Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

House Flip To Boost Privacy Policy Push, Interference Probes

By **Allison Grande**

Law360 (November 7, 2018, 11:02 PM EST) -- Efforts to enact federal privacy legislation and to clamp down on foreign cyberattacks and influence campaigns are likely to receive even greater attention after Tuesday's midterm elections, which put Democrats with significant appetites for digging deeper into these issues in charge of key oversight committees in the U.S. House, experts say.

When a newly divided Congress reconvenes in January with Democrats in control of the House for the first time in eight years, lawmakers will be confronted with the same privacy and cybersecurity issues that they've long been grappling with, including whether there should be a federal standard for how companies should be allowed to use and safeguard consumer data and how to curb efforts by foreign entities to disrupt democratic institutions and attack critical infrastructure.

But the new dynamic set up by the split Congress could make these discussions more fruitful than ever before by giving lawmakers common issues to coalesce around, according to experts.

"When there's a divided Congress that's unlikely to be able to move forward with controversial issues such as middle-class tax cuts or reforming health care, then it becomes more likely that lawmakers will seek to address and bring to the fore issues like privacy that have been percolating and have bipartisan agreement," said McGuireWoods Consulting LLP senior adviser Michael Drobac, who heads the government affairs group's emerging technologies team.

Privacy and cybersecurity issues are clearly important to voters: A recent Morning Consult/Politico poll found that pluralities of both Democrats and Republicans were interested in seeing the next Congress make it a top priority to pass measures that better protect consumer data, and lawmakers on both sides of the aisle have proposed data security, breach notification and privacy standards during the past decades.

But while "there's a lot of common ground to work for, the question will be, and what it will come down to is, how high privacy and cybersecurity issues get up in the agenda" of the incoming Congress, said Mayer Brown LLP partner Marcus Christian.

The committee leadership will play a vital role in determining the priority of these issues, and the reputation of the projected heads of the Commerce, Judiciary and Intelligence committees in both chambers bodes well for privacy and cybersecurity concerns being thrust into, and staying in, the spotlight, according to attorneys.

Rep. Frank Pallone, a New Jersey Democrat who is expected to take over the gavel for the House Commerce Committee, "has been incredibly eager to do research and to get information from companies about what privacy practices and safeguards have been put in place for consumers," and Sen. Roger Wicker, R-Miss., who will likely step in as chairman of the Senate Commerce Committee, has similarly shown an interest in making tweaks to the privacy landscape so that companies "are not dealing with a patchwork of privacy laws," Drobac said.

Additionally, Rep. Jerrold Nadler, a New York Democrat expected to take control of the House Judiciary Committee, is likely to display a willingness to discuss how to craft meaningful notice and disclosures regulations that make sense for a broad range of members of the digital ecosystem, according to Drobac.

Pallone, Nadler and Wicker "have shown an affinity and interest in doing a deep dive into what has taken place with the tech industry and how that compares with consumers' expectations, and what needs to be done to address different laws that have been imposed and have been enacted in other states and countries, and they are likely to take leadership on these issues," Drobac said.

Democratic Sen. Maria Cantwell of Washington, who could take over for Commerce Committee ranking member Bill Nelson if he loses his tight re-election race in Florida, could also be influential, given that she's a former tech executive and is likely to be interested in exploring the balance between privacy regulation and business interests, according to Drobac.

And on the foreign interference side, Rep. Adam Schiff, D-Calif., the ranking member of the House Intelligence Committee, is expected to assume leadership of the committee and reopen inquiries into possible Russian interference in the 2016 U.S. presidential election, which is likely to draw renewed attention to foreign espionage and cyberattack efforts, attorneys said.

"The strategies being developed by the federal government with respect to cyber offensive efforts and similar initiatives are likely to get a more critical eye by new leadership that will likely to be willing to ask harder questions about that," said Brian Finch, a partner at Pillsbury Winthrop Shaw Pittman LLP.

The Staying Power of Federal Privacy Legislation

The push to enact a national privacy regime hit a boiling point this past summer, when California enacted the nation's first law to give consumer more access and control over what private companies do with their data.

While the Senate Commerce Committee held a pair of hearings with tech industry representatives and privacy advocates to discuss what a comprehensive privacy regime might look like, no proposal has yet been widely embraced. But that could easily change in the next Congress, even with a divided legislature, experts say.

"The topic in a lot of ways crosses party lines," Finch said.

