BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-3641
Minority (202) 225-2927

June 1, 2026

MEMORANDUM

To: Members, Subcommittee on Commerce, Manufacturing, and Trade
From: Committee Majority Staff
Re: Subcommittee on Commerce, Manufacturing, and Trade Hearing on June 3, 2026

I. INTRODUCTION

The Subcommittee on Commerce, Manufacturing, and Trade has scheduled a hearing on June 3, 2026, at 10:15 am in 2123 Rayburn House Office Building. The hearing title is "Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law."

II. WITNESSES

- Tyler R. Bridegan, Partner, Womble Bond Dickinson; Former Director of Privacy and Technology Enforcement, Office of the Texas Attorney General
- Kate Goodloe, Managing Director, Business Software Alliance
- Ashli Watts, President and CEO, Kentucky Chamber of Commerce
- Caitriona Fitzgerald, Deputy Director and Policy Director, EPIC

III. BACKGROUND

The United States (U.S.) is the global leader in the development and use of digital technologies, including artificial intelligence (AI). The collection, use, and sharing of personal data powers these technologies and has driven significant advancements in American life, including greater access to information and modes of communication; new, cheaper, and more convenient consumer goods and services; innovative and resilient small businesses; safer communities; and discoveries in critical areas such as life sciences. The U.S. digital economy

totals $4.9 trillion, or 18 percent of GDP, and supports 28.4 million American jobs.[1] With increased technological competition from foreign adversaries, continued data-driven growth and innovation is essential to American economic and national security.

Although the collection, use, and sharing of personal data yields significant benefits to consumers, commerce, and national security, legal protections for Americans' personal data have not kept pace with technology changes. The U.S. has a long and robust tradition of protecting the privacy of consumers, including common law torts, the Fair Information Practice Principles, and robust sectoral laws protecting financial, health, and student information.[2] Through its authority to police unfair or deceptive practices, the Federal Trade Commission (FTC) has become the nation's leading privacy and data security agency.[3] The U.S., however, lacks a federal comprehensive privacy and data security law and remains the only G20 economy without one.[4]

In the absence of a national standard, U.S. states have enacted their own comprehensive privacy and data security laws. Since the 2018 enactment of the California Consumer Privacy Act (CCPA), 21 additional states have enacted such laws.[5] Today, the U.S. privacy and data security landscape is a complex and ever-shifting web of federal and state mandates, with confusing, uneven protections for consumers. Consider the example of sensitive data. Among the states that have enacted comprehensive laws, a substantial majority require a consumer's opt-in consent to process their sensitive data.[6] In California, however, a consumer's consent is not required to process such data; the CCPA instead grants consumers only a narrow right to restrict its use and disclosure.[7] The protection of sensitive data—typically encapsulating a person's religious beliefs, racial or ethnic origin, mental or physical health diagnosis, among other information—is only one of the areas where a consumer's privacy protections can vary depending on the state in which they reside.

The current fragmentation of state privacy and data security requirements also impedes interstate commerce in ways that disadvantage small businesses and startups and limit competition. A 2022 report found that the cost of fifty state privacy laws could exceed $1 trillion

---

[1] Kiersten Hansen, *IAB Research; IAB Research: Digital Economy Surges to $4.9 Trillion, Fuels 28.4 Million U.S. Jobs Across All 435 Congressional Districts*, IAB (Apr. 30, 2025), https://www.iab.com/news/measuring-digital-economy-2025/.

[2] Cong. Rsch. Serv. R45631, *Data Protection Law: An Overview* (2019), https://www.congress.gov/crs-product/R45631; Cheryl Saniuk-Heinig, *50 Years and Still Kicking: An Examination of FIPPs in Modern Regulation*, Int'l Ass'n of Privacy Professionals (May 25, 2021), https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation; 15 U.S.C. §§ 6801–6809 ; 42 U.S.C. §§ 1320d–1320d-9 ; 20 U.S.C. § 1232g.

[3] *Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited May 26, 2026).

[4] Global Privacy Law and DPA Directory, Int'l Ass'n of Privacy Prof'ls, https://iapp.org/resources/global-privacy-directory?all (last visited May 26, 2026).

