



1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
brt.org

September 30, 2022

The Honorable Frank Pallone
Chairman
Committee on Energy & Commerce
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Committee on Energy & Commerce
2322 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Pallone and Ranking Member McMorris Rodgers:

On behalf of the members of Business Roundtable, we write regarding H.R. 8152, the American Data Privacy and Protection Act (ADPPA), which was reported to the U.S. House of Representatives by the Committee on Energy & Commerce on July 20, 2022.

Business Roundtable is an association of chief executive officers of America's leading companies. Business Roundtable member companies operate across all sectors of the domestic and global economy, employ 20 million people, and reach virtually every American consumer. Our companies – from technology, communications, retail, financial services, health, public safety and security, manufacturing, hospitality, insurance, and others – cover the breadth of the U.S. economy and rely on data and data-driven processes and solutions, such as digital platforms, every day to deliver and improve innovative products and services across the U.S. and around the world. Consumer trust and confidence are essential elements of our businesses and our relationship with our customers.

Business Roundtable has consistently called for a federal consumer data privacy law that will protect and empower consumers and provide clear, consistent obligations for how companies handle personal data, while fostering responsible and inclusive American innovation and supporting our global competitiveness. To provide a detailed guide for addressing key issues integral to an effective federal data privacy law, in 2018 Business Roundtable released a [Framework for Consumer Privacy Legislation](#). Our framework includes robust protections for consumers by requiring businesses to take responsibility for the collection, use and sharing of personal information, regardless of jurisdiction. The framework also includes sections on enforcement, data security and breach notification, governance, risk-based privacy practices, and the effect on other laws.

We appreciate the hard work that many Members of Congress have dedicated to this bill and to comprehensive data privacy legislation more broadly. While the ADPPA helps advance the debate on data privacy, several of its provisions would place unnecessary and economically harmful burdens on businesses without providing commensurate benefits to consumers. For example, some provisions would hinder the cross-border exchange of personal data, jeopardizing the United States' status as a hub for talent and overseas investment in data and digital research initiatives. Others are overly prescriptive and not limited to personally identifiable information. The ultimate impact of the current language across these provisions would be to significantly undermine the bill's achievement of a unified, national privacy framework, which is essential to protecting U.S. consumers, as well as its efforts to bolster the competitiveness of U.S. businesses in the global marketplace.

With these concerns in mind, Business Roundtable recommends that several key adjustments be made to the ADPPA to ensure that the legislation provides necessary and effective protections to consumers without causing undue harm to U.S. innovation and competitiveness:

First, a national consumer privacy law should be strong and provide consistent protections to consumers across every state in the country. U.S. privacy laws are highly fragmented across industries and jurisdictions, creating a patchwork of requirements which hurts both consumers and companies. Business Roundtable supports express preemption of state and local comprehensive privacy laws, including those already enacted. State exceptions and carve outs to a federal privacy framework would lead to inconsistent and confusing protections for consumers, negative user experiences, and an unworkable compliance structure for companies of all types and sizes, especially small and medium sized businesses. The ADPPA includes nineteen categories of exceptions to the bill's preemption of state laws that undermine the achievement of a unified national privacy framework. These exceptions appear to apply even if such state laws are enacted after the ADPPA is passed and could provide for state-based private rights of action and state common law causes of action alleging a violation of the new federal law. Federal privacy legislation should preclude these challenges by standardizing protections nationwide and making it clear that the ADPPA preempts any sub-national laws related to consumer data privacy.

In one particularly concerning provision, the bill grants extraordinary enforcement authority to a single specified state regulatory agency, the California Privacy Protection Agency ("CPPA"), despite the fact that this agency is already considered a "State Privacy Authority" under the bill. The enforcement authority granted to the CPPA would arguably go beyond even the authority of the Federal Trade Commission ("FTC") and would include the ability to promulgate regulations, conduct investigations and audits, and impose recordkeeping requirements. We agree with those Members from California who want to ensure that Congress enacts a strong privacy law. But we also believe that strong law needs to apply uniformly throughout the United States. Singling out one state agency for far-reaching, unparalleled enforcement authority of a federal law undermines the intended national scope and impact of this bill. It favors one particular state over others with respect to a law intended to provide equal protections for all Americans. This further undermines the primacy of the federal law, leading to inconsistent protections of privacy rights in the U.S. and the diminution of a unified national privacy framework.

