Statement of Tyler R. Bridegan, Partner, Womble Bond Dickinson (US) LLP

U.S. House Committee on Energy & Commerce, Subcommittee on Commerce, Manufacturing, and Trade

Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Data Act)

Thank you, Chair Gus Bilirakis, Ranking Member Jan Schakowsky, and members of the Subcommittee, for the distinct honor of testifying about the privacy legal landscape. My name is Tyler Bridegan, and I am a partner in the Privacy and Cybersecurity team at the international law firm Womble Bond Dickinson (US) LLP. My practice centers on litigation, government investigations, and proactive compliance with privacy and cybersecurity laws and regulations. Prior to my current role, I served as the Director of Privacy and Technology Enforcement for the Texas Attorney General's Office, where I oversaw the implementation and enforcement of Texas' privacy, cyber and technology-related laws, including Texas' comprehensive privacy law, data broker law, and children's privacy and online safety law.

It is my sincere hope that my experience enforcing, litigating, and counseling companies on privacy laws will provide this Committee with helpful background and context as it debates a federal privacy law.

I. Americans Need Comprehensive Privacy Protections at the Federal Level

Consumers and companies urgently need a uniform federal consumer privacy law that extends privacy protections to all Americans and "takes into account the laws that consumers are already living under and that companies are already complying with."[1] Over 20 state legislatures, as laboratories of democracy, have effectively established a core set of agreed upon consumer privacy principles, protections, and requirements. These uniform principles are uncontroversial.

My time enforcing Texas' privacy laws at the Texas Attorney General's Office underscored the strength of these privacy protections, but also the urgency at which they are needed. While most companies make good faith attempts to comply with privacy laws,

[1] J. Polonetsky, Future of Privacy Forum, LinkedIn (May 29, 2026), *available at* https://www.linkedin.com/events/weeklyprivacychatwithfpfceojule7465388164870864897/theater/.

some companies were using data collection tactics that pushed well past the boundaries of Americans' privacy expectations. Their tactics varied, but oftentimes targeted Americans' sensitive data by installing code or programs on every day devices like phones, vehicles and watches.[2] These tactics also gave companies access to shockingly granular data about Americans, such as whether a person picked up their cell phone while moving at speeds greater than 20 miles per hour. Equally concerning was the noticeable shift some companies used and monetized Americans' data. While privacy and data-related harms were once abstract, this shift was clearly causing actual, material consequences for American consumers, many of which had a financial component. As technology continues to advance and data collection becomes even more sophisticated, new types of privacy and data-related harms will undoubtedly emerge.

These harmful practices run afoul of most states' sensitive data consent requirements, and they would also be unlawful under the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (the "Act"). Although still early in the legislative process, the Act already contains the same substantive requirements as the privacy laws that have led to record-breaking recoveries for consumers, such as the billions of dollars recovered under Illinois and Texas' biometric privacy laws. The Act also contains the core set of privacy protections enacted by a large, bi-partisan coalition of state legislatures, including consumer rights, heightened restrictions around sensitive data, and consumer notice requirements. Lastly, and maybe most importantly, the Act would grant enforcement authority to both the Federal Trade Commission (FTC) and state attorneys general, which will undoubtedly drive compliance by companies.

II. The State of State Privacy Laws in America

States, as laboratories of democracy, have long taken an innovative approach to privacy protections. Many of these privacy protections have withstood substantial technological advances and continue to be powerful protectors of Americans' data. One of the first innovations occurred in 2007, when Texas became the first state to pass a biometric privacy law, with Illinois enacting a similar law a year later.[3] These biometric laws' requirements are relatively simple: they require companies to provide consumers with notice and receive their consent prior to obtaining the consumer's retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry. Nearly two decades after their passage, both laws remain potent; with both having resulted in record-setting recoveries for consumers totaling billions of dollars.

---

[2] See Electronic Information Privacy Center, Testimony on Washington People's Privacy Act (HB 1671), https://epic.org/documents/testimony-on-washington-peoples-privacy-act-hb-1671/.

[3] *See* Tex. Bus. & Com. Code § 503.001, *et seq*.; 740 ILCS 14/1, *et seq*.

States have continued to innovate and adopt new types of privacy laws over time. These include cyber breach reporting laws, website privacy notice laws, data brokers laws, and children's privacy and online safety laws. The federal government likewise enacted several privacy and data-related laws that generally focus on sensitive data types or uses, such as the Fair Credit Reporting Act (FCRA), the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley Act (GLBA).

California continued this tradition of state privacy innovation and, in 2018, became the first state to pass a comprehensive consumer privacy law. California's law is primarily based on notice and "opt-out" protections meaning that, by default, companies are permitted to collect, use, and process consumers' personal data, including their sensitive data, so long as the company provides some form of notice to the consumer and allows the consumer to opt out of certain uses of their data.