[5] David Botero, US State Privacy Legislation Tracker, Int'l Ass'n of Privacy Pro., https://iapp.org/resources/article/us-state-privacy-legislation-tracker (last updated May 18, 2026).

[6] For example: Va. Code § 59.1-578(A)(4); Colo. Rev. Stat. § 6-1-1308(7); Conn. Gen. Stat. § 42-520(a)(4); N.J. Rev. Stat. § 56:8-166.12(a)(4); Ky. Rev. Stat. § 367.3617(1)(e).

[7] California Civil Code § 1798.121.

over a decade, with at least $200 billion of this burden falling on small businesses.[8] According to the nonprofit, Engine, startups invest between $100,000 and $300,000 to establish the infrastructure needed to comply with the existing state landscape and spend an additional $15,000 to $60,000 to assess compliance requirement for each new state law.[9] For context, the average seed-state startup operates on roughly $55,000 per month, meaning compliance with a new state privacy law could consume an entire month of a startup's operating expenses.[10] Large, well-established companies, especially technology companies, can easily absorb these costs by comparison.

There is widespread support for a federal comprehensive privacy and data security law.[11] A January 2026 survey found that 86 percent of voters believe consumer data privacy should be regulated at the federal level.[12] Despite such support, the question of how to structure a federal law has been debated across multiple Congresses.[13] For much of the world, the European Union's General Data Protection Regulation (GDPR) has served as a global benchmark on which to base their privacy and data security frameworks.[14] Proposals in previous Congresses have integrated signature concepts of the GDPR, such as a restrictive approach to data collection, sharing, and use, also known as "substantive data minimization."[15]

The GDPR may serve as a cautionary tale for Congress. Enacted a decade ago, the law continues to burden Europe's digital economy and competitiveness. The GDPR has been found to increase market consolidation among technology vendors and decrease new entrants in the mobile app marketplace.[16] It has raised costs in the EU of commercial activity associated with personal data.[17] Although access to compute is a competitive advantage for companies and entire economies in the digital era, European firms have reduced their data processing when compared

---

[8] Daniel Castro, *50-State Patchwork of Privacy Laws Could Cost $ 1 Trillion More Than a Single Federal Law*, New ITIF Report Finds, Info. Tech. & Innovation Found. (Jan. 24, 2022), https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/.

[9] Engine, *Privacy Patchwork Problem: Costs, Burdens, and Barriers encountered by Startups* (Mar. 2023), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6414a45f5001941e519492ff/1679074400513/Privacy+Patchwork+Problem+Report.pdf.

[10] Alexander Wall, *The Newest Attempt at a Federal Privacy Framework and What It Means for Startups*, Engine (May 14, 2026), https://engineadvocacyfoundation.medium.com/the-newest-attempt-at-a-federal-privacy-framework-and-what-it-means-for-startups-ba72485ee62e.

[11] U.S. Chamber of Commerce et al., *Business Associations Welcome Federal Data Privacy Legislation*, U.S. Chamber of Com. (Apr. 23, 2026).

[12] Morning Consult, *Privacy Preemption on the federal Level: Voter views* (Jan. 2026), https://s3.us-east-1.amazonaws.com/brt.org/2026-04/Privacy+Preemption+Study+Deck_2026.pdf.

[13] American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. (2024); American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[14] Ronan Murphy, *Mapping the Brussels Effect: The GDPR Goes Global*, Ctr. For Eur. Pol'y Analysis (Aug. 7, 2025), https://cepa.org/comprehensive-reports/mapping-the-brussels-effect-the-gdpr-goes-global/.; Ayesha Bhatti, *How the Brussels effect Hinders Innovation in the Global South*, Info Tech. & Innovation Found. (Jan. 26, 2026), https://itif.org/publications/2026/01/26/how-brussels-effect-hinders-innovation-in-global-south/.

[15] Jordan Francis, *Data Minimization's Substantive Turn, Key Questions & Operational Challenges Posed by New State Privacy Legislation* (June 2025), https://fpf.org/wp-content/uploads/2025/06/FPF_Data-Minimization.pdf.

