



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 Regulation And Legislation To Watch In 2013

By **Allison Grande**

Law360, New York (January 01, 2013, 2:30 PM ET) -- While legislation designed to insulate the nation's critical infrastructure from cyberintrusions and reform outdated electronic information protections may squeak through Congress in 2013, attorneys say most action will likely come from federal and state regulators, who will focus their attention on improving privacy protections in mobile applications, especially those for children.

Following a year in which Congress failed to pass any of the dozens of pending privacy proposals before it, attorneys predict much of the same for 2013, with regulators from the Federal Trade Commission, California and other states left to pick up the slack.

"There's an old saying that 'nature abhors a vacuum,' and a vacuum is being created by congressional inaction," Fox Rothschild LLP partner Scott Vernick told Law360. "This gap or vacuum is going to be filled by those that are in the position to act, which would be the FTC and the state attorneys general, who will continue to take the forefront in privacy enforcement."

Here are some issues that privacy attorneys will be watching in 2013.

Turning Up The Heat on Mobile Privacy

With concerns mounting over the way mobile devices and applications collect and share user data, legislators, regulators and the industry itself are expected to adopt a number of new rules and procedures for the area in 2013, attorneys say.

"The ability of mobile devices to capture and share data like geolocation information has spurred regulators and legislators to act, and there are currently a number of proposals seeking to impose a legal structure on a wide-open playing field," said Lisa Sotto, the head of Hunton & Williams LLP's global privacy and data security practice.

In the legislative realm, the U.S. Senate Judiciary Committee sent the Location Privacy Protection Act, S. 1223, to the full Senate on Dec. 13. The measure, which was authored by Sen. Al Franken, D-Minn., would require companies to obtain mobile device users' consent before collecting or sharing location data.

But despite the progress, committee members on both sides of the aisle have said more work needs to be done before it reaches the Senate floor. They cite industry concerns that the proposed restrictions would stifle innovation and harm the business model used to deliver free apps and services.

The bill also ran up against another initiative of interest, the industry's attempt to create a voluntary code of conduct for mobile app transparency, DLA Piper partner Jim Halpert

noted.

Stakeholders began meeting in July after the White House proposed they sit down and hammer out a compromise. While progress to date has been slow and hampered by disagreements, industry and privacy groups have set a goal to reach a consensus in the first half of 2013.

"If the multistakeholder process succeeds, we will be much more likely to see an increase in mobile apps offering privacy notices and providing short-form notices that are easier for users to understand," Halpert said.

Regulators are also expected to play a role in shaping the privacy practices of mobile applications, especially following the California attorney general's decision to sue Delta Air Lines Inc. on Dec. 6. The complaint alleged the airline had violated the state's Online Privacy Protection Act by failing to post a privacy policy in its "Fly Delta" app.

The action followed warning letters that California Attorney General Kamala Harris sent to Delta and dozens of other mobile application developers and companies on Oct. 30 that gave them 30 days to bring their disclosures into compliance, raising the possibility that regulators may soon file more suits, attorneys noted.

Developers of mobile apps for children will also want to keep an eye on the FTC, which revealed Dec. 10 that it had initiated a number of investigations to dig deeper into the findings of a recent staff report. The review concluded that the mobile app ecosystem was still falling short in disclosing how apps for children are sharing and collecting information.

"If you have a mobile app, you should definitely be paying attention," said Susan Lyon, co-chair of Cooley LLP's privacy practice group.

Changes to Children's Online Privacy

While watching changes in the mobile space, technology companies will also need take care not to overlook sweeping changes coming to the regulation of children's privacy, according to attorneys..

Following more than two years of back and forth with the industry, the FTC released an update to its 12-year-old Children's Online Privacy Protection Act rule Dec. 19. The update will pull more types of personal information and third-party operators under its purview.

Due to the agency's expansion of the definitions of "personal information" and "operator," creators of plug-ins, social networks and other third-party services that knowingly collect personal information from children under 13 will for the first time have to comply with the rule, and all companies subject to the regulation will need to gain parental consent before collecting persistent identifiers and other new forms of personal information.

These revisions have drawn staunch opposition from the industry, which contends the new rule will prevent it from collecting necessary information and impair the ability of some sites to offer content for free.

"The industry, especially sites with mixed-audience content, worry that if they can't continue to collect information that allows them to serve behavioral advertising, then it might be economically impossible for them to continue to exist," Winston & Strawn LLP partner Lisa Thomas said.

