May 4, 2023

House Energy & Commerce Subcommittee Examines Gaps in Federal Data Privacy Laws

Last Thursday (April 27), the House Energy and Commerce Committee's Subcommittee on Innovation, Data, and Commerce held a hearing on "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information." The Subcommittee had asked witnesses to review the data privacy jurisdiction and effectiveness of the Federal Trade Commission (FTC) as well as four federal laws: the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA) covering patients' health data, and the Gramm-Leach Bliley Act (GLBA) covering financial data. Those acronyms were referred to frequently throughout the hearing.

Members and witnesses contrasted the limits of these "sector-specific" laws with the comprehensive American Data Privacy and Protection Act (ADPPA) that the committee approved in the previous Congress on a 53-2 vote. That bill would establish a pre-emptive national consumer privacy and data security framework built around limitations for collecting, processing, and transferring individuals' information; obligations for covered entities and service providers; and giving consumers control over their personal information.

- *For more information*: https://energycommerce.house.gov/events/innovation-data-and-commerce-subcommittee-hearing-addressing-america-s-data-privacy-shortfalls-how-a-national-standard-fills-gaps-to-protect-americans-personal-information

Opening statements

Subcommittee Chairman Gus Bilirakis (R-FL): In his statement, Subcommittee Chairman Bilirakis noted that this was the subcommittee's sixth hearing on data privacy in the 118th Congress, including hearings on where the FTC's lines of jurisdiction and authority are, and how that interplays with a comprehensive privacy law; the role of data brokers and the lack of consumer protections over a person's data; and finally the current hearing on "how consumers may not be covered by sector-specific laws in a way that is consistent with their expectations." Bilirakis said the hearing would focus on how "sectoral data privacy regimes" like COPPA, FERPA, HIPAA, and GLBA create "gaps in coverage," and "how these gray areas for Americans also result in risk and uncertainty that businesses could better avoid if we had clear rules of the road. This only gets more complicated as fifty different states move towards their own data privacy laws." Full statement.

Ranking Member Jan Schakowsky (D-IL): In her statement, Subcommittee Ranking Member Schakowsky said, "We've been working in this subcommittee and the full committee for at least five years, talking about how are we going to protect consumers' data, and rather than things getting better -- despite our being able to pass it out of the full committee… I think consumers are increasingly concerned about their inability to protect their private information." She said the sector-focused laws "don't do the full job and don't fill the gaps" in health care and other areas. Compared with when HIPAA was enacted, "now we know that there are all kinds of apps that collect

information, and they share that, even sell that…" With financial data, "We now know that there are retailers… who have plenty of information when we do shopping online, and… that leads back to all of our financial information becoming available." She said the committee had addressed data privacy vulnerabilities by approving the ADPPA last year, "and it is time for us to return to that. If there are things that we still need to do, if we want to continue negotiations on various parts… it's [the ADPPA] that we ought to build on."

Full Committee Chair Cathy McMorris Rodgers (R-WA): In her statement, McMorris Rodgers said the ADPPA included safeguards to ensure activities covered by the sector-specific laws "remain governed by the appropriate state and federal regulators." She said that while the level of innovation and competition that has occurred since those laws were written "is amazing," companies "have developed tools that interact to track Americans both online and offline, and they're using our data to manipulate what we see and what we think. This is especially true for our children." Rodgers said the ADPPA included privacy protections for kids online that are stronger than any existing state or federal standards." Rodgers said the bill's pre-emption language is imperative because "any legislation to protect kids online must be rooted in a comprehensive national standard for data privacy and security, to ensure there are broad protections. As long as there are regulatory gaps, companies will exploit them in order to monetize the data captured and refuse to do more to shield children from bad actors like cyberbullies, sexual predators, drug dealers, and others…" Full Statement

Full Committee Ranking Member Frank Pallone (D-NJ): In his statement, Pallone said the "alphabet soup" of HIPAA, COPPA, FERPA and GLBA has "failed to rein in the collection, use and transfer of Americans' sensitive data…. partly because they were not designed for our modern online economy." Speaking of HIPAA, Pallone said, "Today, health information is no longer confined to the safety of a doctor's filing cabinet. … As a result, some of the most commonly used websites, apps and devices have the green light to mine and use Americans' health information without meaningful limitations." Pallone said the absence of strong protections also threatens Americans' financial information because existing laws "largely do not apply to retailers and online marketplaces. Nor do they provide protection from discriminatory algorithms." Pallone said existing children's privacy laws also "leave vast amounts of children and teens' sensitive information unprotected," citing constraints in FERPA and COPPA. He said the committee's comprehensive ADPPA bill "enshrines Americans' right to privacy in law" and "reins in the overcollection of information by mandating data minimization." Full Statement

