HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMITTEE ON CONSUMER PROTECTION AND COMMERCE

"Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security"

June 14, 2022 – 10:30 AM

OVERVIEW

On Tuesday, June 14, the House Energy and Commerce Subcommittee on Consumer Protection and Commerce held a hearing entitled "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security." During the hearing, Members and witnesses discussed: algorithms, discrimination, and protections for marginalized communities; enforcement, including FTC authorities, private right of action, preemption, and State Attorneys General; children and teens' protections, including actual knowledge vs. constructive knowledge standards, educational technology and students' data, and opt-out and consent; impacts on small businesses; and data controls, including minimization, sensitive covered data, third party collection and data brokers, compensation, and privacy by design.

On June 3, Chairman Pallone, Ranking Member Rodgers, and Sen. Roger Wicker (R-MS) released a discussion draft of comprehensive national data privacy and security legislation. The "American Data Privacy and Protection Act" (ADPPA) aims to strike a balance on issues critical to comprehensive data privacy policies, including the development of a uniform, national data privacy framework, the creation of a robust set of consumers' data privacy rights, and appropriate enforcement mechanisms.

Please see **here** for the text of the discussion draft, and **here** for the section-by-section.

OPENING STATEMENTS

- Subcommittee Chairwoman Jan Schakowsky (D-IL)
- Subcommittee Ranking Member Gus Bilirakis (R-FL)
- Committee Chairman Frank Pallone (D-NJ)
- Committee Ranking Member Cathy McMorris Rodgers (R-WA)

WITNESS PANEL

- Ms. Caitriona Fitzgerald – Deputy Director, Electronic Privacy Information Center (EPIC)
- Mr. David Brody – Managing Attorney, Digital Justice Initiative, Lawyers' Committee for Civil Rights Under Law
- Mr. Bertram Lee – Senior Policy Council, Data Decision Making and Artificial Intelligence, Future of Privacy Forum
- Ms. Jolina Cuaresma – Senior Counsel, Privacy and Technology Policy, Common Sense Media
- Mr. John Miller – Senior Vice President of Policy and General Counsel, Information Technology Industry Council (ITI)
- Mr. Graham Dufault – Senior Director for Public Policy, ACT, The App Association
- Mr. Doug Kantor – General Counsel, National Association of Convenience Stores (NACS)
- Ms. Maureen K. Ohlhausen – Co-Chair, 21st Century Privacy Coalition

QUESTION AND ANSWER SUMMARY

Algorithms, Discrimination, and Protections for Marginalized Communities

Chairwoman Schakowsky requested Mr. Lee elaborate on protections for children and marginalized communities included in the proposed bill. Mr. Lee explained the bill would make the internet safer for marginalized communities by prohibiting discriminatory practices and mandating algorithm impact assessments for large data holders. He asserted entities do not fully understand the impacts their processes have on communities, and emphasized the importance of considering civil rights when examining impacts. Mr. Lee noted identity theft predominantly impacts marginalized communities and explained how data minimization could play a key role in improving this. Mr. Lee added marginalized communities were not considered when algorithms were designed, leading to deleterious effects on many communities.

Chairman Pallone asked how the civil rights protections included in the ADPPA will protect against discrimination online. Mr. Brody explained the bill includes an anti-discrimination provision, which prohibits covered entities from processing personal data in a manner discriminating in the provision of goods and services on the basis of protected characteristics. He also highlighted the bill's robust algorithmic assessment requirements, which require companies to assess their systems to test for disparate impacts on protected characteristics or impeded access to services such as housing, jobs, or credit. Mr. Brody added the proposal requires covered entities to evaluate the design of algorithms before they are deployed. He argued this is key to ensuring the public is not treated as test subjects, and algorithms are safe and effective before they result in negative outcomes.

Rep. Bobby Rush (D-IL) raised concerns tech companies abuse the current system to violate civil rights laws, while Congress has failed to rectify the issue. He argued algorithms are used to discriminate against marginalized communities, and inquired how the proposed legislation will address the problem. Mr. Brody recognized algorithmic discrimination is not a new issue, noting redlining is a type of discriminatory algorithm used in the past to create inequities. He explained data collected from these inequities is now used by social media companies to make decisions. Mr. Brody argued algorithms are trained by data collected from society, and contended if societal data is infected with bias, it will produce reflective discriminatory impacts.

