COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

June 10, 2022

To: Subcommittee on Consumer Protection and Commerce Members and Staff

Fr: Committee on Energy and Commerce Staff

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

On **Tuesday, June 14, 2022, at 10:30 a.m. (EDT), in the John D. Dingell Room, 2123 of the Rayburn House Office Building, and via Cisco Webex online video conferencing**, the Subcommittee on Consumer Protection and Commerce will hold a legislative hearing entitled, "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security."

I. BACKGROUND

A. Current Law

Unlike other global economic powers, such as the European Union and China, the United States does not have a comprehensive, national data privacy standard. The United States instead relies on sector-specific privacy-related federal statutes that establish varying degrees of protection, impose different collection and use limitations on various entities, and provide consumers with varying degrees of individual rights.[1] These laws include the Health Insurance Portability and Accountability Act, which protects information collected by a health care provider;[2] the Family Educational Rights and Privacy Act, which regulates the collection of student data by public school officials and those they designate;[3] the Children's Online Privacy Protection Act of 1998 (COPPA), which covers data for children 12 and under with respect to online services directed to children;[4] the Genetic Information Nondiscrimination Act, which prohibits misuse of genetic data in employment or insurance decisions;[5] and the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, which apply to financial institutions and credit reporting agencies.[6]

---

[1] Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, Seattle University Law Review (Apr. 9, 2019).

[2] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191.

[3] 20 U.S.C. § 1232g.

[4] 15 U.S.C. § 6501, et seq.

[5] Genetic Information Nondiscrimination Act, Pub. L. No. 110-233.

[6] 15 U.S.C. §§ 6801-6809; 15 U.S.C. § 1681 et seq.

Many different types of data and entities are not covered by those or other sector specific laws. To bridge those gaps, the Federal Trade Commission (FTC) must rely on its unfair or deceptive acts or practices authority under section 5 of the FTC Act.[7] This authority is limited to cases in which (i) the agency can prove substantial, unavoidable injury from conduct not outweighed by benefits to consumers or competition; or (ii) companies fail to live up to their own promises regarding data practices, regardless of whether such practices themselves are harmful.[8] Moreover, there is no federal requirement for entities to make any such promises.[9]

The FTC is also limited in the relief it may obtain. The agency lacks first-offense civil penalty authority, and the Supreme Court held last year that the FTC may no longer rely on section 13(b) of the FTC Act to obtain monetary relief for consumers who have been harmed, meaning most consumers cannot have their money returned even when the FTC is able to prove a violation.[10]

A growing number of states have acted to try and fill the federal void. California, Virginia, Colorado, Utah, and Connecticut have passed comprehensive privacy legislation. These state laws materially vary in their scope, protections, obligations, and enforcement mechanisms.[11]

B. The Need for Regulation

The consequence of the current approach to data privacy is that most companies monitor themselves and may generally collect, use, share, or sell data without having to notify the individuals to whom that data pertains. Once that data is in the hands of third parties it may be further sold, combined, and used.[12] The lack of a federal standard is more pronounced in the increasingly digital world. One 2021 study showed that 70 percent of companies increased their collection of personal consumer data despite 86 percent of consumers citing data privacy as a growing concern.[13] Over half of American adults now say they have decided not to use a product or service due to worries over the use of their data.[14]

Online privacy harms are well-documented, including data breaches, providing data to

[7] 15 U.S.C. § 45.

[8] Federal Trade Commission, *FTC Report to Congress on Privacy and Security* (Sept. 13, 2021).

[9] *Id*.

[10] *Id*.; *AMG Capital Mgmt., LLC v. FTC*, 141 U.S. 1341 (2021).

[11] Mayer Brown, *Connecticut Passes Comprehensive Privacy Law: Comparing to Other States* (https://www.mayerbrown.com/en/perspectives-events/publications/2022/05/connecticut-passes-comprehensive-privacy-law-comparing-to-other-state-privacy-laws) (May 11, 2022).

[12] *The State of Consumer Data Privacy Laws in the US (and Why It Matters)*, New York Times (Sept. 6, 2021).

[13] KPMG, *Corporate Data Responsibility: Bridging the Consumer Trust Gap* (Aug. 2021) (https://advisory.kpmg.us/articles/2021/bridging-the-trust-chasm.html).

