# Cyber Update
# 6 March 2019
# By Michael Kans

## Privacy Hearings

Last week, two key committees in each chamber held hearings on a possible federal data privacy statute with the witnesses at the House hearing being a mix of civil liberties and privacy advocates and business representatives while the Senate hearing consisted mostly of the latter. Members were advised that a national data privacy standard would benefit Americans; however, witnesses and Members differed on how strong this national standard would be and whether it would preempt state laws, like California's. While there is agreement in Washington that federal legislation is needed, beyond having the Federal Trade Commission have expanded power to police privacy, there are many areas of dispute that will need to be reconciled before privacy legislation can move forward. For example, many Republicans seem to favor an enhanced notice and consent regime under which consumers could better understand how and when their personal data is being used and could then make informed decisions. Yet, many Democrats think this model is fundamentally inadequate for protecting privacy considering the practices of those entities collecting, processing, sharing, and selling data, and hence stronger standards for these entities are needed. In any event, neither party is in a position to disregard the others' policy preferences given Democratic control of the House, Republican control of the Senate, and Democratic leverage in the Senate to filibuster.

*House Energy and Commerce*

On February 26, 2019, the Consumer Protection and Commerce Subcommittee of the House Energy and Commerce Committee held a hearing titled "Protecting Consumer Privacy in the Era of Big Data." Before the hearing, the majority staff made available this background memorandum, and their minority counterparts released their memorandum, as well.

The witnesses at this hearing were:

- Color of Change Senior Campaign Director Brandi Collins-Dexter
- Interactive Advertising Bureau (IAB) Executive Vice President for Public Policy Dave Grimaldi
- American Enterprise Institute Visiting Scholar Roslyn Layton, PhD
- Center for Democracy & Technology President and CEO Nuala O'Connor
- Business Roundtable Vice President Denise Zheng



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

Subcommittee Chair Jan Schakowsky (D-IL) noted this was her subcommittee's first hearing of the new Congress and cited a survey showing that more than 80% of Americans were not very confident that their personal data was being held securely by the social media, retail, and travel industries. Moreover, 67% want government to protect them. She said that "[t]here is good reason for consumers' suspicion." Schakowsky stated that "[m]odern technology has made the collection, analysis, sharing, and sale of data both easy and profitable…[and] [p]ersonal information is mined from Americans with little regard for the consequences." In terms of potential legislation, she asserted that "[t]here should be limits on the collection of consumers' data and on the use and sharing of their personal information." Schakowsky stated that "[m]y goal is to develop strong, sensible legislation that provides meaningful protections for consumers while promoting competitive markets and restoring Americans' faith in business and government." She contended that "[r]ules alone are not enough" and the subcommittee would examine the Federal Trade Commission's (FTC) "enforcement actions have done little to curb the worst behavior in data collection and data security." Also, the subcommittee would look at the agency's use of existing authority under Section 5 of the FTC Act, specifically "why the FTC hasn't used its existing suite of tools to the fullest extent."

Subcommittee Ranking Member Cathy McMorris Rogers (R-WA) said she is hopeful the subcommittee "can move forward on a path to a single American approach to privacy, one that is going to protect consumers and individual privacy, one that ensures that consumers continue to benefit from the amazing technology and innovation that has happened in recent years." She detailed the four principles for legislation that support "free markets, consumer choice, innovation and small businesses –the backbone of our economy:"

- One National Standard: The Internet economy is interstate commerce and subject to federal jurisdiction. There is a strong groundswell of support for a federal privacy law that sets a national standard. Many recognize the burdens a patchwork of state laws would create
- Transparency and Accountability: Companies must also be more transparent when explaining their practices. Transparency is critical. When unfair or deceptive practices are identified there should be enforcement and there should be consequences strong enough to improve behavior.
- Improving Data Security: Another area important to this debate is data security. Perfect security doesn't exist online, and companies are bombarded by hackers every second of every day. Our focus should be on incentivizing innovative security solutions and certainty for companies who take reasonable steps to protect data. Otherwise, we risk proscriptive regulations that cannot be updated to keep up with the bad actors' newest tactics.
  Small Businesses: Established bigger companies can navigate a complex and burdensome privacy regime. But millions of dollars in compliance costs aren't



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

doable for startups and small businesses. We have already seen this in Europe, where GDPR has actually helped increase the market shares of the largest tech companies while forcing smaller companies offline with millions of dollars in compliance costs.