With civil libertarians on both sides of the aisle, lawmakers might come together to work out a compromise, or the White House may be willing to work with both parties on national privacy legislation, according to Finch.

"What it's likely to come down to is whether this type of legislation empowers states or takes away aggressive privacy laws at the state level," he said.

Craig Albright, vice president of legislative strategy at BSA: The Software Alliance, said he's not expecting significant gridlock on these issues, given that both sides have shown interest in the past on enacting federal privacy legislation, and that it's possible that there may be even more momentum to get this effort across the finish line with Democrats in control of the House.

"There are a lot of House Democrats that have wanted to push for federal legislation for a number of years, and now with the ability to control committees, they have more of an ability to move forward and are in a position to do that," Albright said.

In recent months, a crush of business groups, including BSA, the U.S. Chamber of Commerce and the Internet Association, along with companies such as Google and Microsoft, have been increasingly calling for a federal privacy law to offset the California Consumer Privacy Act, which is set to take effect in January 2020, and the European Union's General Data Protection Regulation, which went live in May.

The groups have released their own blueprints and statements laying out principles they say should underpin any national privacy legislation, and experts say there's no reason to believe that those efforts will cease when the new Congress opens next year.

"Tech giants are likely to continue to try to stay ahead of it because their best bet is to try to shape legislation and the environment rather than to let someone else bring it up and try to fight against it," said Robert Braun, a partner at Jeffer Mangels Butler & Mitchell LLP and co-chair of the firm's cybersecurity and privacy group.

With Democrats in control of the House, it's likely that tech groups will have to "change how they approach the game to cater to the expectations and policy preferences of Democrats," Finch said, although Albright said he doesn't anticipate BSA making any changes to its strategy.

"The change in leadership doesn't change our stance and activities as much as it gives us an opportunity to talk to people," Albright said. "We feel like there's a lot of interest in and a good opportunity to pass legislation that would create one clear federal standard."

But Braun was less confident that this new Congress was going to be the "Congress of cyber."

While there has been broad consensus that the "system is broken," no one has really come to grips with how to fix it, according to Braun, who noted that although the midterms saw many younger representatives being voted into the House, none have emerged as particularly tech-savvy or have made information security an issue.

"So where's the impetus coming from?" Braun said. "The real question is whether there's going to be someone who will want to pick this up."

Renewed Russian Probe to Spark Cyberattack Interest

Another major consequence of the leadership change in the House is likely to be the ascent of Schiff, a vocal critic of the scope of probes into allegations of Russian interference in U.S. affairs, to the House Intelligence Committee.

"For the most part, cybersecurity initiatives have been a bipartisan effort," said Phillips Nizer LLP technology practice group chair Thomas G. Jackson. "That said, we are likely to see renewed efforts geared towards the passage of legislation to increase federal and state defenses against election meddling. The Secure Elections Act had bipartisan support but didn't get very far."

Christian noted that there "certainly appears to be interest in Congress" to look into the evolution of hacking threats from stealing information and trade secrets to meddling in national affairs and compromising national security.

"That's something I would expect members on both sides of the aisle to take seriously," Christian said.

The scope of whatever probe Schiff may authorize is also likely to be crucial to determining whether congressional oversight is enough to address businesses' concerns when it comes to malicious state activity, attorneys say.

"What should end up being the focus is not whether a particular political figure in the U.S. was engaging in bad activity. The real question is what were the outside players doing, how did they get in and what can be done to clamp down on that activity?" Braun said. "That would turn it into an actual helpful evolution rather than just a political exercise."

Social media platforms in particular will need to stay attuned to these efforts, especially after President Donald Trump during a lengthy press conference Wednesday said that he would be open to working with Democrats to regulate social media platforms amid concerns that they unfairly censor conservative voices, an effort that is likely to be further complicated by potential First Amendment issues.

“What’s interesting is that here we are less than 24 hours after the election, and there’s already talk about maybe needing to regulate social media platforms,” said April Doss, a partner at Saul Ewing Arnstein & Lehr LLP who formerly served as senior minority counsel for the Senate Intelligence Committee’s probe of Russian election interference.

“We used to think about privacy as whether someone’s credit card or Social Security number got breached,” Doss added. “But now we’re moving into a more complex way of thinking about privacy that relates to whether or how people are being targeted for viewpoint manipulation based on aggregated data profiles about their interests and online activities, so that’s definitely an area that needs to be watched.”

--Editing by Brian Baresch and Jay Jackson Jr.