[14] Pew Research Center, *Half of Americans Have Decided Not to Use a Product or Service Because of Privacy Concerns* ((Apr. 14, 2020) (https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/).

third parties without knowledge, surreptitiously installing tracking software, misleading users about data harvesting, and more.[15] Americans are increasingly distressed by the tradeoff of providing their data in exchange for products and services, with 73 percent now saying this is an "unjustified use" of their information.[16]

As more data is collected on individuals by more products and services necessary for everyday life, the harms from abusive data practices are more pronounced.[17] The coronavirus disease of 2019 (COVID-19) pandemic exacerbated these concerns, particularly for children. One comprehensive study found that 90 percent of remote learning tools recommended by schools tracked students and sent data to advertising companies.[18] Studies consistently show that data is used in ways that disadvantage vulnerable communities and target people of color, often with regard to eligibility for essential products and services such as home loans.[19]

II. SUMMARY OF H.R. ____, THE "AMERICAN DATA PRIVACY AND PROTECTION ACT DISCUSSION DRAFT"

After failed efforts over many decades, the "American Data Privacy and Protection Act" (the Act) is the first bipartisan, bicameral national comprehensive privacy and data security proposal with support from leaders on the House Energy and Commerce Committee and the Senate Commerce, Science, and Transportation Committee. The Act establishes a national standard to protect consumer data privacy, impose common sense obligations on covered entities, and allow for federal, state, and individual enforcement.

A. Types of Data Covered

Covered data is defined broadly to include any information identifying, linked, or reasonably linkable to an individual or device linkable to an individual. Certain covered data such as health, financial, biometric, genetic, and precise geolocation information is considered sensitive and subject to heightened requirements. The FTC may promulgate regulations to specify additional sensitive data categories to account for technological changes.

B. Entities Covered

Covered entities are also broadly defined and include any entity under FTC jurisdiction as well as nonprofits and telecommunications common carriers. Additional distinctions made within the Act apply to service providers, third parties, and third-party collecting entities, but all

[15] *6 Examples of Online Privacy Violation*, Cyber News (Apr. 15, 2020).

[16] *Americans Widely Distrust Facebook, TikTok and Instagram with Their Data, Poll Finds*, Washington Post (Dec. 22, 2021).

[17] *See* note 12.

[18] *Remote Learning Apps Shared Children's Data at a 'Dizzying Scale,'* Washington Post (May 24, 2022).

[19] *See*, e.g., *Disparity in Home Lending Costs Minorities Millions, Research Finds*, CBS News (Nov. 15, 2019).

are still covered entities subject to the Act with specific heightened requirements or unique standards that apply to their individual business models.

The Act imposes additional requirements on large data holders, defined by meeting revenue or data processing thresholds. Large data holders are considered to have a third-party relationship with any entities within the same corporate structure. Finally, the Act exempts from certain requirements those small and medium-sized covered entities that for the prior three years did not derive more than half their revenue from transferring covered data while earning gross annual revenues and collecting or processing the covered data of individuals, other than for processing payments, below specified thresholds. These small businesses that are not third-party collecting entities are eligible to participate in FTC-approved compliance guidelines.

C. Beyond A Notice and Consent Framework

The Act takes a material step forward in privacy regulation in that it does not rely exclusively on the notice and consent regime generally employed by state privacy laws. Covered entities may not collect, process, or transfer covered data beyond what is reasonably necessary, proportionate, and limited to provide specifically requested products and services or communicate with individuals in a manner they reasonably anticipate. This duty applies irrespective of any consent from an individual. Moreover, covered data must be permanently disposed of or deleted once no longer necessary for the purpose for which it was collected, processed, or transferred. The Act further prohibits the violation of specific loyalty duties and the pay for privacy arrangements that can leave low-income families without access to privacy.

The legislation also includes broad anti-discrimination protections to protect consumers irrespective of consent. It also requires large data holders to submit annual algorithmic impact assessments to the FTC that describe steps the entity has taken or will take to mitigate potential harms from algorithms.

Covered entities must also care for and protect consumers' data by maintaining reasonable data security practices and procedures related to their size, complexity, and covered data activities. There are also requirements to assess vulnerabilities, take preventive and corrective action, evaluate systems, provide training to all employees with access to covered data, and designate an officer or employee to maintain and implement their data security practices. The FTC may promulgate rules to establish data security compliance processes.

D. Protection for Kids

Prior to and throughout engaging in any targeted advertising, covered entities must provide individuals with clear and conspicuous means to opt out of such targeting. Targeted advertising is flatly prohibited for any individual under 17 years of age.

The legislation also creates a new Youth Privacy and Marketing Division at the FTC that is responsible for addressing privacy and marketing concerns with respect to children and minors. The division must submit annual reports to Congress and hire staff that includes experts in youth development, data protection, digital advertising, and data analytics regarding children.

Any information related to individuals under 17 is considered sensitive covered data under the Act and therefore subject to heightened restrictions. The risks to those under 17 must be factored into entities' privacy policies, practices, and procedures. Similarly, large data holders must also evaluate their algorithms' unique impacts on children in their algorithm impact assessments. Pre-dispute arbitration agreements and joint action waivers are unenforceable with respect to minors.