Since then, a large, bi-partisan coalition of more than 20 states have enacted their own comprehensive consumer privacy laws. While this bi-partisan coalition adopted some of California's weaker notice and opt-out protections, every single state rejected California's approach to protecting sensitive data. Instead, these states, which includes the likes of Colorado, Delaware, Indiana, Kentucky, New Jersey, and Texas, imposed stronger "consent" requirements for sensitive data, which requires companies to demonstrate a "clear affirmative act that signifies [the consumer's] freely given, specific, informed, and unambiguous agreement [] to process [their] personal data."[4] In other words, before doing *anything* with a consumer's sensitive data, a company must inform consumers of the types of sensitive data it will process, inform them how it will process their sensitive data (i.e., collect, use, sell), and unambiguously obtain the consumer's agreement to do so.

A small minority of states have recently adopted wholesale bans of certain data practices. For example, Maryland recently banned the sale of any sensitive data type, even if a consumer consented to the sale.[5] Such bans go beyond any other comprehensive consumer privacy regime.

III. The SECURE Data Act Contains Strong, Enforceable Consumer Privacy Protections

The Act incorporates core consumer privacy principles, rights, and obligations from existing federal and state privacy laws. These are uncontroversial. Indeed, over 20 states

[4] *See, e.g.*, Tex. Bus. & Com. Code § 541.001, *et. seq.*

[5] *See* Maryland Online Data Privacy Act of 2024.

have enshrined these principles into their respective privacy laws. These principles commonly take the form of requirements relating to:

- A consumer's ability to exercise control of their personal data;
- Heightened safeguards regarding the processing of sensitive data;
- Disclosures to consumers;
- Service provider restrictions and obligations; and
- Data security requirements.

The Act incorporates all of these common requirements.

Equally important, however, is that these agreed upon privacy protections are effective. When enforced properly, these requirements provide a powerful tool for consumers and government regulators alike. The clearest evidence of this relates to the Act's heightened safeguards for sensitive data. With the exception of California, every state privacy law requires that a company obtain a consumer's consent before doing *anything* with a consumer's sensitive data. Consent is generally defined as a "clear affirmative act that signifies [the consumer's] freely given, specific, informed, and unambiguous agreement [] to process [their] personal data."[6]

Notably, consent requirements have long been the hallmark of the strongest data privacy laws in the United States, and are found in laws such as HIPAA, Illinois' Biometric Information Privacy Act (BIPA), and more recently, Washington's My Health My Data Act. Underscoring the potency of consent requirements, these consent-based laws have regularly been used to obtain record-breaking recoveries on behalf of consumers. Examples of this include Texas' use of its biometric privacy law to obtain two $1 billion+ settlements, and Illinois' use of BIPA to obtain a settlement of over $500 million.[7]

IV. Government Enforcement and Codes of Conduct Will Protect Americans' Privacy

The Federal Trade Commission (FTC) and state attorneys general have a long history of working together and are best positioned to interpret and enforce a federal privacy law. While privacy laws are relatively nascent, the FTC and state attorneys general have already developed substantial privacy expertise. This expertise has substantial benefits to companies. First, their expertise will allow them to provide clear

[6] *See, e.g.*, Tex. Bus. & Com. Code § 541.001(6).

[7] Dallas Morning News, "Google finalizes $1.375 billion settlement with Texas over alleged privacy violations," *available at* https://www.dallasnews.com/news/politics/2025/10/31/google-finalizes-1375-billion-settlement-with-texas-over-alleged-privacy-violations/.

and consistent guidance to companies. Second, their expertise gives them a strong understanding of what practices comply with an eventual privacy law. And third, their expertise will allow them to conduct efficient investigations into companies' privacy practices.

Government regulators are also best positioned to legitimately protect the privacy interests of consumers. Traditionally, government regulators have focused their enforcement efforts on obtaining strong, injunctive relief for consumers. While it is essential that government regulators have the authority to obtain substantial monetary penalties, the monetary component of an enforcement action is oftentimes a secondary concern. This tendency to prioritize injunctive relief as opposed to monetary relief puts government regulators in the best position to protect Americans' privacy interests.

The Act also, notably, creates a code of conduct mechanism by which government regulators can preserve resources and streamline their enforcement. Specifically, the Act would establish a mechanism for the creation of government-approved independent codes of conduct. Such codes of conduct would be required to meet or exceed the requirements of any federal privacy law. Such a mechanism is highly valuable to government regulators. Codes of conduct allow them to review and approve proposed standards that meet or exceed any eventual federal privacy law. This then allows government regulators to more easily ensure that companies are in compliance with any eventual federal privacy law. This, importantly, takes a substantial burden off of government regulators and allows them to preserve enforcement resources.

* * *

Ultimately, there is widespread support for a federal comprehensive consumer privacy law that extends privacy protections to all Americans. States have also done a remarkable job of laying the groundwork for what a federal privacy law should ultimately look like. Accordingly, it is my sincere hope that Congress moves forward and passes a federal privacy law.[i]

[i] On a personal note, I want to thank my current and former colleagues that have constantly pushed and encouraged me to become a better lawyer. I also want to specifically recognize my former Federal Communications Commission colleague, Joyce Bernstein, who passed away in the days leading up this hearing. She was an incredible life-long public servant.