Cyber Update
23 January 2019
By Michael Kans

Chairs and Committees Announced

Last week, a number of key Congressional committees named their Democratic and Republican chairs, ranking, members, and full committee rosters. Many of the leaders of the subcommittees with jurisdiction over cybersecurity, data security, and privacy issues were in key positions in the last Congress. However, given the turnover produced by retirements and electoral defeats in the mid-term elections, there will be new players on some committees and subcommittees.

Two weeks ago, the Senate Commerce, Science, and Transportation Committee's new Chairman Roger Wicker (R-MS) announced the Subcommittees and Chairs for the 116th Congress, including a new Security Subcommittee "will address the intersection of economic and national security" and that the other subcommittee jurisdictions have been "reconfigured." Senator Dan Sullivan (R-AK) will chair this new Subcommittee, but Senator Maria Cantwell (D-WA) has not yet named Ranking Members so it is unclear who Sullivan's Democratic counterpart will be.

The House Energy and Commerce Committee announced subcommittee chairs, including those with jurisdiction over cybersecurity, data security, privacy, and other related issues:

- Communications and Technology – Representative Mike Doyle (D-PA)
- Consumer Protection and Commerce – Representative Jan Schakowsky (D-IL)
- Oversight and Investigations – Representative Diana DeGette (D-CO)

In the same press release, the majority announced the full committee rosters on the Democratic side as well.

House Energy and Commerce Republicans followed suit, and named their ranking members and rosters:

- Communications and Technology – Representative Bob Latta (R-OH)
- Consumer Protection and Commerce – Representative Cathy McMorris Rodgers (R-WA)
- Oversight and Investigations – Representative Brett Guthrie (R-KY)

Michael Kans, Esq. | mdk@michaelkanslaw.com | @michael_kans

The Senate Armed Services Committee announced that Senator Mike Rounds (R-SD) will again chair the Cybersecurity Subcommittee while Senator Joe Manchin (D-WV) will replace former Senator Bill Nelson (D-FL) as the Ranking Member. While House Armed Services has not formally designated the next chair of the Emerging Threats and Capabilities Subcommittee, it is likely Representative Jim Langevin (D-RI) will take the gavel given his service as the Ranking Member in the last Congress and leadership on cybersecurity policy in both the military and domestic spheres.

Other committees of jurisdiction have not yet released their subcommittee chairs, ranking members, and subcommittee rosters, including House and Senate Judiciary, House and Senate Homeland Security, and House Oversight and Government Reform.

Rubio Releases Privacy Bill

Last week, Senator Marco Rubio (R-FL) released a bill, the "American Data Dissemination (ADD) Act" (S. 142) that offers a different approach on privacy and technology by using the "Privacy Act of 1974" as a template for regulating those entities providing services on the internet. However, this approach, and other details in the bill, make it a likely non-starter for many House and Senate Democrats, particularly since it would preempt in significant part (if not entirely) the "California Consumer Privacy Act" (AB 375) and other privacy-oriented state statutes. Nonetheless, Rubio is a new entrant to the field of privacy and data security policy and may influence whatever legislation Congress produces.

Like most other data security and privacy bills, the Federal Trade Commission (FTC) would be the agency to enforce the new requirements and would be given jurisdiction over "covered provider[s]" a term defined as "a person that provides a service that uses the internet; and in providing the service…collects records." This definition would encompass most entities doing business over the internet but would seem to exclude data brokers and other entities that buy, sell, collect, or share the personally identifiable information of people. Consumers would be given the right to access the "records" "covered providers" hold on them and then request changes to erroneous information. If the ultimate regulations align with the "Privacy Act of 1974" (5 USC 552a), then there may be significant exemptions that would function to limit consumer access to and control over the information held, used, and shared by businesses.

Rubio's bill takes the unusual step of requiring that the FTC essentially clear its regulations with the House Energy and Commerce Committee and the Senate Commerce, Science, and Transportation Committee. The FTC would be required to submit to Congress "detailed recommendations for privacy requirements that Congress could impose on covered providers that would be substantially similar, to the extent practicable, to the requirements applicable to agencies under the Privacy

Act of 1974." 12-15 months after the FTC submits this report, it would be required to submit to Congress proposed regulations that would similarly make covered entities subject to requirements along the lines of how the Privacy Act of 1974 applies to federal agencies.

The FTC is directed by the legislation to address a number of topics in these regulations, including:

- criteria by which the FTC could exempt certain small covered providers that would otherwise be subject to this bill based on the time an entity has been covered by the ADD Act, its revenues, and the number of people for whom they have records
- establishing a process by which people could request access to a record and possibly have that record deleted if the covered provider elects to do so
- requiring that consumers show that a record is "not accurate, relevant, timely, or complete" (terms to be defined by the FTC) before a covered entity is required to amend a record
- establishing a dispute resolution process like the one for disputes between consumers and credit reporting agencies under the Fair Credit Reporting Act (FCRA) regarding one's credit file
- the establishment of "a code of 'fair information practices', for the secure collection, maintenance, and dissemination of records, with which a covered provider must comply."

These regulations would also be published, presumably for comment from interested parties. However, the bill is silent on whether the FTC would have to use the more extensive Moss-Magnuson rulemaking procedures or the Administrative Procedures Act process, which most agencies utilize. Yet, the drafters of the bill may intend for the FTC to use the process outlined in the bill, meaning a new route by which the FTC would promulgate regulations. In any event, if a statute based on the initial recommendations is not enacted within two years of passage of the ADD Act, then the FTC would be required to promulgate final regulations.

The Privacy Act of 1974 has been criticized by privacy and civil liberties advocates as being inadequate for protecting the privacy of Americans given how exceptions have been utilized by agencies and the arguably out-of-date definitions and concepts in the 45-year-old legislation. Additionally, unlike many Democratic bills, state attorneys general would have no role in enforcing the new regulations or laws.