Full Committee Chair Frank Pallone Jr (D-NJ) acknowledged that "[w]ithout a doubt, there are positive uses of data…[b]ut in some cases, data use results in discrimination, differential pricing, and even physical harm." He said that "[w]e can no longer rely on a "notice and consent" system built on such unrealistic and unfair foundations." Pallone stated that "we need to look toward comprehensive privacy legislation – legislation that shifts the burden off consumers and puts reasonable responsibility on those profiting from the collection and use of our data."

Full Committee Ranking Member Greg Walden (R-OR) stated that "I believe it is important that we work together toward a bipartisan federal privacy bill that: improves transparency, accountability, and security for consumers; protects innovation and small businesses; and, sets one national standard."

Collins-Dexter articulated the principles she would like to see in federal privacy legislation:

- Stop High-Tech Profiling and the rampant use of digital stop and frisk disproportionately targeted towards communities of color.
  Ensure Fairness in Automated Decisions. Look at the impact of computerized decision making in the areas of employment, health, education and lending.
- Preserve Constitutional Principles. Digital tools, platforms and tracking should not be used to circumvent due process, warrants, or other independent oversight of law enforcement. Government databases must not be allowed to undermine privacy and freedom of association.
- Enhance Individual Control of Personal Information. Individuals should have meaningful, flexible control over how a corporation gathers data from them, and how it uses and shares that data. Non- public information should not be disclosed to the government without judicial process.
- Protect People from Inaccurate Data. Government and corporate databases must allow everyone the ability to ensure the accuracy of personal information that is used to make important decisions about them. This requires disclosure of the underlying data, and the right to correct it when inaccurate.

Grimaldi said "the IAB asks Congress to support a new paradigm that would follow certain basic principles:

- First, in contrast to many existing privacy regimes, a new law should impose clear prohibitions on a range of harmful and unreasonable data collection and use practices specifically identified in the law.

- Second, a new law should distinguish between data practices that pose a threat to consumers and those that do not, rather than taking a broad-brush approach to all data collection and use.
- Third, the law should incentivize strong and enforceable compliance and self-regulatory programs, and thus increase compliance, by creating a rigorous "safe harbor" process in the law.
- And finally, it should reduce consumer and business confusion by preempting the growing patchwork of state privacy laws.

Layton stated that since the implementation of the General Data Protection Regulation (GDPR), large firms have gained market share in the European Union (EU). She asserted that "Congress review the empirical research on privacy and data protection that the Europeans ignored, notably the process for innovation in privacy-enhancing technologies and the primacy of user knowledge as a component of online trust." Layton said that "[t]he US does not need to copy the European Union on data protection…[and] [i]t can fundamentally improve on the GDPR by making a policy that actually works—promoting privacy without destroying prosperity, empowering people to make informed decisions, and ensuring innovators the freedom to invent and improve privacy-enhancing technology."

*Senate Commerce, Science, and Transportation*

On February 27, the Senate Commerce, Science, and Transportation held a hearing titled "Policy Principles for a Federal Data Privacy Framework in the United States" and the witnesses were:

- 21st Century Privacy Coalition Co-Chairman Jon Leibowitz
- Internet Association President and Chief Executive Officer Michael Beckerman
- Retail Industry Leaders Association Chief Operating Officer Brian Dodge
- BSA – The Software Alliance President and Chief Executive Officer Victoria Espinel
- Northeastern University School of Law Professor Dr. Woodrow Hartzog
- Interactive Advertising Bureau Chief Executive Officer Randall Rothenberg

Chairman Roger Wicker (R-MS) asserted that "Congress needs to develop a uniquely American data privacy framework that provides consumers with more transparency, choice, and control over their data…[and] [t]his must be done in a manner that provides for continued investment and innovation, and with the flexibility for U.S. businesses to compete domestically and abroad. Wicker said that "[i]t is clear to me that we need a strong, national privacy law that provides baseline data protections, applies equally to business entities – both online and offline – and is enforced by the nation's top privacy enforcement authority, the Federal Trade Commission.