Besides enforcement of the rule, which attorneys predict to be aggressive, the coming year could also bring a legal challenge to the commission's bid to expand the definitions under COPPA, Morrison & Foerster LLP partner Reed Freeman noted.

"The comments collected in connection with the rule suggested that the agency may face litigation if it tries to enforce a rule that broadly defines these defining," he said.

Thwarting Cyberattacks

As for legislation to watch for, companies should keep their eyes on long-running efforts to safeguard the nation's banks, transit systems, power plants and other critical infrastructure, which may finally come to fruition in 2013, attorneys say.

Though Senate Republicans in 2012 twice derailed legislation that would have set corporate cybersecurity standards and pushed businesses that operate critical infrastructure to share information with the federal government, attorneys predict the effort is far from dead. The threat of a rumored executive order and a renewed commitment to the issue by Congress make progress likely, they say.

"It's possible that after the administration issues an executive order, that will change the dynamic that stalemated the previous legislation, and Congress will be motivated to address some issues outside the scope of the order," Halpert said.

The bill with the most traction in Senate — the Cybersecurity Act of 2012, S. 3414 — faced opposition from Republicans concerned that the measure would burden companies with unnecessary regulations, while Democrats countered that failing to establish even voluntary cybersecurity practices would render the legislative effort useless.

"It's clear that comprehensive cybersecurity legislation is on the very top of the priority list for President [Barack] Obama and Congress," Dechert LLP partner Tim Blank said. "Given the rhetoric equating a potential breach to a cyber 9/11, we can hope and expect to Congress will actually have a bill to the president sometime before June."

Modernizing E-Privacy

Another legislative proposal that could soon pass Congress is a long-awaited and much-needed reform to protections for government access to electronic communications originally passed in 1986, according to attorneys.

With courts split on how the outdated Electronics Communications Privacy Act applies to modern technologies like cloud storage and cellphones, the Senate Judiciary Committee advanced the bill — H.R. 2741 — to the full Senate on Nov. 29.

The update, which was proposed by Committee Chairman Patrick Leahy, D-Vt., would change the requirement for government access to electronic communications that are opened or in storage for more than 180 days, raising the bar from a subpoena standard to a probable-cause warrant standard.

But Republicans in both the House and Senate — including Senate Judiciary Committee Ranking Member Charles Grassley, R-Iowa, and incoming House Judiciary Committee Chair Bob Goodlatte, R-Va. — have voiced concerns that the heightened standard would hinder the ability of law enforcement and regulators to conduct investigations.

While Congress failed to take further action on the bill in December, both Leahy and Grassley have vowed to work with their colleagues to evaluate the measure and work out a compromise, leaving attorneys hopeful that courts, companies and law enforcement will finally receive clarity on the search standards in 2013.

"ECPA reform is likely to be a significant issue in the coming year," Halpert said. "With Goodlatte pledging to work on this and Grassley interested in it, there is the setting for

movement on the issue.”

European Data Protection Overhaul

Outside the U.S., attorneys will be watching the European Union's efforts to modernize its data protection regime by replacing its existing directive with more uniformed and stringent regulation.

While the proposed reforms won't be finalized in 2013, attorneys will follow the ongoing legislative process in order to track how objections to the stricter data protection and security requirements raised by regulators, companies and other stakeholders will affect the pending measure.

“Since nearly all business is global, the changes will certainly have an impact on U.S. businesses and we will be watching developments there closely,” Mintz Levin Cohn Ferris Glovsky & Popeo PC member Cynthia Larose said.

While the existing data protection directive already has “quite an extraterritorial reach,” the proposed binding regulation, which the commission unveiled in January, would cast an even wider net by exercising jurisdiction over companies that target European consumers, even if they don't have an actual presence in the bloc, U.K.-based Dechert counsel Renzo Marchini noted.

New requirements for companies to employ a dedicated data protection officer, conduct privacy assessments for each new product and report breaches within 24 hours could also prove costly and may negate the savings that the European Commission has said companies would enjoy due to the regulation's harmonization of member-state laws, Marchini added.

“During the first year, a lot of criticism was thrown at the proposal,” he said. “The commission seems serious about negotiating with stakeholders and making revisions, so now we'll see where it goes.”

--Editing by Elizabeth Bowen.

All Content © 2003-2013, Portfolio Media, Inc.