The Leadership Conference
on Civil and Human Rights

1620 L Street, NW
Suite 1100
Washington, DC
20036

202.466.3311 voice
202.466.3435 fax
www.civilrights.org

The Leadership Conference

June 3, 2026

The Honorable Gus Bilirakis
Chair
Subcommittee on Commerce, Manufacturing, and Trade
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
U.S. House of Representatives
Subcommittee on Commerce, Manufacturing, and Trade
Washington, DC 20515

Dear Chair Bilirakis and Ranking Member Schakowsky,

On behalf of The Leadership Conference on Civil and Human Rights' Center for Civil Rights and Technology (Center), we thank you for the opportunity to submit our views regarding the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act, or SECURE Data Act. The Leadership Conference is a coalition charged by its diverse membership of more than 240 national organizations to promote and protect the rights of all persons in the United States. We ask for this letter to be entered into the record of the Subcommittee on Commerce, Manufacturing, and Trade hearing titled *Examining Legislation to Establish a Federal Comprehensive Privacy and Data Security Law* on June 3, 2026. We have supported comprehensive federal privacy legislation in the past and as a coalition have called for laws that meaningfully regulate data collection and use, limit harmful data practices, and prevent discrimination.

Public opinion is clear: people have become increasingly aware of how their data is being collected and used and, unsurprisingly, they are fearful. People want their privacy protected.

- In a Pew Research survey, 81% of respondents said they are concerned about how companies use the data they collect about them, with 61% having little to no understanding of what is being done with their data.

The Leadership Conference

- The results also show that most (73%) believe they have little or no control over what companies do with their data.
- When it comes to AI, 81% of people surveyed said they fear their personal information will be used in ways they won't be comfortable with or that weren't originally intended. [1]
- Consumer Reports found that 78% of people across party lines would support a law regulating how companies can collect, store, share, and use their personal data.[2]

The Leadership Conference has weighed in with the full Energy & Commerce Committee and its subcommittees many times over the past five years regarding a comprehensive federal privacy and data security law.[3] Our position has remained consistent over this time: we strongly support the need for federal legislation, but any law passed by Congress must be protective of civil rights. We stand behind the following language, first shared with the full committee following the removal of civil rights protections from the American Privacy Rights Act (APRA) and shared again with the House Republican Privacy Working Group:

> *"Privacy rights and civil rights are no longer separate concepts — they are inextricably bound together and must be protected. Abuse of our data is no longer limited to targeted advertising or data breaches. Instead, our data are used in decisions about who gets a mortgage, who gets into which schools, and who gets hired — and who does not. All too often, those data-driven decisions come with discriminatory outcomes, which have been compounded as algorithmic technologies and AI have advanced at an unprecedented pace. Individuals who face discrimination on the basis of their race, ethnicity, sex, disability, national origin, sexual orientation, gender identity, immigration status, or religion already contend with rampant harms as a result of invasive and predatory data practices. For example, companies have used AI to discriminate based on these characteristics against job applicants, deny equal access to credit, impair access to healthcare, and unfairly prejudge students' academic prospects. A privacy bill that does not include civil rights protections will not meaningfully protect us from the most serious abuses of our data.*"

Unfortunately, the SECURE Data Act fails to deliver those necessary safeguards at a time of pervasive data collection, algorithmic decision making, and AI-driven profiling. Even worse, the SECURE Data Act

---

[1] Colleen McClain, Michelle Faverio, Monica Anderson, and Eugenie Park, "How Americans View Data Privacy," *Pew Research Center,* (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

[2] Scott Medintz, "Americans Want Much More Online Privacy Protection Than They're Getting," *Consumer Reports* (Nov. 20, 2024), https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/.

[3] Letter from the ACLU, Lawyers' Committee for Civil Rights Under Law, and The Leadership Conference on Civil and Human Rights to The Honorable Cathy McMorris Rodgers, (June 25, 2024), https://civilrights.org/resource/civil-society-letter-house-energy-commerce-committee-privacy-legislation/.

will impede states' efforts to protect their residents' personal data by preempting any privacy laws they may pass.

Relying on an outdated "notice and consent" model does not work today.