Second, the ADPPA limits the collection, processing, and transfer of covered data for certain "permissible purposes," which creates uncertainty and unintended consequences for uses of covered data that benefit consumers. For example, the processing of covered data for some of the purposes listed in the legislation appears *not* to be permissible unless the data has been collected for a different lawful purpose. These restrictions on permissible purposes and related data collection appear to apply even to essential business operations such as (1) processing data to perform system maintenance or diagnostics; (2) repairing a product; (3) conducting analytics to improve a product or service; (4) performing inventory or reasonable network management; and (5) ad measurement. These limitations should be narrowed to continue allowing business operations that are foundational to the digital economy and do not pose a risk to consumer privacy. In addition, the ADPPA imposes restrictions on these ostensibly permissible purposes based upon the bill's "loyalty duties." Business Roundtable strongly urges that permissible purposes not be subject to any other obligations or restrictions in the bill and that the inconsistency between permissible purposes and loyalty duties be resolved.

Third, the ADPPA includes a private right of action. Business Roundtable continues to have serious concerns about a private right of action, which will lead to high-cost, frivolous litigation that will not provide meaningful relief to consumers while diverting company resources away from actual security and privacy compliance. The Illinois Biometric Information Privacy Act provides a stark example of what happens when plaintiff's lawyers are incentivized to bring even frivolous claims.¹ These lawsuits enrich plaintiffs' attorneys without providing meaningful redress to consumers. In addition, a private right of action will undermine the uniformity and predictability of a national privacy framework by delegating key decisions on privacy law to private plaintiffs and the judicial system, with the law splintering across the country as courts in hundreds of jurisdictions across the country continually reinterpret the law. The necessity of a private right of action is further negated because the ADPPA provides enforcement authority not only to the FTC, but also to State Attorneys General.

Fourth, several of the ADPPA's definitions and obligations are overly prescriptive and expansive. One example is the overly broad definition of biometric information, which may undermine companies' ability to provide important fraud and security protections for consumers. Another is the bill's expansive definition of "covered algorithm," and related extensive reporting requirements that implicate an enormous number of day-to-day business decisions facilitated by technology, including decisions made entirely by humans. Business Roundtable suggests that Section 207 be made advisory rather than mandatory and, at minimum, the definition of "covered algorithm" be narrowed and all related requirements focus on high-risk uses that are contextual, proportional, risk-based, and use-case specific, and linked to clearly defined harms. Furthermore, Section 207 should not encompass decisions with respect to covered data that involve humans. The inclusion of these changes will refine the bill to focus efforts on potentially harmful uses of algorithms, such as automated decision-making systems that produce legal or other similarly significant adverse effects on individuals, without placing unnecessary burdens on essential and routine business activities or diverting meaningful artificial intelligence compliance resources to ineffectual or redundant administrative tasks. At the very least, the terms "consequential risk" and "consequential decision" need to be defined in statute.

Finally, the current version of the bill presents a bevy of new restrictions that will directly impact how large data holders, many of whom are Business Roundtable members, are able to utilize data provided by third parties for healthcare research. Specifically, to continue to advance healthcare and benefit from clinical trial data, the bill should exclude data which has been "de-identified" according to the current HIPAA standards.

Business Roundtable looks forward to working with you and your colleagues as the discussions surrounding a national data privacy bill progresses. We urge you to make these changes to H.R. 8152 to address our concerns before the legislation is considered by the U.S. House of Representatives.

Sincerely,



Kristen Silverberg
President & Chief Operating Officer
Business Roundtable

¹ See <https://news.bloomberglaw.com/privacy-and-data-security/as-biometric-lawsuits-pile-up-companies-eye-adoption-with-care>.