Rep. Jerry McNerney (D-CA) expressed support for the continued development of artificial intelligence (AI) to address societal challenges, but recognized the need for impact assessments to identify how AI may harm consumers. He inquired if the mandated algorithm impact assessments in the ADPPA would capture the negative effects of AI. Mr. Lee agreed the impact assessments would effectively identify harms caused by AI. He argued the EU AI Act and algorithmic assessments included in the ADPPA have acknowledged the need to examine the global impact of AI, particularly on high-risk individuals. Mr. Lee explained there is an overlap of protected categories in the EU Convention on Human Rights, US civil rights laws, and the EU

AI Act, which provides broad coverage and analysis of an algorithm's lifecycle and a better understanding of how AI might impact consumers' lives.

Rep. Debbie Lesko (R-AZ) reported her constituents often share concerns algorithms may be used to discriminate against individuals on the basis of political viewpoints. She questioned if political viewpoints should be added to the list of categories examined in the ADPPA's mandated algorithm impact assessments. Mr. Lee acknowledged there may be First Amendment concerns with respect to including political class as a protected category.

Rep. Yvette Clarke (D-NY) noted the algorithm impact assessment requirements include mandates to evaluate algorithms during initial design phases to scan for potential harmful impacts, and require consultation with independent auditors and researchers. She asked why algorithm design evaluations are crucial to protect consumers from discriminatory uses of data. Mr. Lee argued many systems and datasets are often based on a historical concept of discrimination, and explained as a result, data for automated processes such as examining resumes or issuing loans are not necessarily representative of America's full diverse capacity. He contended algorithm design assessments could analyze the potential negative impacts of historical data on marginalized communities and identify ways to avoid those impacts. Rep. Clarke questioned why external researchers and auditors are essential, as opposed to internal company auditors. Mr. Lee argued independent actors could help ensure businesses comply with assessments.

Rep. Tim Walberg (R-MI) noted the ADPPA would prohibit targeted advertising to any individual under 17, and asked how this prohibition could impact children's mental health. Ms. Fitzgerald argued children have less developed critical thinking skills and often cannot distinguish between advertisements and non-commercial content. She asserted the ban is necessary to protect them as they develop skills.

Enforcement

Chairwoman Schakowsky inquired how enforcement mechanisms in the bill would ensure consumers are protected. Mr. Brody explained the bill empowers the Federal Trade Commission (FTC) with a range of new authorities and establishes a new privacy bureau and children's division. He also highlighted provisions empowering State Attorneys General (AGs) with the authority to enforce the law. Mr. Brody commended these provisions, arguing State officials have stronger connections to their community, and can fill gaps where the FTC may not have visibility. Mr. Brody also noted the bill includes a private right of action. He explained State AGs and the FTC may not always have the capacity to address every harm, and expressed support for individuals' ability to go to court and seek relief.

FTC Authorities

Ranking Member Bilirakis requested insight on the proposed Office of Business Mentorship at the FTC, which would be established under the ADPPA. He asked how the new Office will allow for a greater understanding of requirements and compliance for covered entities. Ms. Ohlhausen explained the FTC has a long history of engaging with education efforts, and argued the new Office is a positive investment. She contended all entities will benefit from a comprehensive understanding of requirements, including the FTC, as it will not need to expend as many resources on enforcement.

Ranking Member Rodgers noted the ADPPA moves several Federal Communications Commission (FCC) authorities to the FTC to create more parity for online services. She argued, however, it stops short on categories for video and phone services. Ranking Member Rodgers asserted a dual regulatory regime on these categories between the FTC and FCC does not make sense, and inquired about the consequences. Ms. Ohlhausen explained consumers do not pay close attention to legacy regulations, and do not recognize a difference between traditional voice systems and new innovations, while companies continue to collect the same type of information. She stressed the importance of consistent protections for all services, with the same regulator in place. Specifically regarding video services, Ms. Ohlhausen noted there are strong, balanced protections included in the Cable Act, the Satellite Act, and the Consuming Communications Act which should be transferred to the FTC to preserve protections and benefits enjoyed.

