

A D D E N D U M
to
PROTECTING THE VIRTUAL YOU:
SAFEGUARDING AMERICANS' ONLINE DATA

This Addendum is available at:

<https://www.govinfo.gov/content/pkg/CHRG-119shrg61893/pdf/CHRG-119shrg61893-add1.pdf>

Submitted by Chair Blackburn:

Consumer Technology Association (CTA®), letter 2

Submitted by Senator Schiff:

California Privacy Protection Agency (CPPA), letter 4



1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

July 30, 2025

Senator Marsha Blackburn
Chairman
Senate Subcommittee on Privacy, Technology, and the Law
Senate Judiciary Committee
United States Senate
Washington, DC 20510

Senator Amy Klobuchar
Ranking Member
Senate Subcommittee on Privacy, Technology, and the Law
Senate Judiciary Committee
United States Senate
Washington, DC 20510

Dear Chairman Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee:

The Consumer Technology Association (CTA®) submits this statement for the record for the Senate Judiciary Committee hearing on “Protecting the Virtual You: Safeguarding Americans’ Online Data.”

Privacy as a Foundation for Innovation

Privacy protection remains a central pillar of CTA’s 2025 Innovation Agenda. As digital technologies and online services become even more embedded in American life, consumers rightly expect both privacy safeguards and continued access to the innovative, data-driven products and services that enhance daily life. A robust privacy framework must maintain this balance while supporting American technological leadership.

The Need for a Comprehensive, Uniform Federal Approach

Current state-by-state privacy statutes have created a fragmented regulatory landscape resulting in consumer confusion, uneven rights, and disproportionate compliance burdens—especially for startups and smaller businesses. CTA strongly supports a uniform, national privacy law with the following key attributes:

- Federal Preemption
- No Private Right of Action
- Risk-Based and Tiered Compliance
- Harmonization with Sectoral Laws

Clear Definitions, Consumer Rights, and Transparency

A federal law should adopt precise definitions for roles, types of data, and regulatory responsibilities, avoiding overbroad requirements for low-risk data. Ensuring concise, accessible consumer disclosures—without overwhelming legal jargon—is central to fostering trust and meaningful consent.

Data Security, Safe Harbor, and Enforcement Structure

Strong security requirements, such as encryption for sensitive data and use of recognized best practices, should adapt to evolving threats. CTA recommends public-private partnerships to enhance cybersecurity and inform consumers.

CTA firmly supports a well-structured safe harbor provision, granting affirmative legal defenses for responsible companies following established frameworks. This incentivizes best practices and protects small businesses especially from opportunistic litigation.

Enforcement should rest with the Federal Trade Commission, in partnership with agencies like National Institute of Standards and Technology (NIST) and Cybersecurity and Infrastructure Security Agency (CISA) for technical guidance. Rulemaking and enforcement should remain separate, with the FTC focused on consistent, expert enforcement.

Avoiding Restrictive Models and Championing U.S. Leadership

CTA cautions against rigid frameworks modeled on the EU's GDPR, which have demonstrably stifled innovation and disadvantaged small businesses in Europe. Instead, the U.S. should advance an innovation-friendly model, align with successful industry standards, and ensure ongoing compatibility with existing federal laws.

Conclusion

The above discussion is consistent with CTA's well-established position in favor of a uniform, national privacy law.

On April 7th, CTA wrote to the House Energy & Commerce Committee Privacy Working Group in response to its Request for Information to explore a data privacy and security framework. In our response, CTA argued that a well-structured federal framework without a private right of action would enhance consumer protection while fostering regulatory certainty that spurs American innovation.

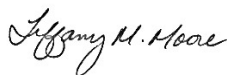
On July 9th, CTA's VP of Digital Health René Quashie echoed these calls while serving as an expert witness before the Senate Committee on Health, Education, Labor, & Pensions' hearing titled, "Securing the Future of Health Care: Enhancing Cybersecurity and Protecting Americans' Privacy." In his testimony, he highlighted the importance of patient data privacy and the need for a federal solution.

CTA appreciates the Subcommittee's leadership and stands ready to collaborate with Congress in crafting a balanced national privacy framework—one that ensures regulatory clarity, preserves American innovation, and delivers robust protections to all consumers.