Wicker said that "I hope our witnesses will address the critical issues that this committee will need to consider in developing a federal data privacy law, including:

- How best to protect consumers' personal data from being used in ways they did not consent to when collected by the stores or websites they visit.
- How to ensure that consumers are presented with simplified notices about what information an organization collects about them, instead of lengthy and confusing privacy notices or terms of use that are often written in legalese and bury an organization's data collection activities.
- How to enhance the FTC's authority and resources in a reasonable way to police privacy violations and take action against bad actors anywhere in the ecosystem.
- How to create a framework that promotes innovation and values the significant contributions of entrepreneurs, start-ups, and small businesses to the U.S. economy;
- How to provide consumers with certainty about their rights to their data – including the right to access, correct, delete, and port their data, while maintaining the integrity of business operations and avoiding unnecessary disruptions to the internet marketplace; and
- How to ensure a United States data privacy law is interoperable with international laws to reduce compliance burdens on U.S. companies with global operations."

Ranking Member Maria Cantwell (D-WA) said that "[i]n May of 2018, the European's General Data Privacy Regulations (GDPR) went into effect, providing the EU and its citizens with an array of new protections from certain types of corporate data practices…[a]nd in addition, the state of California has recently passed the California Consumer Privacy Act (CCPA), which also provided California's citizens with new rights and protections." She said that "[s]o, together the implementation of these two pieces of legislative policy, GDPR and CCPA, have brought new insights to the congressional efforts to pass meaningful privacy and data security laws." Cantwell declared that "[w]hat is clear to me is we cannot pass a weaker federal law at the expense of states." She asserted that "I am certainly open to exploring the possibility of meaningful, comprehensive federal privacy legislation…[and] I want to work with [Wicker] and all the members of this committee, many of which have already introduced various pieces of privacy legislation, for thoughtful discussion about how we come to a resolution on these issues."

Leibowitz said "[w]e strongly believe that Congress needs to enact national privacy legislation that gives consumers statutory rights to control how their personal information is used and shared; provides increased visibility into companies' practices when it comes to managing consumer data; and includes an opt-in consent regime for the use and sharing of customers' sensitive personally identifiable information—including health and financial information, precise geo-location information, social

security numbers, and children's information—consistent with the framework articulated by the FTC in its [2012] Privacy Report." He said that "[t]he recommendations in the Privacy Report, which were lauded by the privacy community for their muscular approach to consumer protection, were based on institutional expertise accrued over decades, through hundreds of cases brought by the FTC against companies to ensure privacy and security of consumer information, as well as from the input of dozens of stakeholders (including businesses, privacy advocates, and academics), and multiple consumer privacy and data security workshops."

Hartzog stated that "I have spent most of my efforts researching [privacy] over the past few years" and have come to focus on "the way our current privacy regime asks too much of people and too little of those entrusted with our data…[and] I make two recommendations for the Committee:

- First, I recommend that lawmakers should resist the traditional approach to data protection, which emphasizes transparency through notice to users and choice through user consent. It passes the risk of online interaction from data collectors onto people under an illusion of protection. This "notice and choice" approach has failed.
- Second, the best path forward is to move beyond traditional procedural regimes towards substantive and robust rules that garner people's trust in entities and establish firm boundaries that companies cannot cross without consequences.

Hartzog stated that "[m]eaningful data privacy reform must do more than merely strengthen commitments to concepts like transparency, consent, and control." He claimed that "[s]econd helpings of "I agree" buttons and turgid, unreadable terms of use would not have prevented the Cambridge Analytica debacle, the epidemic of data breaches, or the harmful decisions and predictions made by wrongfully biased algorithms powered by personal data." Hartzog said that "[n]or will they prevent the problems of manipulation, discrimination, and oppressive surveillance that we face in a future of automation." He asserted that "[l]awmakers should instead create non-waivable robust and substantive duties and data mandates for companies."

## CYBERCOM Reveals Operations Against Russia

Last week, the *Washington Post* quoted "several U.S. officials" who stated that U.S. Cyber Command conducted offensive cyber operations against Russia's Internet Research Agency ahead of the 2018 mid-term elections. Cyber Command's Russia Small Group, an entity of Cyber Command and National Security Agency (NSA) personnel, undertook the operation. The bases for these actions are the still unreleased National Security Presidential Memorandum 13, which streamlined the process for offensive cyber operations, and the FY 2019 National Defense Authorization Act (P.L. 115-232).