Witness Testimony

Morgan Reed, President, ACT, on behalf of the App Association: Reed said that "regardless of the regulatory silo, what our members hear from consumers is loud and clear. They want access to their information, health, education and financial in digital form, and they want to manage it on their smartphone. Moreover, they want all of that to happen in an environment that meets their expectations around privacy and security." Reed stressed three concepts: First, she said expanding HIPAA is a nonstarter, because it is a portability and interoperability regime that is "designed for insurers and providers…. Expanding HIPAA to all entities processing data with any connection to health, like grocery stores… would turn the Office of Civil Rights into a second FTC." Reed said the nation needs a comprehensive privacy bill, but that bill "cannot be an outgrowth of a health record portability law. We need your bill to become law." Second, she said, "We need to ensure that after financial data is passed from a GLBA-covered entity to the consumer, it is treated as sensitive [personally identifiable information] and provide a

risk-based framework so the financial services industry understands where their liability risks are." Finally, on children's privacy, Reed said overlap between existing laws creates "uncertainty for parents, commercial industries and the educational institutions alike. We need to improve clarity and avoid making confusion worse – some data is opt-out under FERPA but opt-in under COPPA. This helps no one." Full Testimony

Donald Codling, Senior Advisor for Cybersecurity and Privacy, REGO Payment Architectures: Codling said, "What we are now experiencing in the financial industry is the convergence of several trends that though individually benign, will collectively cause unnecessary harm to our nation's children." Codling said most "FinTech" companies that provide financial services products to children adhere to the 1999 GLBA, which requires them to offer an opt-out option for sharing their data with non-affiliate parties. Codling said the REGO product is "the only certified COPPA and third-party GDPR-compliant financial platform for families and children of all ages," designed to give banks and credit unions the capacity to provide a secure family banking platform fully integrated with their banks, brands and systems." He said REGO supports enacting comprehensive, bipartisan federal privacy legislation like the ADPPA, which would include "strong data minimization and data security standards and will update privacy laws to protect children." Full Testimony

Edward Britan, Head of Global Privacy, Salesforce Inc: Britan said the U.S. is now one of the few developed nations without a comprehensive data privacy law. "It's not too late for Congress to act. The world has advanced the concepts that the U.S. first introduced," he said. Britan said HIPAA effectively protects data related to health conditions and provision of health care data by plans and providers, "but HIPAA fields cover health-related data that may be collected by non-covered entities, such as through connected devices and online services that monitor and improve health and fitness." Britan said the various state-level efforts "are important and demonstrate the need and demand for comprehensive privacy law, however, one's level of privacy should not depend on their ZIP code." He praised the committee's approval of ADPPA last year, saying that bill would "meaningfully protect privacy, increase trust in industry, and position the U.S. as a world leader on tech issues." Full Testimony

Amelia Vance, Founder and President, Public Interest Privacy Center: Vance said Congress should enact "baseline federal privacy protections for all consumers that include additional protections for children and students that recognize children's unique vulnerabilities." Vance said that existing federal laws don't adequately protect children and students online, and state-level efforts have "primarily created confusion and hampered efforts by schools, districts and parents to protect kids online." Full Testimony

Q&A

Subcommittee Chairman Bilirakis asked the panel to identify some of the ways COPPA does not go far enough to protect kids, and some circumstances where a parent might expect their child's data to be covered, when in reality it isn't. Codling spoke about children's financial data, while Vance told Bilirakis that COPPA is limited to information collected from children, "but there's also confusion about whether COPPA protects information when you have a label of 'family friendly' or 'kid safe.'" Britan said COPPA's greatest shortcoming is that it only protects children under 13, while kids 13 to 18 aren't protected. Reed agreed with the others while adding that "verifiable parental consent has to work for parents. We called it the 'over-the-shoulder test.' If the device has to go over the

shoulder, come back to the parent who has to enter in something, the parent then says, 'You know what, just go to the general audience app.'" Bilirakis then ran Codling through some explanations of how the REGO app works.

Ranking Member Schakowsky asked what kinds of sensitive health data people should avoid giving to health apps. Reed told her that the answer depends on particular platforms and products, and that many of his organization's members abide by state laws and Europe's GDPR law. He said there is a well-known website with portions that are covered by COPPA and HIPAA, but another part of the site "allows people to have discussions about their symptoms and have a sense of community about it. But the information that they're typing into that website is available to be harvested for targeted behavioral advertising. People often are misled… by the names of the product in a way that can allow that data to flow to data brokers in a way that doesn't meet their expectations."

Full Committee Chair Rodgers asked about lessons learned from navigating "this emerging patchwork of laws at the state level… but also the gaps in the other laws?" She also asked if Reed had concerns about the FTC last year announcing a commercial surveillance rulemaking, and if he believed "the FTC by itself has the ability to fill all the gaps created by these current laws." Reed said the FTC does not have that ability; Rodgers then asked if there are heightened risks posed when new AI models are incorporated into products with "reckless transparency methods." Britan told her, "The best way to ensure that AI is built responsibly is comprehensive regulation of data. That's how the U.S. is presently looking at AI and regulating AI, and examining 'generative AI' through the GDPR." He said a comprehensive data privacy law is necessary "so that the U.S. has a voice in how these technologies develop responsibly."

