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 2012

By **Allison Grande**

Law360, New York (January 01, 2012, 12:00 AM ET) -- While it is unlikely that comprehensive privacy legislation will pass the U.S. Congress in 2012, bills regulating data breach notification standards and the tracking of children online may still emerge from the pack of more than two dozen pending measures, attorneys say.

And in the regulatory space, attorneys anticipate that new rules governing the protection of health care information and children's online privacy in the U.S. and data protection in the European Union will change the way companies collect and safeguard users' personal information.

Here are some of the measures and regulatory actions that privacy attorneys will be watching in 2012.

## Data Breach Bills

Out of all of the proposed privacy legislation, a data breach notification and security bill seems to be the most likely measure to pass Congress in the upcoming year, according to experts.

“Businesses are crying out for some sort of unified breach notification standard in order to dispense with having to look at 46 different state laws,” Mintz Levin Cohn Ferris Glovsky & Popeo PC member Cynthia Larose said. “Congress might view this issue as the low-hanging fruit and decide to do this instead of taking a broader, more comprehensive approach to privacy regulation, especially since a federal standard would lessen companies' response costs.”

A trio of legislative efforts proposed by Sens. Patrick Leahy, D-Vt.; Richard Blumenthal, D-Conn.; and Dianne Feinstein, D-Calif., appears to have the most momentum in this area, with all three having passed the U.S. Senate Judiciary Committee in September.

Leahy's bill would create a nationwide standard for notifying consumers of data breaches within 60 days, require companies to have programs to prevent breaches and increase penalties for concealing data breaches. Feinstein's bill would create a nationwide standard for notifying consumers of data breaches, and Blumenthal's bill would stiffen penalties for collecting personal data without permission, as well as create a private right of action that would enable citizens to file suit.

"There will be no room left under these bills for taking a business risk and choosing not to notify consumers or regulators about a data breach," Proskauer Rose LLP privacy and data security group head Kristen Mathews said.

The extent to which any final federal law should preempt existing state laws will be a major point of contention, according to attorneys.

"The current framework of 46 different state laws is incredibly inefficient, and if there's one thing our federal government can do here, [it's to] make this a useful statute that creates a uniform way that citizens are notified of breaches if they occur," Dechert LLP partner Timothy Blank said. "If there's no state law preemption, this is just going to be another law layered on top of existing laws."

The Leahy bill is S. 1151, the Personal Data Privacy and Security Act of 2011. The Blumenthal bill is S. 1535, the Personal Data Protection and Breach Accountability Act of 2011. The Feinstein bill is S. 1408, the Data Breach Notification Act.

**Tracking and Geolocation Bills**

Congress is also considering a variety of bills in both houses that would address consumers' fears about having their movements tracked or their travel data collected without their knowledge for purposes they have not authorized.

While most will likely be held up through the election year, a bill introduced by Rep. Ed Markey, D-Mass., that would curb companies' monitoring of kids online and through electronic devices could sneak through the legislature, according to attorneys.

"Regardless of party lines, it's hard to vote against children," Sheppard Mullin Richter & Hampton LLP partner Craig Cardon said. "It makes sense to most people and sounds good practically, but it may be hard to do because you're taking something that involves a passive activity like tracking and requiring companies to contact an individual and establish a relationship to obtain consent, which could lead down a slippery slope."

Congress' failure to regulate tracking activities could spur states to take the issue into their own hands, as they did nearly 10 years ago when they began passing anti-spam measures, Cardon added.

But states' efforts could run into the same challenges as the anti-spam laws, which many courts found to be in violation of the dormant commerce clause of the U.S. constitution because they attempted to regulate interstate commerce, according to Cardon.

Two highly anticipated moves could help break the congressional gridlock and help propel one of the pending bills through the legislative process, attorneys said. Sen. Harry Reid, D-Nev., has said he will release comprehensive cybersecurity legislation aimed at uniting several of these measures in January, while the White House has promised to reveal its position on privacy legislation within the next month or two.

Notable tracking bills include H.R. 1895, the Do Not Track Kids Online Act of 2011, and S. 913, the Do Not Track Online Act of 2011. Notable geolocation bills include H.R. 2168, the Geolocation Privacy and Surveillance Act; S. 1212, the GPS Act; and S. 1223, the Location Privacy Protection Act of 2011.

**COPPA Revisions**

The Federal Trade Commission's anticipated finalization of amendments to its online privacy rule for children will alter the way businesses that cater to children operate by expanding the definition of personal information and creating new obligations for gaining consent, according to attorneys.