With respect to enforcement, the FTC could request that a federal court levy civil fines as high as $40,000 per violation as any violations would be considered "a violation of a rule defining an unfair or deceptive act or practice." The bill would exempt HIPAA-covered entities and those regulated under the "Family Educational Rights and Privacy Act of 1974." The FTC is given authority to determine whether the follow-on

statute or regulations put in place under the ADD Act supersede Gramm-Leach-Bliley and the Children's Online Privacy Protection Act (COPPA) in the case of conflicts. However, common carriers are explicitly made subject to the FTC's authority to regulate privacy practices as the agency shares jurisdiction over these companies with the Federal Communications Commission (FCC).

House Passes Quartet of Cyber Bills

In an obvious reverse of course, after pulling the bill the week before last, House Democratic leadership brought the "Federal CIO Authorization Act of 2019" (H.R. 247) back to the floor and the bill passed unanimously. After the bill had been pulled from the floor schedule last week, there was talk that the bill would not come back to the floor until after the shutdown had ended. Clearly, someone in leadership rethought that approach. Sponsors Representatives Will Hurd (R-TX) and Robyn Kelly (D-IL) had introduced the same bill in the last Congress and it passed the House overwhelmingly in December, but the Senate never took up the bill.

H.R. 247 would codify the positions of Chief Information Officer (CIO) and Chief Information Security Officer (CISO), make the positions presidential appointments, require the CIO to report directly to the Office of Management and Budget (OMB) Director, require each agency to submit reports on all IT expenditures to the CIO, and task the CIO with submitting a plan to Congress "for consolidating information technology across the Federal Government…and increasing the use of shared services, including any recommendations for legislative changes that may be necessary to effect the proposal."

There still is not a Senate counterpart bill and even if there were, the ultimate fate of this legislation remains unclear.

The House was also supposed to consider four energy-related cybersecurity bills but these bills were pulled from the floor schedule for January 15:

- The "Enhancing Grid Security through Public-Private Partnerships Act" (H.R. 359), a bill that would require the Department of Energy to work with electric industry stakeholders to undertake a range of activities to foster better cooperation between government and industry in securing the cyber and physical grid infrastructure.
- The "Energy Emergency Leadership Act" (H.R. 362), which would amend the Department of Energy's organic statute requiring the Secretary to task an Assistant Secretary with "[e]nergy emergency and energy security functions" including cybersecurity.
- The "Cyber Sense Act of 2019" (H.R. 360), a bill that would "require the Secretary of Energy to establish a voluntary Cyber Sense program to test the

cybersecurity of products and technologies intended for use in the bulk-power system."

- The "Pipeline and LNG Facility Cybersecurity Preparedness Act" (H.R. 370) would mandate that the Department of Energy "carry out a program relating to physical security and cybersecurity for pipelines and liquefied natural gas facilities."

It is unclear when these bills might be brought to the House floor.

House Republican Committee Members Send Letters To Telecoms

Last week, Republican leadership on the House Energy and Commerce Committee sent letters to Zumingo, Microbilt, T-Mobile, AT&T, Sprint, and Verizon, "requesting information…about the sale and misuse of cell phone geolocation data" according to the their press release. These letters follow a letter sent last week by House Energy and Commerce Committee Chairman Frank Pallone Jr (D-NJ) to the Federal Communications Commission (FCC) regarding the allegations in a *Motherboard* article that "T-Mobile, Sprint, and AT&T are selling access to their customers' location data." Republicans claimed that their "letters seek to increase transparency surrounding how U.S. wireless carriers and third parties are accessing, transferring, storing, and securing customer location information." They also asserted that "[t]he letters also build off letters the committee sent last year to location aggregation companies LocationSmart, Securus Technologies, and 3C Interactive." The letters pose a number of questions to these companies regarding their privacy practices and whether consumers have affirmatively opted into the regime under which their location information is shared or sold with third parties. Republicans have also requested that these companies brief committee staff by January 30, 2019.

Apple CEO Again Calls For U.S. Privacy Statute

In a *TIME* op-ed, Tim Cook, CEO for Apple, called on "Congress to pass comprehensive federal privacy legislation—a landmark package of reforms that protect and empower the consumer." Cook reiterated the four principles he believes should underlie any such legislation:

- First, the right to have personal data minimized.
- Second, the right to knowledge—to know what data is being collected and why.
- Third, the right to access. Companies should make it easy for you to access, correct and delete your personal data.
- And fourth, the right to data security, without which trust is impossible.

Cook pointed to "invisible" privacy violations and secondary markets for consumer data, a so-called "shadow economy," as the biggest threats to privacy. He proposed that the Federal Trade Commission (FTC) be given authority over data brokers:

> Meaningful, comprehensive federal privacy legislation should not only aim to put consumers in control of their data, it should also shine a light on actors trafficking in your data behind the scenes. Some state laws are looking to accomplish just that, but right now there is no federal standard protecting Americans from these practices. That's why we believe the Federal Trade Commission should establish a data-broker clearinghouse, requiring all data brokers to register, enabling consumers to track the transactions that have bundled and sold their data from place to place, and giving users the power to delete their data on demand, freely, easily and online, once and for all.

Last year, in an address to the International Conference of Data Protection and Privacy Commissioners, Cook warned of a "data industrial complex" under which "[o]ur own information, from the everyday to the deeply personal, is being weaponized against us with military efficiency."

Cook's call for legislation aligns Apple to some extent with some large technology companies except that companies like Facebook or Google would likely prefer that any federal legislation strike a different balance between companies that traffic in consumer data and the right of people to control their personal data.