[16] John M. Yun, *A report Card on the Impact of Europe's Privacy Regulation (GDPR) on Digital Markets*, 31 Geo. Mason L. Rev. F. 104, 109 (2024), https://lawreview.gmu.edu/wp-content/uploads/2024/04/Yun-31-Geo.-Mason-L.-Rev.-F.-104-2024.pdf.

[17] *Id*.

to their U.S. peers over the last decade and spend 40 percent of their information technology budgets on compliance.[18] The EU also experienced a decline in new venture deals, including in the healthcare and financial sectors, following the GDPR's enactment.[19] In response, the EU is considering reforms to begin addressing these concerns.

An alternative to the GDPR can be found among the U.S. states that have enacted comprehensive privacy and data security laws.[20] While there are notable differences between states, resulting in the current patchwork of requirements, there are nonetheless commonalities across many of these laws.[21] The core provisions of this "consensus state framework" include consumer rights to access, correct, delete, and transfer their personal data, as well as to opt-out of data sales, targeted advertising, and certain automated decisions. Nearly all states that have enacted comprehensive laws distinguish between "controllers" and "processors" and tailor obligations according to each of these roles.[22] Importantly, these laws impose affirmative data security requirements onto companies and generally require consent before processing sensitive data. The overwhelming majority require controllers to only collect data that is adequate, relevant, and reasonably necessary for a disclosed purpose. Each state law is enforced by a government regulator; none is generally enforceable by a private right of action.

A comprehensive privacy and data security law also intersects with U.S. interests in foreign commerce and national security. The flow of personal data across borders underpins commercial activity across every sector of the economy. The Secretary of Commerce is a longstanding leader of promoting such data flows in a privacy-protective manner, as exemplified by the Global Cross Border Privacy Rule System and the U.S.-EU Data Privacy Framework.[23] Foreign adversaries, including the People's Republic of China, also increasingly seek to access Americans' personal data. In 2024, Congress enacted the *Protecting Americans' Personal Data from Foreign Adversaries Act* to address these risks with respect to data brokers.[24] While a relatively new enforcement area, the FTC has taken steps to enforce the law.[25] In 2025, the

---

[18] *Id*. ; Tom Fairless & David Luhnow, *The Tech Industry Is Huge – and Europe's Share of It Is Very Small*, The Wall Street Journal (May 19, 2025), https://www.wsj.com/tech/europe-big-tech-ai-1f3f862c.

[19] *John M. Yun, A report Card on the Impact of Europe's Privacy Regulation (GDPR) on Digital Markets, 31 Geo. Mason L. Rev. F. 104, 109 (2024), https://lawreview.gmu.edu/wp-content/uploads/2024/04/Yun-31-Geo.-Mason-L.-Rev.-F.-104-2024.pdf.*

[20] Ash Johnson, *State Privacy Laws Show the SECURE Data Act's Merits and Political Appeal*, Info. Tech. & Innovation Found. (May 15, 2026), https://itif.org/publications/2026/05/15/state-privacy-laws-show-the-secure-data-acts-merits-and-political-appeal/.

[21] Business Software Alliance, *US: 2025 Models of State Privacy Legislation* (Oct. 23, 2025), https://www.bsa.org/policy-filings/us-2025-models-of-state-privacy-legislation.

[22] *Id*.

[23] Global CBPR Forum, https://www.globalcbpr.org/ (last visited May 27, 2026); Data Privacy Framework Program, *Data Privacy Framework (DPF) Program Overview*, https://www.dataprivacyframework.gov/Program-Overview (last visited May 27, 2026).

[23] U.S.C. Chapter 123 (§§ 9901–9903).

[25] Press Release, Fed. Trade Comm'n, *FTC Reminds Data Brokers of Their Obligations to Comply with PADFAA* (Feb. 9, 2026), https://www ftc.gov/news-events/news/press-releases/2026/02/ftc-reminds-data-brokers-their-obligations-comply-padfaa.