The current "notice and consent" model, in which companies provide notice of data collection and implore users to consent to their data being used, is ineffective in both protecting users' privacy and in empowering people to control how their data is used. Unfortunately, instead of meaningfully addressing this issue, the SECURE Data Act fails to include restrictions on data collection and use and instead simply repackages the status quo.

Privacy protections should not depend on individuals' ability or willingness to navigate complex disclosures written in dense legalese. In maintaining the status quo, the SECURE Data Act recklessly puts the burden of protecting their data on individuals, leaving them at the mercy of Big Tech and the companies that use their technologies.

Another issue is the lack of strictures on companies' ability to coerce consent for data collection and use. The SECURE Data Act has no prohibition on coercive practices like dark patterns, to obtain consent, and despite language that *appears* to prohibit a company from limiting a user's access to their services because that person declined to provide their data, the SECURE Data Act allows companies to provide different tiers of services based on a person's willingness to turn over their data. Such a framework is ripe for abuse and could result in coerced consent.

The public wants strong limits, not just more disclosures. According to Consumer Reports, 86% of Americans support federal privacy legislation that truly limits data collection and use, going beyond the simple and past-its-prime notice and consent framework embodied in the SECURE Data Act.[4]

Data and AI are inexorability linked; any data protection bill must include civil rights protections and algorithmic accountability.

As we wrote in the Civil Rights Principles in the Era of Big Data,[5] privacy laws must *"*ensure that data is not used in ways that reinforce existing inequities or create new forms of discrimination*."* The SECURE Data Act, unlike prior bipartisan comprehensive federal privacy legislation considered and passed by the Committee, will allow algorithmic discrimination, digital redlining, biased automated decision making, continued use of opaque AI systems trained on people's personal data, and algorithmic profiling based on AI inferences about individuals.

---

[4] Scott Medintz, "Americans Want Much More Online Privacy Protection Than They're Getting," Co*nsumer Reports,* (Nov. 20 2024), https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/.

[5] The Leadership Conference on Civil and Human Rights, "Civil Rights Principles for the Era of Big Data," (Feb. 2024), https://civilrights.org/2014/02/27/civil-rights-principles-era-big-data/.

The Leadership Conference

The "protections" in the SECURE Data Act are narrow, incomplete, and riddled with loopholes and exceptions.

In addition to expecting a systemic problem to be addressed by individuals' actions, the SECURE Data Act is riddled with loopholes and exceptions that renders individual choice effectively meaningless.; it will do little to nothing to actually restrict what data companies can collect or how they will use it[6].

While the SECURE Data Act includes provisions addressing sensitive data, the definition is narrow and excludes the processes of making inferences and predictions based on the data collected — both of which may include what should be protected traits, such as gender, religion, political affiliation, disability, and sexual orientation. And despite providing for an "opt-in" for sensitive data, it is undermined by broad exceptions, like for "operational purposes," "product development," "service improvement," and "internal research." The outcome is that companies will continue to collect whatever data they wish and use it in whatever way they wish. The "protections" in the SECURE Data Act are anything but.

Congress should not weaken stronger state protections. Instead we must pass meaningful federal privacy protections.

Simply put, the SECURE Data Act will leave people worse off.

The public deserves a privacy law that limits data collection, includes enforceable civil rights protections, regulates automated AI decision making, and ensures accountability. The SECURE Data Act does not achieve these goals. If Congress wants to help bolster the public's trust in technology — including AI, thereby helping to ensure its sustained use and acceptance — it must address the mounting public skepticism about technology. Congress can do so by pursuing a comprehensive privacy bill that actually protects people and their data.

We stand ready to work with Congress on policies that will protect civil rights, prevent unlawful discrimination, and advance equal opportunity. Should you require further information or have any questions regarding this issue, please feel free to contact Jonathan Walter, senior policy counsel, at walter@civilrights.org

Sincerely,

Alejandra Montoya-Boyer
VP, Center for Civil Rights and Technology

---

[6] Mario Trujillo, "The SECURE Data Act is Not a Serious Piece of Privacy Legislation," *Electronic Frontier Foundation.* (May 6, 2026), https://www.eff.org/deeplinks/2026/05/secure-data-act-not-serious-piece-privacy-legislation.