Rep. Robert Latta (R-OH) highlighted Ms. Ohlhausen's testimony which argued the bill does not preempt the FCC's privacy and data security authority related to voice services. He inquired if this refers to Section 222 of the 1996 FCC Telecommunications Act. Ms. Ohlhausen responded affirmatively, and argued privacy regulations in the FCC Act for voice services should be transferred to the FTC for consistent enforcement.

Rep. Latta inquired about the difference between completed rulemakings and issued guidance at the FTC. Ms. Ohlhausen explained if Congress provides the FTC authority to engage with Administrative Procedure Act (APA) rulemaking, the Commission could issue a rule with enforcement capacity. She noted the FTC also issues guidance, which is the Commission's interpretation of its Organic Unfair and Deceptive Practices Authority. Ms. Ohlhausen explained violating guidance is not subject to a fine, the way violating a rule might be; guidance has more limited redress authority.

Rep. Kathy Castor (D-FL) noted under the Children's Online Privacy Protection Act (COPPA), the actual knowledge standard has been a large loophole for Big Tech companies, and argued there is room for improvement on this issue in the ADPPA draft. Rep. Castor asked how companies have used the current regulatory loophole to avoid age restriction compliance, and how the proposed Youth Division at the FTC might help address the problem. Ms. Cuaresma explained the FTC has limited resources, while Congress has requested they enforce 82 statutes. She argued the Youth Division could address the problem, but only if it is resourced with appropriate expertise and funding.

Rep. McNerney inquired if the ADPPA adequately protects personal data, and if the FTC could define effective encryption standards. Ms. Ohlhausen noted the legislation includes data security protections. She explained the FTC has not traditionally been a technical agency, so it would need to consult external expertise to define encryption standards.

Rep. McNerney noted Section 203 provides the FTC with the rulemaking authority to establish provisions for individual data ownership and controls, including restricting how long companies hold data. He inquired if data deletion standards would be beneficial. Ms. Fitzgerald recognized the bill sets an effective standard for data deletion, and clarifies deletion must mean permanently erasing or modifying to be permanently unreadable. She argued technology changes rapidly, and FTC rulemaking is always beneficial to ensure standards evolve with technology. Rep. McNerney noted it is challenging to identify if data has been deleted in the cloud, and asked if standards could provide additional clarity and guidance. Ms. Fitzgerald agreed.

Rep. Robin Kelly (D-IL) asked about the importance of ensuring privacy policies are accessible to users in different languages. Mr. Brody agreed language accessibility is essential. He argued the FTC's Office of Business Mentorship could play a strong role in assisting businesses with language accessibility for policies, guidelines, and regulations issued by the Commission to ensure broad compliance.

Private Right of Action

Rep. Brett Guthrie (R-KY) inquired about how a limited private right of action might impact small businesses, compared to a more expansive right of action that includes statuary or punitive damages. Mr. Dufault argued a private right of action could create a "sue and settle" business model, such as is the case with patent controls, for example. He explained individuals looking to take advantage of the legal system tend to target small businesses, as they do not typically have legal departments and are more willing to settle. Mr. Dufault acknowledged safeguards should exist, but recommended recalibrating the redress to address larger security and privacy harms. Mr. Kantor agreed the capacity for litigation with decreased safeguards is cause for concern. He noted the private right of action provisions allow for compensatory damages, which include damages such as mental anguish and inconvenience, sometimes used to increase awards.

Preemption

Rep. Fred Upton (R-MI) noted Mr. Kantor testified in favor of preemption of state privacy laws, while recognizing the discussion draft's provisions on the issue require clarification and adjustment. He requested Mr. Kantor further elaborate. Mr. Kantor argued, based on previous courts' interpretation of preemption, the

ADPPA's language will not meet the intended goal of preempting all state privacy legislation, partly due to the many exceptions included in the draft.

Rep. Kelly Armstrong (R-SD) noted Section 404b of the ADPPA details statutes not preempted by the bill, often referred to as anti-preemption. He recognized, however, anti-preemption is underdeveloped in federal courts, leaving several substantive questions. Rep. Kelly inquired if anti-preemption protections for specific state laws will be extended should the state amend the law. Mr. Miller argued clarification is needed to determine whether the ADPPA should preempt laws covered by the provisions of the act, or preempt all laws related to subject matter in the Act. He explained, for example, the Illinois Biometric Privacy Law is covered by provisions in the act, but is preempted, while other laws, such as the Texas Biometric law, are not. Mr. Miller agreed litigation will arise if these questions are not addressed before the bill is enacted.