Department of Justice's Data Security Program, restricting the flow of personal data to countries of concern, was also finalized and took effect.[26]

IV. LEGISLATION

The Subcommittee intends to discuss the following legislation:

A. H.R. 8413, The SECURE Data Act (Rep. Joyce)

This bill establishes a national framework for consumer rights and the protection of Americans' personal data. It establishes consumer privacy rights, including the right to know whether a controller possesses their personal data and the right to access, correct, delete, and receive a portable copy of such data from a controller. Consumers may opt out of a controller's targeted advertising, sale of personal data, and certain automated denials of healthcare, housing, or employment. A consumer's consent is required for a controller to process sensitive data, which includes a health diagnosis, biometric data, and precise geolocation data, among other categories. A parent's consent is required for a controller to collect personal data from a child (under 13) or teenager (under 16). Only a parent may exercise a consumer right on behalf of a child or teenager.

A controller must limit personal data collected from a consumer to what is relevant, adequate, and reasonably necessary for the purposes disclosed. A controller must also limit secondary use of the personal data collected or it must obtain additional consent from a consumer. A controller may not process personal data in violation of a federal law that prohibits unlawful discrimination against a consumer. It may not discriminate against a consumer for exercising any consumer privacy right. A controller must provide an accessible, clear, and meaningful privacy notice that includes the category of personal data collected, the purpose for processing, how to exercise any privacy rights, and the category of controllers with whom the personal data is shared. A controller must provide notice if any personal data of a consumer is transferred to, processed in, stored in, or sold to a foreign adversary, including the People's Republic of China.

This bill requires controllers to establish, implement, and maintain reasonable data security practices to protect the personal data of consumers. Such practices must reflect the state-of-the-art and the volume, sensitivity, and nature of the data processed. A group of controllers or processors may propose a code of conduct to the Secretary of Commerce that would meet or exceed requirements under the Act. The Secretary must review any application, publish it for public comment, and may revoke approval for a code of conduct. This bill also establishes a controller's obligations with respect to handling deidentified data and pseudonymous data. It imposes new requirements for data brokers to register with the FTC, which will make available a public-facing, searchable registry.

---

[26] Data Security, U.S. Dept. of Just., Nat'l Security Div., https://www.justice.gov/nsd/data-security (last updated Sept. 24, 2025).

This bill clarifies that the Secretary of Commerce is the principal advisor to the President on policy relating to international flow of personal data and the protection of personal data in international commerce. The Secretary shall take any necessary action to support the international flow of personal data and the protection of personal data in international commerce, including assessing the laws and frameworks of foreign governments and the impact of such laws and frameworks on American consumers and businessss and national security., This bill directs the Secretary to conduct a study on commercially available technologies for a universal opt-out mechanism.

This bill will be enforced by the FTC and state attorneys general. A violation will be treated as a violation of a rule under the FTC Act. A controller or processor is afforded a right to cure an alleged violation within 45 days of a written request by the FTC or state attorney general, provided they give written assurances that it will not repeat the violation. The requirements of this bill apply to any person who conducts business in the U.S., offers a product or service to a resident of the U.S., or engages in the sale of the personal data of a U.S. resident and who meets one of the following: the person (1) collects and processes personal data of 200,000 or more consumers annually and has an annual gross revenue of $25 million or more; or (2) collects and processes personal data of 100,000 or more consumers annually and derives 25 percent or more of its annual gross revenue from the sale of such personal data. Several exemptions are provided for, including for federal and state governments, nonprofits, and entities and data subject to existing privacy laws.

This bill would establish a uniform national standard for consumer privacy rights and the protection of personal data. It maintains existing federal privacy and data security laws, including the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act.

V. KEY QUESTIONS

- How can a federal comprehensive privacy and data security law protect consumers, allow for beneficial uses of personal data, and preserve economic competitiveness?
- What approach should a federal comprehensive privacy and data security law take with regard to consumer rights, business obligations, and enforcement?
- Why are state comprehensive privacy laws generally enforceable by government agencies, as opposed to enforcement by a private right of action?
- What lessons can Congress learn from the states that have enacted comprehensive privacy and data security laws? What are commonalities and differences between these different state frameworks?
- How can a federal comprehensive privacy and data security law promote international data flows and address privacy risks associated with foreign adversaries?

VI. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Giulia Leganski, Evangelos Razis, or Jackson Rudden of the Committee Staff at (202) 225-3641.