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

Congress Must Pass Cyber Legislation Before Next Attack

Law360, New York (October 31, 2014, 10:29 AM ET) --

Kathleen B. Rice

As the year winds down in Congress, the prospects of passing cyber legislation in the Senate and getting it sent to President Obama for signature seem to be fading once again. Both House Intelligence Committee Chairman Mike Rogers, R-Mich., and Senate Intelligence Committee Vice Chairman Saxby Chambliss, R-Ga., have been making the case that cyberinformation sharing legislation needs to and can get done this year.

Currently, there are two key information sharing bills: the Cyber Intelligence Sharing and Protection Act, which was passed by the House, and the Cybersecurity Information Sharing Act of 2014, which was reported by the Senate Intelligence Committee. Speaking at the Intelligence and National Security Summit in September, Rep. Rogers said bluntly, “We're in this last window. If we don't get this bill done in the lame duck this year, the whole process starts over and I guarantee you it will take another two years to get this done.”

Given that many of the key players on cyber legislation, including Rep. Rogers and Sen. Chambliss, as well as Sens. Jay Rockefeller, D-W.Va., Carl Levin, D-Mich., and Tom Coburn, R-Okla., are retiring from Congress this year, Rogers is probably right. It is likely that any new legislation will have to start over through the committee process next year. For cyber legislation, this process has involved numerous hearings before the relevant House and Senate committees, including Intelligence, Commerce, Homeland Security, Armed Services and Judiciary, and involved the solicitation of comments from industry, privacy groups and government representatives.

Some may wonder what difference it makes whether Congress passes an information sharing bill. More sectors are developing information sharing and analysis centers and are engaging in informal and formal sharing relationships with each other and with the government — all without any protection from lawsuits or open government laws. The U.S. Department of Justice and Federal Trade Commission have issued guidance that some see as resolving concerns about antitrust prosecutions or enforcement in the context of sharing cyberthreat information. So, is there really a need for a bill?

Yes. As James Comey, the Director of the Federal Bureau of Investigation, said at the RSA Cyber Security Conference earlier this year, private sector companies are the “primary victims of the evolving cyberthreat,” but with their expertise and the information they have, they are “also the key to defeating

it."[1]

In the wake of high-profile breaches against banks, retailers and health care providers, some companies are proactively trying to get ahead of the threat, including by doing more to share the cyberthreat and technical information they have that might be useful to others in industry and the federal government. These companies recognize that having the right information at the right time is critical to detecting, deterring, preventing or mitigating a cyberthreat. But they also recognize the legal risk they are accepting by exchanging such information.

Currently, there are no clear liability protections and exemptions from federal and state antitrust and open government laws that would incentivize reluctant companies to move off the sidelines and fully share information about their own breaches or vulnerabilities. The DOJ and FTC's jointly issued guidance is just that — guidance, and its conclusion that "properly designed sharing of cyber threat information should not raise antitrust concerns"[2] still leaves room for an antitrust prosecution or enforcement action.

In addition, the guidance has no impact on private antitrust litigation or state enforcement. And without explicit federal statutory exemptions that also preempt state law, companies that share proprietary, employee or customer information in confidence with state and federal governments could potentially see that same information subject to release under the Freedom of Information Act and comparable state laws. Given these legal risks, the only real incentive for sharing seems to be a desire to do the right thing. But, when faced with potential litigation and questions from shareholders, boards of directors and customers, wanting to do the right thing is not a great legal defense.

The lack of clarity stemming from the continued failure of Congress to pass information sharing legislation means that companies wanting to share threat information will most likely seek legal advice before any information is ever shared. Yet, in an environment of growing cyber incidents and threats, effectively forcing companies to seek out legal advice before sharing timely information is neither practical for confronting fast-moving threats, nor is it good policy.

Companies need laws that provide clarity and certainty — a point that was at the core of CISA and CISPA. Granted, the bills differ significantly in their approaches toward liability and how information will flow to and throughout the government, but the underlying message is the same: if liability protection is provided to the private sector for specific, defined activities, the private sector will be more likely to share — and share timely — the cyberthreat information that can be so useful in identifying, preventing, and mitigating cyberthreats.

Unfortunately, the debate in Congress over information sharing legislation has become entangled in the more controversial debate over the government's data collection and surveillance activities under the Foreign Intelligence Surveillance Act and USA Patriot Act. Privacy groups, motivated by what they learned from the National Security Agency information leaked by Edward Snowden last year, have been actively campaigning to put a halt to, or strongly curtail, the government's FISA activities. And they are finding support for this argument, including within the Obama administration, even as the fight goes on against the Islamic State and other terrorist groups.