State Attorneys General

Rep. Kathleen Rice (D-NY) noted the ADPPA includes provisions allowing state agencies to seek relief for consumers harmed by abusive data practices. She questioned what challenges state entities face in pursuing cases against companies without a comprehensive privacy standard. Mr. Brody argued State AGs would play an important role in enforcing the bill and augmenting both the FTC's authority and private rights of action. He noted, however, a lack of transparency into companies' data usage presents a challenge to state entities when bringing cases forward. Mr. Brody contended provisions in the ADPPA on transparency, data access and deletion, and algorithm assessments should provide State AGs with the necessary information to successfully address harms. Rep. Rice asked Mr. Brody to elaborate on additional resources the ADPPA provides State AGs to prosecute cases of data abuse and privacy protection violations. Mr. Brody highlighted enforcement authority to bring actions for any type of violation, and seek injunction for civil penalties and compensatory damages.

Children and Teens' Protections

Chairman Pallone noted in President Biden's State of the Union (SOTU) Address, he discussed protecting children and teens online, and the negative impact of social media companies. Chairman Pallone questioned how the ADPPA will address some of the difficulties for teens using social media. Ms. Cuaresma noted the bill's definition of sensitive covered data includes children under 17. She expressed support for the draft's exclusion of an actual knowledge standard with respect to sensitive data. Ms. Cuaresma added the bill also includes protections for children in the section dedicated to targeted advertising. She noted this section prohibits companies from advertising to children under 17. Ms. Cuaresma argued the actual knowledge standard must be adjusted, but recognized the difficulties determining a user's age.

Actual Knowledge vs. Constructive Knowledge Standards

Ranking Member Bilirakis raised concerns about the methods companies may deploy to collect data to determine users' age, given requirements in the ADPPA specific to underage users. He inquired about the type of information needed to determine age, and about the difference between actual knowledge standards and constructive knowledge standards. Mr. Dufault argued the inclusion of an actual knowledge standard is a reasonable compromise. He explained is it difficult to collect adequate evidence demonstrating whether a company knew of underage users on their platform. He added under COPPA, parents are required to give verified consent for data collection on underage users. To accomplish this, Mr. Dufault explained companies may require users to take tests only an adult could reasonably pass to determine age. He argued this evidence is already difficult to collect, while constructive knowledge standards could exacerbate the problem and create additional evidence requirements. Mr. Dufault recommended first defining what evidence qualifies for knowledge before expanding it. He recognized technology has aided in age determination, as well as parental controls at the platform level, and argued the proposed legislation should align with those innovations.

Rep. Castor inquired how the ADPPA might be improved to better protect minors online. Ms. Cuaresma commended provisions in the ADPPA prohibiting companies from collecting, processing, and sharing data on children under 17, unless a parent provides express consent. She recommended, however, adjusting those standards to cover all minors under 18. Ms. Cuaresma argued harmonizing requirements for minors, as opposed to including specific provisions for those under 13, 17, and 18, would make compliance easier. Ms. Cuaresma contended this is especially important when implementing knowledge standards. She explained current standards allow for too many mistakes, and create unnecessary burdens for covered entities.

Rep. Larry Bucshon (R-IN) inquired if Congress should consider additional guardrails for children's data privacy to assist the Youth Privacy and Marking Division's goals at the FTC. Mr. Dufault recommended considering a stronger standard for actual knowledge. He noted the FTC often struggles to gather the right evidence to enforce the actual knowledge standard, and advocated for improvements to enforcement capacity, especially before moving to consider constructive knowledge instead.

Rep. Walberg inquired about the actual knowledge standard as it functions in COPPA, and why it would be preferred over constructive knowledge. Ms. Ohlhausen explained when COPPA was enacted, an actual knowledge standard was adopted under the presumption websites could appeal to a broad audience. She noted there were concerns about placing obligations on companies based on the assumption children may be part of the audience, and argued the FTC focused on content targeted specifically to children. Ms. Ohlhausen added a subsequent attempt to verify users' age, the Child Online Protection Act (COPA) was struck down on First Amendment issues as being over-inclusive and sweeping into many adults.