Rep. Robin Kelly (D-IL) asked a series of yes-or-no questions during which Reed agreed when information about cardiovascular health, or a patient's symptoms, or reproductive health are collected by apps or websites, that data is not any less sensitive than when it is collected by a physician. She asked Reed if there is "any good reason why apps, websites and fitness trackers shouldn't be required to safeguard consumers' sensitive health information and treat it with the same care as a physician?" Reed told her the ADPPA "has important factors like intimate data minimization and the right to delete, but when something is in your electronic health record, and you're a physician, it's really important that it not be deleted and the physician have the full totality of your record. So we have to be very careful when we consider who the audience is for the product… You see tools that allow the management of obesity and Type 2 diabetes being absolutely critical to" communities of color. Reed said that while the ADPPA provides key rules of the road, "I want to be careful that we don't suggest that what the doctor gets is covered in the same way, because the physician must know about your condition over time to properly treat you."

Rep. Larry Bucshon (R-IN) said that Reed in his testimony had mentioned cases where non-health information can be used to extrapolate health-related information, and that putting extra restrictions on the latter would limit consumers' access to digital health tools. But he called health data "the most monetizable data in the world…" Bucshon asked, "Would it be feasible to require disclosures from an entity to a consumer, if the entity does use or gather data to extrapolate private health information?" Reed said this was an issue his organization worked on continually, including a member company based in Bucshon's district. "One of the problems we've run into there, as you know, under 'social determinants of health,' you could run into what they do, which is agriculture and food being considered health data… I do think that we have to think about the totality, and then we don't end up with

grocery stores and agriculture technologies" being captured by privacy laws. When Bucshon asked what the biggest challenges are for implementing such a regime, Reed said, "We look at things like [whether the app] doesn't record physiologic data about you. The FDA already explores these questions of collection of physiologic data… But as you know, we have to preserve the ability to do research as well. And whether it's through an [Institutional Review Board] or other methodologies, we need to be very careful about not requiring such extreme data minimization that you can't do the research we need to do."

Rep. Lisa Blunt Rochester (D-DE) noted that Vance's testimony highlighted the issues surrounding manipulative device design practices, often called "dark patterns," that are intended to trick users, including children, into making bad choices. Rochester said she plans to reintroduce the DETOUR Act, which would crack down on deceptive design practices. Rochester asked if Vance believed a comprehensive privacy bill that includes regulations on dark patterns would be a more effective approach than a privacy bill that only protects children? Vance said it "absolutely" would be, "especially since those when they turn 18 go to higher ed and that affects all of their features. So it's essential."

Rep. Tim Walberg (R-MN) said he was extremely concerned about "how common and easy it is for apps to collect, store and sell children's data." Despite existing sector privacy laws, "obviously significant amounts of information about kids are being collected and sold by these tools every day." Reed told him that while he had previously advocated for verifiable parental consent (VPC), "unfortunately, VPC has not taken the world by storm."

Yvette Clark (D-NY) asked Britan how the lack of a clear national standard will impact the United States' ability to lead in data-intensive innovations like generative AI, quantum computing, and smart cities. Britan told her that "regulation is really important for ensuring that these new innovative technologies are released in a responsible manner, because if we release it in a way that that reduces trust, it's virtually impossible to regain that trust. There are important global conversations happening right now, and the U.S. needs to be part of that conversation. And in order for the U.S. to be an effective part of that conversation. We need comprehensive privacy law."

Kathy Castor (D-FL) said she has recently reintroduced her Kids Privacy Act. "I was heartened last session that the committee included portions of the Kids Privacy Act in the ADPPA, but we really need to move forward quickly. And on kids, one of the things that that we aim to do is raise the age. Right now, really it's just kids 12 and under who are protected; is there any reason we shouldn't give all adolescents a fighting chance here and protect their privacy by increasing the age?" Vance said such a change is "absolutely vital. We also need to recognize, though, that teenagers have different needs and are at a different developmental stage."

Castor asked whether ADPPA should include an age-appropriate design code similar to the Europeans' approach. Vance said, "I think it definitely needs to be based on the foundation of a comprehensive consumer privacy law… Obviously, the EU legal landscape versus the U.S. legal landscape is not the same. So there's a lot of details to work out, as California is finding out, but the underlying principles – location off by default, just-in-time notifications, consideration of different age ranges and what is appropriate – all of those protections should be there."

If you have questions, please contact Heather Meade or Heather Bell.

Washington Council Ernst & Young

Washington Council Ernst & Young (WCEY) is a group within Ernst & Young LLP that combines the power of a leading professional services organization with on-the-ground knowledge, personal relationships and attention to detail of a boutique policy firm. We provide our clients with timely, relevant Washington insight and legislative advisory services customized to their needs. To learn more, contact wcey@ey.com.