lovells partner Eduardo Ustaran, who is based in London.

While the European Commission and Parliament have already backed the legislative proposal, efforts have been held up at the European Council, which has struggled to reach a consensus on controversial provisions such as the one-stop-shop mechanism that would allow multinational companies to deal with

only one lead privacy regulator.

However, the justice ministers that make up the council in December made progress on several outstanding issues, and chances are high that the regulation will finally be adopted and published in 2015, which would set off a two-year reprieve before the changes take effect.

“Two years are not much, given the significant changes under the regulation, so companies are still well advised to monitor this development,” von Diemar said.

FCC's Expanding Privacy Role

While the Federal Trade Commission has basically staked its claim as the nation's leading privacy regulator, having brought 50 data security actions during the past decade, the FCC took a surprising foray into the field in 2014 that is likely to carry over into the new year, attorneys say.

In October, the FCC jumped into data security enforcement by revealing plans to hit TerraCom Inc. and YourTel America Inc. with a $10 million fine for allegedly placing the personal data of up to 300,000 consumers at risk by storing Social Security numbers, names, addresses, driver's licenses and other sensitive customer information on unprotected Internet servers that "anyone in the world" could access.

“The FCC through these actions has attempted to significantly expand its privacy and data security authority through enforcement action rather than rulemaking,” Waltzman said. “It's clear now that the commission has a heightened interest in this, so it will be interesting to see in 2015 whether they try to proceed through enforcement actions or adopt new rules.”

The commission's first data security action came on the heels of another significant privacy action in which Verizon Communications Inc. agreed to pay a then-record $7.4 million to resolve the regulator's probe into claims the telecom giant used personal information from nearly 2 million subscribers to target them for advertising without their consent, illustrating that the commission is unlikely to back down from being one of the regulators on the privacy block.

“With the FCC now getting into the game of bringing privacy and data security enforcement actions, the telecom world has to be [on] heightened alert, because there's no longer only one sheriff in town,” McDermott Will & Emery LLP partner Anthony Bongiorno said.

Emerging Tech Meets Regulatory Concerns

In recent years, technological developments such as the growth of devices that have the ability to connect with one another over the Internet and the rising use of consumer-generated health data not covered by federal privacy laws have captured the attention of regulators and lawmakers, and the trend is unlikely to lose steam in 2015, attorneys say.

On the topic of the Internet of Things, the common name for the growing connectivity of everyday devices through digital means, a bipartisan groups of U.S. senators in October called on the leaders of the Commerce Committee to hold a hearing to probe the privacy and data security risks posed by the development, and the FTC held a workshop on the issue in November 2013.

While the attention may not result in legislation at least initially, "a big question to watch will be where

the FTC is going to draw the line on the Internet of Things and if it's going to allow the technology to develop or be more aggressive and step in while it's still developing," Morrison & Foerster LLP partner Andrew Serwin said.

Attorneys expect a similar approach to be taken by lawmakers and regulators to the growing collection of health data that is not covered by federal health privacy laws, which has drawn increased attention in the wake of the rise in the use of wearable fitness devices such as Fitbit and the recent release of Apple Inc.'s Health Kit.

"There is a growing consensus that the regulation gap needs to be filled, but not any consensus on how to fill that gap," Wiley Rein LLP privacy practice chair Kirk Nahra said. "So I would expect in 2015 that there will be a lot of noise on this topic in the form of hearings and white papers while policymakers try to figure out this issue."

--Editing by Emily Kokoll.