Critics of the NSA metadata collection program have insisted that FISA reform be passed first, before any new authority is given to the private sector to share cyberthreat information with the government under a grant of liability protection. This insistence seems to be driven by strong opposition to certain government agencies receiving cyberthreat information directly from the private sector. As can be

expected, companies across sectors have over the years developed their own relationships with different agencies, including the NSA and FBI. These are trusted relationships and many companies — and federal agencies — do not want to lose them or have to start over building new ones. These relationships help the government learn immediately about threats to private networks and they help the private sector receive timely intelligence from the government that might help prevent, defeat or mitigate that threat. At the same time, privacy advocates have expressed concerns that the House bill and the Senate Intelligence Committee bill offer insufficient protection for private information, especially for consumers who do not want their information shared with the NSA. Ironically, some solutions that call for companies to do even more to proactively identify and remove personally identifiable information could actually result in a greater intrusion on privacy.

But, is it reasonable or responsible for cyber legislation to be held hostage in this fight over government surveillance? It's important to remember that both cyber bills are voluntary — they contain no requirement for the private sector to share information with anyone. Moreover, the bills are not a free-for-all to share any information, rather sharing authorities are limited to carefully defined cyber threat information. These facts alone should be enough to separate these bills from the issue of government collection, including court-authorized collection, of foreign intelligence information.

At the Intelligence and National Security Summit, Rogers expressed frustration that the cyber legislation debate has become one over privacy, but having this debate should not become an excuse for inaction in the Senate. There is a path forward, if Senate Majority Leader Harry Reid, D-Nev., chooses to take it.

Given the Obama administration's objections, and concerns on both sides of the aisle in the Senate, CISPA is unlikely to pass the Senate. Thus, it seems that the best path to success would be for the Senate to take up and pass the Senate Intelligence Committee's bill and send it to the House. There could still be a full debate over privacy and other issues, but an agreement could be sought to consider amendments under a 60-vote threshold before any changes would be made to the underlying text. This way the debate could go on, and if there is enough support for specific positions, the bill would change accordingly.

This approach has worked in similar contexts relating to national security legislation and would be appropriate here too. At the end of the day, cyber threat information will get to all the same players: the U.S. Department of Homeland Security, FBI, NSA, U.S. Department of Energy and others. But in the cyber world, giving information directly to the agency best suited to provide assistance relating to a particular threat, whether it is the DHS, NSA or the FBI, can be essential to stopping an attack, identifying the source and preventing large-scale economic loss.

Congress has the opportunity to lead now on this critical national security issue and provide much-needed legal clarity. It would be a mistake to squander this moment and wait to legislate until there is a catastrophic cyberattack. Legislation hurriedly passed in the heat of such a crisis can easily miss its mark. Right now, cyberattacks threaten our safety, steal our intellectual property and cause considerable economic loss.

As Rep. Rogers said, cybersecurity is "the greatest national security threat America is not ready to handle." Whether Congress steps up to the plate and gets the job done remains to be seen, but the window is closing this year, and our nation will continue to bear the consequences of inaction.

—By Kathleen B. Rice, Mary Bono and Robert J. Ehrich, Faegre Baker Daniels LLP

Kathleen Rice is counsel and a senior director in Faegre Baker Daniels' South Bend, Indiana, and Washington, D.C., offices. Before joining the firm, Rice spent nearly 20 years in law enforcement, intelligence and government affairs. Her experience included serving as counsel on the U.S. Senate Select Committee on Intelligence and she was the lead negotiator on cybersecurity information sharing legislation in the Senate during the 112th and 113th Congresses, where she was heavily involved in the passage of legislation relating to the Foreign Intelligence Surveillance Act and USA PATRIOT Act.

Mary Bono is a senior vice president in FaegreBD Consulting's Washington, D.C., and Palo Alto, California, offices. Prior to joining the firm, Bono was a congresswoman who represented California's Inland Empire and Desert Region in the House of Representatives from 1998-2013.

Robert Ehrich is director of FaegreBD Consulting in the firm's Washington, D.C., office. Prior to joining the firm, Ehrich was a military legislative assistant to Sen. Evan Bayh, D-Ind., and designated staff member to the Senate Armed Services Committee, where he advised Sen. Bayh and staff on matters before the committee. In that role, he managed all defense-related appropriations and authorization requests and projects and interacted with officials from the Pentagon as well as the defense industry.

[1] Prepared remarks of James B. Comey, Director of the Federal Bureau of Investigation, at the RSA Cyber Security Conference, Feb. 26, 2014.

[2] Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information, April 10, 2014, p. 9; see also, Letter from Assistant Attorney General William J. Baer to Steven J. Bowers regarding TruSTAR cyber intelligence data-sharing platform, Oct. 2, 2014.