E. Individual Data Rights

Under the Act, individuals have the right to access, correct, delete, and export their covered data. Sensitive covered data may not be collected, processed, or transferred to a third party without the individual's express affirmative consent. This consent to transfer data may not be obtained through manipulative means, such as dark patterns. Individuals may opt out of the transfer of any covered data to a third party.

Separately, the FTC must establish an online, public, and searchable registry of registered third-party collecting entities, sometimes called data brokers. Individuals may elect to have all covered data about them held by such entities deleted within 30 days.

The bill also includes a unified opt-out that would be put into place if the FTC finds it feasible. This would allow individuals to exercise that opt-out, as well as the opt-out rights related to targeted advertising and transferring sensitive data to third parties, in a universal fashion that will apply across all covered entities instead of requiring individuals to make these selections with respect to each covered entity. The Act also makes general exceptions to use covered data for limited, specific purposes when the use is necessary, proportionate, and limited to the specific purpose.

F. Transparency and Corporate Obligations

Covered entities must provide privacy policies detailing their activities with respect to covered data in a readily available and understandable manner, including information on where and why covered data is sent, collected, processed, and retained. The policies must also be provided in each language a company operates in. Short-form notices of the covered entity's practices with respect to covered data are also required in some instances.

All covered entities must designate privacy and data security officers to implement privacy and data security programs and ensure ongoing compliance. Large data holders are subject to additional requirements, including annual certifications from their CEO, direct reporting to the CEO, and privacy impact assessments.

G. Enforcement and Relationship to Other Laws

The legislation provides three means of enforcement—the FTC, state attorneys general, and a private right of action. The FTC may obtain civil penalties for all violations of the Act. Any relief the FTC or the Department of Justice obtains enforcing the Act that cannot be

provided directly to harmed individuals will be deposited in a Victims Relief Fund and be available to provide relief to individuals harmed by violations under the Act.

State attorneys general may bring cases pertaining to violations of the Act in federal court for injunctive relief; to obtain damages, penalties, restitution, or other compensation; and to obtain reasonable attorney's fees and other litigation costs. States retain all their existing investigatory and administrative powers under state law.

Starting four years after the Act takes effect, persons or classes of persons may bring a civil action in federal court seeking compensatory damages, injunctive relief, declaratory relief, and reasonable attorney's fees and litigation costs for most provisions of the Act. This right does not apply to data minimization, privacy by design, or data security requirements. Pre-dispute joint action waivers for arbitration or administrative proceedings are precluded in all cases.

To bring a private claim, the FTC and the attorney general where a person resides must be notified of the intent to sue and may take up the case if warranted as an intervenor. Improper demand letters seeking monetary payment that do not include a specified disclaimer will prevent suits from proceeding. For claims in which injunctive relief is sought against a covered entity, the Act provides the covered entity a right to cure the alleged violation.

The Act does not limit existing federal law, except where specified. Covered entities subject to and in compliance with the related requirements of specified federal laws shall be deemed in compliance with the related provisions of the Act only to the extent that covered data is subject to the requirements in the other laws. Insofar as covered entities are providers of [broadband internet access service, satellite carriers, or cable operators,][20] no privacy provisions enforced by the Federal Communications Commission shall apply.

State laws covered by the Act are preempted, other than specified state laws. Those laws include general consumer protection laws; civil rights laws; employee and student privacy protections; data breach notification laws; contract and tort law; certain criminal laws; laws on cyberstalking, cyberbullying, nonconsensual pornography, and sexual harassment; laws addressing certain public, financial, and tax records; facial recognition laws; certain surveillance laws; the Illinois Biometric and Genetic Information Privacy Acts;[21] laws addressing medical information; and the right of individuals to sue for data breaches under California law.[22]

H. FTC Structure and Resources

The Act establishes a new FTC privacy bureau to carry out the Act that is comparable to the current bureaus of consumer protection and competition. The new bureau must be fully operational within a year of enactment and include an office of business mentorship to assist

[20] This language is bracketed in the discussion draft of the Act.

[21] 740 ILCS 14 et seq.; 410 ILCS 513 et seq.

[22] Cal Civ. Code § 1798.150, as amended.

covered entities with compliance. The Act authorizes the FTC to be appropriated the sums necessary to carry out the Act.

III. WITNESSES

The following witnesses have been invited to testify:

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center

David Brody
Managing Attorney, Digital Justice Initiative
Lawyers' Committee for Civil Rights Under Law

Bertram Lee
Senior Policy Counsel, Data Decision Making, and Artificial Intelligence
Future of Privacy Forum

Jolina Cuaresma
Senior Counsel, Privacy & Technology Policy
Common Sense Media

John Miller
Senior Vice President of Policy and General Counsel
Information Technology Industry Council

Graham Dufault
Senior Director for Public Policy
ACT | The App Association

Doug Kantor
General Counsel
National Association of Convenience Stores

Maureen K. Ohlhausen
Co-Chair
21st Century Privacy Coalition