These articles expands on the information reported by *The New York Times* in October 2018 regarding U.S. Cyber Command operations, possibly linked to the actions revealed this week, that targeted individual Russian hackers to deter them from interfering with the 2018 election. Allegedly, these hackers were individually informed that the U.S. government was aware of their activities and was tracking them. This piece also quoted unnamed U.S. officials, very likely the leadership at Cyber Command and the National Security Agency (NSA). A *ZDNet* article quoted an Internet Research Agency (IRA) linked news site in Russia as asserting the cyber-attack wiped the hard drives of some of these Russian hackers. However, this news source framed the U.S. attack as a "complete failure" and as a "failed operation." Moreover, it was alleged that U.S. operatives accessed IRA servers in Amazon's Estonia and Sweden data centers. Finally, the October 2018 *New York Times* article was confirmed by the IRA.

This article appeared the same week the House began marking up the "For The People Act" (H.R. 1), a package containing provisions to stiffen federal and state cybersecurity of elections against foreign interference. Moreover, the Financial Services and General Government Subcommittee of the House Appropriations Committee held a hearing titled "Election Security: Ensuring the Integrity of U.S. Election Systems."

Chairman Mike Quigley (D-IL) asserted that "[o]ur election infrastructure remains outdated, low-tech, and nowhere near where it needs to be to prevent future intrusions." He claimed that "[i]n the 2018 elections:

- 41 states used voting machines that were over a decade old and susceptible to cyber-intrusions and system crashes.
- Thirteen states used voting machines that fail to produce a paper ballot or record, leaving them unable to conduct meaningful post-election audits.
- Thirty-four states used electronic pollbooks in at least some polling locations—including six states that used them statewide—which are vulnerable to hackers who can alter or delete voter registration data.

He contended that "[s]ome of these states are taking steps to replace their outdated systems, but they lack the necessary tools and funding…[and] [w]e need to give state and local election officials the tools they need to adequately defend the security of our election system." Quigley said that "[a]fter an eight-year gap in federal funding, the Fiscal Year 2018 Financial Services and General Government Appropriations Act included $380 million for grants to help states fortify and protect election systems. And we saw an overwhelming demand for assistance." He said that "[e]very single state and eligible territory requested grant funding, and the Election Assistance Commission (EAC) has disbursed every single dollar of the $380 million."

Ranking Member Tom Graves (R-GA) noted that the Departments of Homeland Security and Justice and the Office of National Intelligence found no material interference with the 2018 mid-term election. He lauded the efforts of the National Security Agency and U.S. Cyber Command in defending U.S. electoral systems. Graves called for greater information sharing between federal agencies and the state and local governments that conduct elections. He articulated his opposition to a "heavy-handed federal" approach to election security, including greater federal oversight of election security standards or preemption of states roles in conducting elections, a feature of federalism he believes should be perpetuated and protected. Graves also warned against spending more federal funds on election security, calling this a responsibility of the states.

University of Michigan Professor Dr. J. Alex Halderman said "[f]ortunately, we know how to better defend election infrastructure and protect it from cyber-attacks in 2020 and beyond…[and] [t]here are three essential measures:

1. First, we need to replace obsolete and vulnerable voting equipment, such as paperless systems, with optical scanners and paper ballots—a technology that 30 states already use statewide. Paper ballots provide a resilient physical record of the vote that simply can't be compromised by a cyberattack.
2. Second, we need to consistently check that our election results are accurate, by inspecting enough paper ballots to tell whether the computer results from the optical scanners are right. This can be done with what's known as a risk-limiting audit (RLA). Such audits area common-sense quality control. By manually checking a random sample of the ballots, officials can quickly and affordably provide high assurance that the election outcome is correct.
3. Lastly, we need to raise the bar for attacks of all sorts—including both vote tampering and sabotage—by applying cybersecurity best practices to the design of voting equipment and registration systems and to the operation of computer systems at election offices.

The Belfer Center for Science and International Affairs Co-Director Eric Rosenbach stated that "Congress should prioritize" the following actions "to secure our elections before 2020:

1. Bolster domestic defenses and resilience:
    - First, Congress should authorize and appropriate regular, ongoing federal funding focused on improving the security of our elections.
    - Furthermore, Congress should pass a comprehensive national privacy law that protects Americans' personal data and information from abuse by both leading tech firms and nation-state intelligence services in Russia and China.
    - Congress should also immediately pass regulation to ensure that online platforms such as Facebook, Twitter, and YouTube are not used as tools of foreign information operations.

- Additionally, Congress and the federal government should use the various levers at their disposal to improve cyber risk management.
- Finally, the role of the federal government in defending elections is crucial.

