April 25, 2023

TO:	Members, Subcommittee on Innovation, Data, and Commerce
FROM:	Committee Majority Staff
RE:	Hearing Entitled "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information"

I. INTRODUCTION

The Subcommittee on Innovation, Data, and Commerce will hold a hearing on April 27, 2023, at 2:00 p.m. in 2123 Rayburn House Office Building. The hearing is entitled "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information."

II. WITNESSES

1. Morgan Reed, President, ACT | The App Association
2. Donald Codling, Senior Advisor for Cybersecurity and Privacy, REGO Payment Architectures, Inc.
3. Edward Britan, Head of Global Privacy, Salesforce, Inc.
4. Amelia Vance, Founder and President, Public Interest Privacy Center

III. BACKGROUND

In the 21st century, consumer information provides opportunities for businesses to make informed decisions and develop products responsive to customer feedback, and subsequently offer goods and services to consumers. More generally, different types of information facilitate the ability for consumers to make financial decisions, allow medical professionals to treat symptoms and render critical health care, and provide educational institutions ease of moving a child's learning forward.

In each of these instances related to individuals' specific information, sectoral laws protect and limit the purposes for how such information can be collected, used, or shared. Currently, several sectoral laws exist in the United States including:

- The Gramm-Leach Bliley Act (GLBA)[1] establishes requirements for financial institutions whose business of which is engaging in activities that are financial in nature or incidental to such financial activities, as determined by section 4(k) of the Bank Holding Company Act of 1956.[2] Financial institutions can include banks, securities brokers and dealers, insurance underwriters and agents, finance companies, mortgage bankers, and travel agents.[3] Nonpublic personal information includes information: that a consumer provides to a financial institution to obtain a financial product or service from the institution; results from a transaction between the consumer and the institution involving a financial product or service; or a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.[4] Information, including certain financial information that is not collected by an entity covered under the GLBA may not currently be protected under the law.

- The Children's Online Privacy Protection Act (COPPA)[5] prohibits operators of websites or online services directed towards children under the age of 13 from collecting, using, and disclosing information from such children.[6] Information that relates to children 13 and older is not be protected by COPPA.

- The Health Insurance Portability and Accountability Act (HIPAA)[7] establishes standards to protect patient health information, including all medical records and other individual identifiable health information used or disclosed by health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services has adopted standards[8] from being disclosed without the patient's consent or knowledge.[9] Information that relates to an individual's health but is not collected by an entity covered by the Act may not be protected by HIPAA.

- The Family Educational Rights and Privacy Act (FERPA)[10] protects the privacy of certain student education records. Specifically, the law applies to schools that receive funds under an

---

[1] 15 U.S.C. §§ 6801-6809

[2] Federal Deposit Insurance Corporation, FDIC Consumer Compliance Examination Manual – April 2021, available at: https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-1-1.pdf

[3] Id

[4] Id

[5] 15 U.S.C. §§ 6501–6506.

[6] Id

[7] 42 U.S. Code § 1320d–6..

[8] U.S. Department of Health and Human Services, National Institutes of Health , HIPAA Privacy Rule available at: https://privacyruleandresearch.nih.gov/pr_06.asp#:~:text=Covered%20entities%20are%20defined%20in,which%20HHS%20has%20adopted%20standards.

[9] Centers for Disease Control and Prevention, Public Health Professionals Gateway, Health Insurance Portability and Accountability Act of 1996 (HIPAA), available at: https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

[10] 20 U.S.C. § 1232g.

applicable program of the U.S. Department of Education.[11] Most information collected by private educational institutions and information that is collected by a mobile educational application not assigned by an educational institution covered under FERPA may not be protected.

Sectoral privacy laws regulate the collection, use, or sharing of specific types of information and for specific institutions. The gaps established by these laws create confusion for consumers over what expectations they should have, related to the protection and security of their information, when sharing it with an entity. A consumer may reasonably expect that health information collected from a mobile application would be protected under HIPAA, however that may not be the case because "we leave the data largely unprotected, or subject to the commitments made by private companies when we are outside of the HIPAA space."[12] Securing this data left wayside by the gaps in sectoral privacy "falls on Congress, not the Department of Health and Human Services."[13]

Last Congress, Reps. Pallone (D-NJ), Rodgers (R-WA), Schakowsky (D-IL), and Bilirakis (R-FL) introduced H.R. 8152, the "American Data Privacy and Protection Act" (ADPPA) on June 21, 2022, and it subsequently passed out of Committee by a 53-2 vote. The ADPPA is the first bipartisan, bicameral national comprehensive privacy and data security proposal.

ADPPA "aims to fill the gaps that these specific laws have produced overtime. . . ."[14] by establishing a preemptive 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 providing individuals with control with respect to their personal information. The legislation does not supplant the sectoral privacy laws, but ensures that entities regulated under those laws, who are captured under the ADPPA's definition of "covered entity" and collect, process, or transfer personal information defined under the legislation, must abide by the requirements of the ADPPA to give consumers coverage in any gaps that exist in current federal law.

This hearing will provide an opportunity for members to analyze where the gaps in protections for consumers' personal information are, how businesses navigate the compliance of sectoral laws, and why Congress must enact a comprehensive privacy and data security law to fill these gaps.

IV.ISSUES

- What are the types of consumer information that are not protected by different sectoral laws?

---

[11] U.S. Department of Education, Family Educational Rights and Privacy Act (FERPA), available at: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[12] Jessica Davis, *"National data privacy proposal may shape health data not covered by HIPAA"(*September 26, 2022), available at: https://www.scmagazine.com/feature/privacy/national-data-privacy-proposal-may-shape-health-data-not-covered-by-hipaa

[13] Id.

[14] Formiti, "the US Federal Privacy Law The ADPPA Could Be Here Sooner Than Anticipated" (August 8, 2022), available at: https://www.lexology.com/library/detail.aspx?g=fdfb7558-0825-47f7-845c-b98ec33632d5

- How does a gap in the types of information protected under sectoral privacy laws create confusion for businesses trying to comply with sectoral laws?
- How does action at the State level to build upon sectoral protections cause further confusion for Americans and businesses?
- Should regulatory regimes reflect obligations according to the activities they are engaged in, or how the business is primarily defined?
- How do we ensure that definitions across regimes work in unison so as not to cause further confusion?

V.STAFF CONTACTS

• Tim Kurth, Chief Counsel
• Teddy Tanzer, Senior Counsel
• Brannon Rains, Professional Staff Member
• Michael Cameron, Professional Staff Member
• Lacey Strahm, Technology Fellow
• Jessica Herron, Clerk