Rep. Walberg asked about the different obligations for app developers between constructive and actual knowledge standards. Mr. Dufault explained a constructive knowledge standard would require more data collection to determine age, which could present issues. He added a broader range of services may also be swept into constructive knowledge requirements.

Educational Technology and Students' Data

Rep. Lori Trahan (D-MA) raised concerns about students' data privacy and questioned why the Family Educational Rights and Privacy Act (FERPA) is insufficient to protect students from surveillance software used to predict cheating or monitor engagement. Ms. Fitzgerald argued this problem stems back to the sectoral nature of current privacy laws. She explained FERPA covers educational records, such as attendance, grades, and discipline, but does not cover data collected from websites and apps used in classrooms. Rep. Trahan inquired how provisions in the ADPPA to establish the Youth Privacy and Marketing Division and implement privacy by design and algorithm impact assessments could support the FTC's efforts to protect student data rights. Mr. Fitzgerald stressed the importance of oversight and enforcement to protect privacy. She noted the algorithm impact assessments must be submitted to the FTC, which will provide additional oversight to examine how tools are used in an educational setting. Ms. Fitzgerald recommended adjusting the legislation to be slightly more prescriptive on what is included in those impact assessments.

Rep. Trahan asked how the bill's Youth Division and algorithm impact assessments might provide guidance for educational technology companies. She also inquired if additional provisions, such as an age-appropriate design code, as implemented in the UK, would be beneficial. Ms. Fitzgerald suggested staffing the FTC with experts on youth privacy to offer guidance for educational technology companies. She argued many companies and school districts do not fully understand the volume of data they collect, or the implications of that collection.

Opt-Out and Consent

Rep. Lesko highlighted Section 205b of the bill, which addresses data transfer requirements related to minors. She noted the section states, "a covered entity shall not transfer the covered data of an individual to a third party without affirmative, express consent of the individual, or the individual's parent or guardian if the covered entity has actual knowledge the individual is between the ages of 13 and 17." Rep. Lesko argued this section may need additional clarification, as the section could be interpreted to allow minors to give consent to opt-out. She inquired if Ms. Cuaresma shares these concerns. Ms. Cuaresma agreed the section requires clarification, and argued children should not be able to give consent to opt-out of third party data collection. Ms. Cuaresma also noted the bill does not define minors, but acknowledged there is widespread legal recognition individuals under 18 cannot contract. She argued this ambiguity would eventually need litigation and suggested adjusting the bill before it is passed.

Rep. Darren Soto (D-FL) inquired if the ADPPA leaves out any relevant privacy rights. Ms. Ohlhausen argued the bill is comprehensive and does not leave out major rights. Ms. Cuaresma recommended banning third part advertising to children, given the ambiguity in the opt-out section.

Impacts on Small Businesses

Ranking Member Bilirakis argued there is a difference between children's data received by small businesses and data collected by large platforms, such as TikTok or Instagram. He inquired if collection regulations should be reserved for large companies only. Mr. Kantor argued the bill must work for everyone, but disagreed with segregating regulations by entity size. He contended actual knowledge is an important standard, and noted NACS members should be able to comply if the bill is constructed correctly.

Ranking Member Rodgers argued Congress should learn from some of the mistakes of the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), and their impacts on small businesses. Ranking Member Rodgers questioned how the ADPPA compares to the GDPR in terms of encouraging a competitive environment for startups. Mr. Dufault agreed the US can learn from lessons from the GDPR in two ways. First, Mr. Dufault argued the discussion draft includes more consideration for younger companies. He explained the GDPR includes a blanket ban on data processing unless entities can identify a specific lawful basis. He argued startups must be more flexible to respond to market changes and consumer demands, and data processing can be used to eliminate some uncertainties when addressing those changes. Second, Mr. Dufault highlighted the ADPPA's measures to provide compliance programs for small businesses. He explained compliance programs provide resources for small companies seeking to comply with requirements and compete with larger companies, but may need assistance to do so.