2. Develop precise and legal offensive cyber capabilities;
3. Adopt a clear, public deterrence posture.
    - We have to raise the cost of attacks and decrease the benefits that our adversaries seek.
    - Public attribution is the most important component of raising those costs.
    - We need to support our allies and partners too, many of whom face the same threats.

**Warner's Healthcare Cybersecurity Letters**

Senate Intelligence Committee Ranking Member Mark Warner (D-VA) sent letters to a. number of federal agencies, "seeking details on any measures being taken by the federal government to reduce vulnerabilities in the health care sector" according to his press release. Warner stated that he "pointed to apparent gaps in oversight, expressed concern about the impact of cyber-attacks on the health care industry, asked for strategic recommendations, and conveyed his desire to work alongside federal agencies and health care entities to develop strategies that strengthen information security." Warner sent letters to the Food and Drug Administration, Department of Health and Human Services, Centers for Medicare and Medicaid Services, and National Institute of Standards and Technology.

It is unclear whether Warner is looking to gather input to introduce legislation to tighten the current cybersecurity requirements the healthcare sector is subject to under HIPAA and the HITECH Act. It is possible that Warner is looking to drive improvement in cybersecurity across the sector through increased scrutiny on the federal agencies responsible for ensuring that healthcare providers meet the requisite requirements.

Last week, Warner sent similar letters "to major health care entities, including the American Hospital Association, American Medical Association, Virginia Hospital and Healthcare Association, and others," "to seek input on ways to best improve cybersecurity in the health care industry."

Warner asked the agencies the following questions:

1. To date, what proactive steps has your Department/Agency taken to identify and reduce cyber security vulnerabilities in the health care sector?
2. How has your Department/Agency worked to establish an effective national strategy to reduce cybersecurity vulnerabilities in the health care sector?

3. Has your Department/Agency engaged private sector health care stakeholders to solicit input on successful strategies to reduce cybersecurity vulnerabilities in the health care sector? If so, what has been the result of these efforts?
4. Has your Department/Agency worked collaboratively with other federal agencies and stakeholders to establish a federal strategy to reduce cybersecurity vulnerabilities in the health care sector? If so, who has led these efforts and what has been the result?
5. Are there specific federal laws and/or regulations that you would recommend Congress consider changing in order to improve your efforts to combat cyberattacks on health care entities?
6. Are there additional recommendations you would make in establishing a national strategy to improve cybersecurity in the health care sector?

## CA AG and State Senator Release CCPA Update

Early last week, California Attorney General Xavier Becerra and State Senator Hannah-Beth Jackson "legislation to strengthen and clarify the California Consumer Privacy Act (CCPA)." According to their press release, "SB 561 helps improve the workability of the law by clarifying the Attorney General's advisory role in providing general guidance on the law, ensuring a level playing field for businesses that play by the rules, and giving consumers the ability to enforce their new rights under the CCPA in court."

SB 561 would eliminate the requirement that the California Department of Justice must furnish an opinion to a business or other entity with "guidance on how to comply with the provisions" of the CCPA. The legislation would also expand the private right of action available to California residents. Now, they may sue if their rights are violated as opposed to the current statutory language limiting actions to "consumers whose nonencrypted or nonredacted personal information…is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Finally, the bill would remove the current 30-day window in which businesses alerted to CCPA violations can "cure" the noncompliance. SB 561 would allow the Attorney General to sue for an injunction and civil penalties of $2,500 per violation or $7,500 per "intentional violation."

## Other Hearings and Events

"Department of Defense Information Technology, Cybersecurity, and Information Assurance" House Armed Services/ Intelligence and Emerging Threats and Capabilities

"Securing U.S. Surface Transportation from Cyber Attacks" House Homeland Security/ Transportation and Maritime Security

**Further Reading**

"Are you being scanned? How facial recognition technology follows you, even as you shop" – The Guardian
"How Facebook Trains Content Moderators" – Motherboard, "Facebook Grappling With Employee Anger Over Moderator Conditions" – Bloomberg, and "The Trauma Floor" – The Verge
"While Two Nuclear Powers Were On The Brink Of War, A Full-Blown Online Misinformation Battle Was Underway" – BuzzFeed
"Facebook and Telegram Are Hoping to Succeed Where Bitcoin Failed" – The New York Times
"NSA's Joyce outlines how U.S. can disrupt and deter foreign hacking" – cyberscoop



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