The revisions, which were proposed in September and were out for public comment until Dec. 23, provide a much-needed update to the Children's Online Privacy Protection Act rule, which the FTC implemented in 2000 and gives parents control over what personal information websites may collect from children under 13 years old.

The amendments will expand the definition of personal information to include geolocation information and persistent identifiers such as Internet Protocol addresses and tracking cookies used for behavioral advertising.

Although the rule only applies to children, the proposed expansion of this definition could challenge and ultimately uproot the way that consumers and regulators think about personal information for adults as well, according to Morrison & Foerster LLP global privacy and data security group chair Miriam Wugmeister said.

"It would be very difficult to have two different definitions of personal information under federal law," Wugmeister said. "So if a broader definition were to be codified under COPPA, it would have a significant impact on how personal information is defined in all privacy laws."

The rule's potential changes to this definition and traditional mechanisms of gaining parental consent could also extend the range of businesses directly impacted by the rule, Pryor Cashman LLP partner Jeffrey Johnson said.

"The measure will impose new obligations on not just website operators, but also [on] those who serve advertising to drop advertisements that ask for feedback that would be considered personally identifiable information," Johnson said. "It's a reasonable regulation that recognizes the reality of how people view the Internet and the kind of information they share, but it will impose upon a whole industry that hasn't really thought about COPPA compliance before."

## EU Data Protection Overhaul

The European Commission's proposed overhaul of its data protection directive, slated to be unveiled in January, will subject businesses in the member states and abroad to a more unified but more stringent data protection regime, according to attorneys.

"If it's published in its current form, the regulation is going to have enormous ramifications for the way that companies protect data and for enforcement actions," Wugmeister said.

Among a myriad of proposed changes, this revision would replace the EU's current data protection directive, which allows each state to make its own laws, with an immediately enforceable regulation that applies uniformly to all 27 member states, while tightening notification requirements and significantly increasing fines for noncompliance.

"To the extent that privacy regulation becomes much more Brussels-focused, it would be beneficial to the same extent as state law exemption in the U.S., but the workability of these proposed changes is still in doubt," Steptoe & Johnson LLP homeland and national security practice head Stewart Baker said.

Companies in the U.S. and other foreign countries that do business in this region will also have to be mindful of these proposed changes, especially those that concern the cross-border transfer of information and expanded jurisdictional reach of member state regulators.

"European data protection law will be a continued thorn in U.S. companies' side because of the difficulty of complying with the law as written and the enthusiasm that European regulators have for choosing to go after American companies," Baker said.

## FTC Enforcement

While the European Commission is looking to control privacy concerns through regulation, federal regulators in the U.S. will continue to use enforcement actions to crack down on violations related to the rise of social media and other new technology, according to attorneys.

The FTC's settlements with technology giants Facebook Inc., Playdom Inc. and Google Inc. during 2011 over privacy violations suggest that the agency will ramp up its enforcement in the online and mobile realms in 2012.

"These enforcement actions send a message that they are not going to allow new business models to emerge without having some say about how consumer enforcement is done, and that they intend to enforce the same rules of the road in the electronic space as in other spaces," said Andy Serwin, the founding chair of Foley & Lardner LLP's privacy, security and information management practice.

The agency's focus on these privacy issues also reflects an attitudinal shift among consumers about how their information is used and protected in new social media platforms, Davis & Gilbert LLP partner Gary Kibel added.

“With the advent of social media, we’ve become more open to sharing, and people’s reasonable expectation of privacy has changed,” Kibel said. “Now the challenge is to find the right balance between enabling innovation in the technology industry and protecting consumers’ expectation of privacy online, whatever that might be.”

**HITECH Rule Enactment**

The U.S. Department of Health and Human Services’ expected finalization of amended health care privacy regulations under the Health Information Technology for Economic and Clinical Health Act in 2012 will be of particular interest not only to the health care sector, but also to the expanded group of business entities of health care providers that for the first time will be subjected to these regulations, attorneys say.

“It’s sort of a misnomer to think that this regulation just impacts the health care industry; it covers a whole lot of other entities outside health care,” Wiley Rein LLPpartner Kirk Nahra said.

The proposed final rule, which was released in July 2010 and is expected to be implemented in the first quarter of 2012, will not only change the way that companies protect health care information, but will also provide an increased opportunity for the government, especially state attorneys’ general, to do more enforcement, Nahra added.

“It’s kind of surprising that attorneys general haven’t done much with the increased enforcement power that they got under the HITECH statute yet,” Nahra said. “Attorney general enforcement in this area seems appealing, and would help to boost their political profiles.”

--Additional reporting by Erin Fuchs. Editing by Elizabeth Bowen.