Rep. Guthrie asked how preserving digital advertising and opt-out provisions impacts small businesses. Mr. Miller argued the definition of targeted advertising, combined with sensitive data, is restrictive. He explained the bill, as written, could restrict targeted advertising even from a company to its own digital customers. Mr. Miller noted privacy laws passed in Virginia, Utah, Colorado, and Connecticut provide a different balance, which allows for companies to reasonably advertise to users on their own sites. He added the provisions in the discussion draft impact companies of all sizes.

Rep. Neal Dunn (R-FL) noted many small businesses with limited resources may struggle to comply with complicated privacy regulations. He inquired about the need to ensure comprehensive legislation is clear and consistent, given the differing sizes and sophistication of companies nationwide. Mr. Kantor agreed clarity and consistency are crucial, especially as smaller companies engage with much larger technology companies and service providers to conduct business. He explained a level playing field where legal responsibilities are clear would help ensure liability remains in the correct place.

Rep. Dunn noted the ADPPA includes a financial transaction exemption for small businesses, but raised concerns small businesses may still qualify as large data holders if their business model depends on many small transactions. Mr. Kantor agreed with Rep. Dunn's concerns, and noted some successful corner stores could reasonably serve up to 100,000 customers in a year. He argued without including a payment data exemption, many NACS members could be considered large data holders under the ADPPA. Mr. Kantor, noted, however, there is a small data exception in the bill, which does recognize payment data should be treated differently.

Rep. McNerney noted Mr. Kantor advocated for more distinction between covered entities. He asked how Congress can ensure small businesses are able to implement effective, sufficient data security practices. Mr. Kantor recognized the FTC is instructed in the ADPPA to consider the size of an entity, but noted there are several requirements for data security which may not be appropriate to size. He argued setting specific requirements presents a compliance challenge for small businesses, while also falling short of adequate measures for large companies. Mr. Kantor recommended implementing a “reasonableness standard” to ensure data security requirements fit the size of the company and the amount of data they handle.

Rep. Upton noted Section 203 of the ADPPA would change how third party data can be collected, processed, and used. He inquired what steps small businesses can take to ensure access to data needed to operate, given the proposed changes in the discussion draft. Mr. Kantor highlighted Section 304 of the bill, which provides the FTC the ability to certify authorized compliance programs. He argued compliance programs would be very helpful to small businesses to identify ways they can access data consistent with the law. Mr. Kantor argued the programs will be valuable in both guidance and compliance.

Rep. Rice noted the ADPPA contains exemptions for small and medium-sized covered entities that do not meet specified thresholds for revenue derived from data collection, processing, or transfer. She questioned if this legislation would help level the playing field for small businesses struggling to compete with large companies. Mr. Kantor recognized there are key provisions in the bill to support small businesses, but argued there is still room for improvement. He explained the bill sets statutory requirements for covered entities and service providers to lay out their individual responsibilities. Mr. Kantor argued this is key to ensuring large businesses cannot impose costs by contract. To improve the ADPPA, Mr. Kantor recommended ensuring entities are not liable for others’ activities, while still allowing for reliance on each other’s services.

Data Controls

Minimization

Chairman Pallone noted the proposed bill includes strong data minimization provisions and argued they will be significantly more effective than the current notice and consent regimes. He inquired why data minimization is an important inclusion in any comprehensive data privacy bill. Ms. Fitzgerald asserted data minimization is essential, as it removes the onus from individuals to protect their privacy and requires companies to implement appropriate collection limitation measures. She explained this collection would then better align with consumers’ goals. Chairman Pallone questioned how data minimization is distinguished from notice and consent. Ms. Fitzgerald explained notice and consent does not protect privacy, and instead requires companies to report on their data practices in long disclosures, rather than minimizing the collection and usage of data. She added online services have become central to consumers’ lives, so there is no consumer choice on data usage. Chairman Pallone questioned how the ADPPA’s provisions are more protective of consumers’ data compared to previous efforts. Ms. Fitzgerald argued data minimization provisions set it apart compared to other proposals. She asserted the draft demonstrates privacy should be the default moving forward and goes beyond notice and consent pop-ups.