Sincerely,



Gary Shapiro
CEO and Vice Chair



Tiffany M. Moore
SVP, Political and Industry Affairs



Rachel Nemeth
Sr. Director, Regulatory Affairs

Cc: Members, Senate Subcommittee on Privacy, Technology, and the Law, Senate Judiciary Committee

July 29, 2025

The Honorable Chuck Grassley, Chair
The Honorable Dick Durbin, Ranking Member
The Honorable Marsha Blackburn, Chair, Subcommittee on
Privacy, Technology, and the Law
The Honorable Amy Klobuchar, Ranking Member, Subcommittee on
Privacy, Technology, and the Law
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

**Re: U.S. Senate Judiciary Subcommittee on Privacy, Technology, and the Law Hearing,
“Protecting the Virtual You: Safeguarding Americans’ Online Data”**

Dear Chair Grassley, Ranking Member Durbin, Chair Blackburn, and Ranking Member Klobuchar,

The California Privacy Protection Agency (CPPA or Privacy Agency) thanks the Senate Judiciary Committee and its Subcommittee on Privacy, Technology, and the Law for holding a hearing to consider the best ways to safeguard Americans’ data.¹ All Americans deserve strong, meaningful protections over the collection, use, and disclosure of their personal information, and we urge you to ensure that any federal privacy legislation preserves the ability of states to maintain and strengthen their privacy protections. States play a crucial ongoing role in addressing emerging privacy challenges, and federal privacy laws should establish a floor, not a ceiling, of protection. Failure to do so would likely cause many citizens to lose important privacy rights they enjoy today.

California has been at the forefront of protecting individual privacy rights, with protections enshrined in our state constitution and strengthened through laws and ballot initiatives.² In 2018, California became the first state in the nation to adopt a comprehensive consumer privacy law, the California Consumer Privacy Act (CCPA).³ Then in 2020, California voters affirmed their desire for robust privacy protections by passing Proposition 24, which amended the CCPA and established the Privacy Agency to implement and enforce the law. Since then, California has adopted multiple pieces of legislation to further strengthen privacy protections, including the Delete Act which established a first in the nation data broker deletion requirement.⁴ These protections represent the will of Californians and have proven both effective and necessary in response to the evolving digital economy.

¹ Established by California voters in 2020, the California Privacy Protection Agency was created to protect Californians’ consumer privacy. The Privacy Agency implements and enforces the California Consumer Privacy Act. It is governed by a five-member board that consists of experts in privacy, technology, and consumer rights.

² Cal. Cons. Art 1§1

³ Cal. Civ. Code § 1798.100 et seq

⁴ *Id.* at § 1798.99.80

Similar legislation, inspired by California’s success, has been enacted in states across the nation establishing a nationwide laboratory for privacy protection. To date, twenty states have enacted comprehensive privacy laws, all of which provide similar protections.⁵ These state laws pioneered the very concepts and frameworks that now frequently inform federal proposals. They introduced American consumers to rights of deletion, access, and correction and rights to opt-out of data sales and certain types of processing, and they developed and refined approaches to transparency, data minimization, and purpose limitations. Together, they represent years of careful deliberation and modification, stakeholder engagement, and implementation that has proven to be workable and effective.

States also continue to play an important ongoing role addressing emerging privacy challenges from rapidly evolving technology. As we witness the growth of artificial intelligence, biometric technologies, connected devices, and new data practices we cannot yet imagine, states have proven capable at amending their privacy laws in a timely manner. For example, in recent years California enacted laws that address privacy concerns posed by new neural data technologies and ensure that consumers maintain their privacy protections when interacting with artificial intelligence systems.⁶ Similarly, California’s Delete Act charges the CPPA to establish a first-of-its-kind accessible deletion mechanism that will allow Californians to request that their personal information be deleted from over 500 different data brokers in one easy step. This innovative legislative solution to the serious privacy risks posed by unregulated data brokers would be lost by federal preemption of this area.

In contrast to the federal lawmaking process that moves more deliberately to consider changes, states’ demonstrated flexibility and nimbleness that allows them to adapt quickly to novel threats makes them essential partners in the ongoing work of privacy protection. For example, in the seven years since the CCPA was enacted, 19 additional states have passed similar consumer privacy laws. The federal Children’s Online Privacy Protection Act (COPPA), passed in 1998, has not yet been updated to address today’s technical realities, including widespread cell phone and social media use, though amendments to the law have been introduced over several terms.⁷ Several states have, however, enacted their own COPPA-style laws to protect children’s privacy in the digital era.⁸ Federal preemption would hobble this state-level responsiveness precisely when technological change demands it most.