Rep. Tony Cárdenas (D-CA) noted many apps collect more data than is strictly necessary to function. He highlighted, for example, how Facebook Messenger, designed for messaging and video calls, collects health and fitness data, financial information, and location data. Rep. Cárdenas asked why apps collect unnecessary data, and how the ADPPA aims to address the problem. Mr. Brody argued apps collect an excess of data because it can be monetized, and there are no regulations preventing them from doing so. He explained the ADPPA includes strong data minimization provisions to ensure when consumers use an app, only data necessary for the service is collected. Mr. Brody contended these protections are essential to ensure sensitive information is not abused, either through predatory actors or data breaches.

Sensitive Covered Data

Rep. Latta highlighted Mr. Miller’s testimony, which raised concerns the definition of sensitive covered data in the proposed bill may be too broad. Rep. Latta inquired about the implications of the current definition, and why it should be made narrower. Mr. Miller argued the current provision could be interpreted extremely broadly and prevent many standard online activities. Mr. Miller explained information related to search activity might include identifiers such as IP addresses, and leaving the bill as is could impact users’ ability to adequately use a search engine. For example, Mr. Miller highlighted users may be required to provide consent every time they use search engines. He also contended the current sensitive covered data definition may impact data security. Mr. Miller noted security prevention is not exempt in the bill, and security companies use many data analytics and information related to online activity; they would not be able to conduct those processes under this definition. Mr. Miller argued while the bill includes many robust security protections, other provisions in the bill, such as the sensitive covered data provision, may undermine those protections.

Rep. Lizzie Fletcher (D-TX) asked why health data should be considered sensitive data, and why it is not sufficiently protected by the Health Insurance Portability and Accountability Act (HIPAA) in an online ecosystem. Ms. Fitzgerald explained many consumers assume their privacy is covered by HIPAA, when in many cases it is not, partly due to the sectoral nature of the law. She clarified HIPAA only covers interactions with health providers, and not data collected in apps.

Third Party Data Collection and Data Brokers

Rep. Rush inquired about the importance of curbing third party data collection. Ms. Fitzgerald argued data brokers are "some of the worst offenders in the data space," as they do not have a direct relationship with the individuals whose data they are harvesting. She expressed support for the substantive limits in the proposed bill, which Ms. Fitzgerald argued would curtail the data broker industry. She added a data broker registry would increase transparency in the data broker industry, and expressed support for the establishment of the registry.

Rep. Dunn raised concerns foreign state actors plan to attack the United States' digital system to steal intellectual property and collect Americans' personal data. He noted there is currently no legal requirement for Big Tech companies to report if they transfer or store personal data in China, Russia, Iran, North Korea, or other adversarial nations. Rep. Dunn asked about the importance of ensuring national privacy laws incorporate transparency and require covered entities to report if their data is transferred to state actors. Mr. Miller agreed a provision mandating increased transparency is essential, to both protect against bad actors and keep consumers informed about their data.

Rep. Fletcher raised concerns about the purchase of geolocation data, and how it might be misused. She questioned why heightened restrictions on this category of data are important, especially as it relates to data brokers looking to make a profit. Ms. Fitzgerald argued these issues stem back to users' expectations about their data; she noted consumers expect weather apps to collect location data to provide insight on the weather, and not sell that data to brokers so they can develop online profiles. Ms. Fitzgerald also contended promises about anonymization are misleading.

Compensation

Rep. Greg Pence (R-IN) inquired about opportunities to compensate users in exchange for the data they provide to platforms. Ms. Fitzgerald cautioned against policies where only the wealthy can afford privacy. She raised concerns proposals to compensate users would incentivize lower-income consumers to accept harmful terms and sacrifice data privacy.

Privacy by Design

Rep. Bucshon noted data privacy by design measures have been implemented globally, including in the EU's GDPR. He inquired if these measures have been well received, and if they work effectively for consumers. Mr. Miller argued privacy by design policies have been generally well received by both businesses and advocates. He also noted the concept as it appears in the GDPR has been welcomed. Mr. Miller recognized entities often question how to implement privacy by design, as regulations do not detail implementation in practice. He recommended developing a framework for implementation, similar to the National Institute of Standards and Technology's (NIST) privacy framework.

--

Please click here for the archived hearing.