The business sector’s successful adaption to state privacy laws demonstrates that these laws work. While the tech sector often argues that the “patchwork” of state laws is burdensome, the reality is that the state laws in place today share similar frameworks and build upon each other, thereby promoting interoperability. The Consortium of Privacy Regulators, a bipartisan group of eight state privacy regulators, are collaborating on implementation and enforcement of their privacy laws.⁹ Major corporations have been complying with various state privacy regimes for years, developing systems and processes that respect consumer rights while maintaining thriving business. California, for example, is the fourth largest economy in the world and is home to many major companies while also providing consumers with cutting-edge privacy rights and protections.¹⁰ Indeed, privacy practices are now often viewed as a competitive advantage with

⁵ California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, Oregon, Texas, New Hampshire, New Jersey, Rhode Island, Tennessee, Utah, and Virginia. *See*, IAPP, US State Comprehensive Privacy Laws Report: 2024 Legislative Session (October 2024), https://iapp.org/media/pdf/resource_center/us_state_privacy_laws_report_2024_session.pdf

⁶ CA SB 1223 (2024); CA AB 1008 (2024)

⁷ 15 U.S.C. § 6501 et seq.; *see also*, e.g., S 748, 116th Congress (2019-2020); Kids PRIVCY Act, HR 4801, 117th Congress (2021-2022); Children and Teens Online Privacy Protection Act, S 1418, 118th Congress (2023-2024)

⁸ *See e.g.*, AK HB 1717 (2025); Va. Code § 59.1-578; C.R.S. § 6-1-1308.5

⁹ California Privacy Protection Agency, *State Regulators Form Bipartisan Consortium to Collaborate on Privacy Issues* (April 16, 2025), <https://cppa.ca.gov/announcements/2025/20250416.html>

¹⁰ Office of Governor Gavin Newsom, *California is Now the Fourth Largest Economy in the World* (April 23,

some companies integrating state law requirements into their national operations.¹¹

In light of these existing state regimes, a federal proposal that incorporates preemption could strip away many crucial protections that consumers in California and across the country currently enjoy under state privacy laws. Revoking established rights would harm consumers and betray the trust they have placed in the government to safeguard their personal information. This would be a significant step backward in privacy protection at a time when privacy threats from new technology are increasing, not diminishing.

Preemption is also not necessary for effective federal regulation. Many privacy-protecting proposals, like the AI Accountability and Personal Data Protection Act introduced by Senators Hawley and Blumenthal, offer strong federal protections to Americans while not limiting states' ability to act.¹² Additionally, many existing federal privacy laws, for example the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act, recognize the importance of state-level innovation in privacy protection and explicitly preserve states' abilities to adopt stronger protections for their residents.¹³ This approach respects federalism, protects consumers, and ensures that privacy law can continue to evolve as quickly as the technologies it governs.

States have been the laboratories for effective privacy protections, innovating quickly to protect consumers as new harms arise. Federal legislation should, therefore, establish strong baseline protections while preserving states' authority to respond to their citizens' needs and emerging technologies. We urge you to reject any federal proposals that would preempt state privacy laws and instead embrace the collaborative federal-state framework that has been successful in ensuring Americans are adequately protected today and in the future.

Respectfully,



Tom Kemp
Executive Director
California Privacy Protection Agency

cc: Members, Senate Judiciary Committee

2025), <https://www.gov.ca.gov/2025/04/23/california-is-now-the-4th-largest-economy-in-the-world/>

¹¹ Julie Brill, *Microsoft will honor California's new privacy rights throughout the United States* (November 11, 2019), <https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/>

¹² AI Accountability and Personal Data Protection Act, 119th Cong., (Hawley Print 2026), <https://www.hawley.senate.gov/wp-content/uploads/2025/07/Hawley-AI-Accountability-and-Personal-Data-Protection-Act.pdf>

¹³ 45 C.F.R. Part 160, Subpart B; 15 U.S.C. § 6807.