Comments of Jennifer Huddleston and Emma Hopp in Response to Request for Information (RFI) on Exploring a Data Privacy and Security Framework

Chair Guthrie, Vice Chair Joyce, and distinguished members of the House Energy and Commerce Committee:

We welcome the opportunity to respond to the request for information on exploring a potential data privacy and security framework. This statement is largely based on past relevant research regarding issues related to data privacy, speech, and artificial intelligence. It will focus on the questions in Sections III, V, and VI of the request.

III. Existing Privacy Frameworks & Protections

A. Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group's efforts, including these frameworks' efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.

Internationally, comprehensive data privacy legislation such as the General Data Privacy Regulation (GDPR) in the European Union have often failed to protect consumers while limiting innovation and creating barriers to entry for startups and smaller players. Studies show that there is a lack of evidence to support the argument that the GDPR increased consumer trust around data collection.[1] In fact, after its initial implementation, many shared anecdotes of how the GDPR led to companies handing over data to wrong individuals[2] or without verification[3].

The GDPR also negatively affects the marketplace, making it more difficult for companies of all sizes to engage in common benign and beneficial uses of data without incurring additional

[1] Paul C. Bauer et al., "Did the GDPR Increase Trust in Data Collectors? Evidence From Observational and Experimental Data," *Information, Communication and Society 25*, no. 14 (2022).
[2] Irina Ivanova, "Amazon's Alexa Sent 1,700 Recordings to the Wrong Person," *CBS News*, December 20, 2018.
[3] Bobby Hellard, "Researcher Exploits GDPR Rules To Uncover Partner's Data," *ITPro*, August 9, 2019.

significant costs. Large companies shell out millions to ensure compliance[4] limiting their ability to innovate or dedicate these resources to better serving their customers, while small players find it more difficult to enter the market at all due to increased cost of conducting business. Indeed, there was a decreased development of new apps in Europe,[5] and decreased investment in startups overall in the short run following GDPR.[6]

If the U.S. were to adopt comprehensive data privacy legislation that is similar in breadth and costs to the GDPR, then it would also experience similar negative effects to that of the European Union. Europe's regulatory regime contributes to its lack of a robust tech market. These laws also do not encounter the same legal system around who will bear the burden of litigation costs. Additionally, specific facets of such regulations like a "right to be forgotten" might conflict with U.S. legal standards regarding free speech.

The U.S., with its dynamic and innovative tech industry, would be hindered if it looked to abroad for guidance on how to draft and implement data privacy legislation.

B. Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.

Every year, the number of states with data privacy legislation grows. When we wrote about this subject last year, there were 13 states that had passed data privacy legislation. As of now, that number has increased to 20 states and continues to grow.

The varying nature of state comprehensive data privacy laws create additional costs for businesses and confusion for consumers. One study found that a 50-state patchwork of data privacy laws could exceed $1 trillion over ten years, with at least $200 billion affecting small businesses.[7] Such costs would stifle the growth of businesses and limit their ability to innovate. Consumers may not understand why certain products or product features are not available in

[4] Damien Geradin et al., "GDPR Myopia: How a Well-Intended Regulation Ended Up Favouring Large Online Platforms – the Case of Ad Tech," *European Competition Journal 17*, no. 1 (2021).
[5] Thomas Claburn, "Europe's GDPR Coincides With Dramatic Drop in Android Apps," *The Register*, May 9, 2022.
[6] Ginger Jin et al., "The Short-Run Effects of GDPR on Technology Venture Investment," *VoxEU*, January 7, 2019.
[7] Daniel Castro et al., "The Looming Cost of a Patchwork of State Privacy Law," *ITIF*, January 24, 2022.

their state as well as what specific rights they have when it comes to obtaining or correcting their data.[8]

In some cases, given the cost of compliance and specific limitations of a state's law, such a law might have impacts well beyond its borders. Because of the costs or penalties for non-compliance, companies may choose to apply the most burdensome data privacy model nationwide, resulting in consumers in some states finding that their available options are influenced by another state's law.

The state data privacy legislation patchwork generates huge costs to businesses and innovators and leaves consumers with uncertainty and inconsistent access to products and product features based on the state where they reside. In 2022, more than 80% of voters polled supported a federal data privacy law.[9] It is not surprising that in the absence of a federal bill states began to enact laws to meet these preferences.[10] However, these state laws, even if enacted in all 50 states, would still provide more significant burdens and problems that create confusion for consumers and significant costs particularly for small businesses.

C. Given the proliferation of state requirements, what is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?

The state data privacy framework consists of layers of different requirements in different aspects of data privacy, burdening businesses and confusing consumers. Therefore, it is necessary that any federal data privacy law contains express preemption of state laws that sets a federal law as a ceiling not a floor. As previously mentioned, companies under the current framework may defer to the strictest state model nationwide or maintain state-by-state operations. Either way, these companies incur massive costs to do so.

In the absence of a federal preemption or judicial intervention, companies are experiencing a domestic "Sacramento Effect" that allows the state of California to pass de facto data privacy

---

[8] Alix Langone, "You Can't Use Google's New Selfie Art App in These States," *TIME*, January 17, 2018.
[9] Chris Teale, "Voters Overwhelmingly Back Major Provisions of Proposed Federal Data Privacy Law," *Morning Consult*, June 15, 2022.
[10] Alfred Ng, "The Raucous Battle Over Americans' Online Privacy Is Landing on States," *POLITICO*, February 22, 2023.

policy for the rest of the country. Its regulations around privacy — such as its California Consumer Privacy Act[11] — and the proposed framework around "automated decision-making" hinders innovation and may apply outside of its borders to the entire country.[12] Such a phenomena is not necessarily limited to California, but with its large market and role in the tech industry it seems to most commonly have such extra-territorial effects.

A federal, light-touch approach to data privacy that expressly preempts costly and burdensome state laws would allow the numerous uses of data that benefits businesses and consumers to continue while still ensuring that malicious uses and bad actors could be appropriately responded to. Allowing state laws to build on top of a federal law would not only fail to solve the patchwork problem, it would result in a federal law further adding to the costs and burdens of regulation.

V. Artificial Intelligence

AI has raised potential challenges to certain presumptions about the use of data as well as illustrated how static regulation can be an unexpected hindrance to dynamic innovation and disruptive technologies. It is important that a federal data privacy framework carefully consider the tradeoffs between privacy and other values as well as how such a framework might play out not only for existing technology and data uses but how it might impact future beneficial uses of data. Jennifer more fully discusses the complicated questions around data privacy and AI in her statement to the House AI Taskforce last year.[13]

Europe's policies illustrate the potential consequences of a more regulatory approach to both data privacy and AI on both AI development and deployment. For example, some AI products were unable to launch in Europe not because they were engaged in bad privacy practices but

[11] Cal. Civ. Code § 1798.100 et seq.
[12] California Privacy Protection Agency, "A New Landmark for Consumer Control Over Their Personal Information: CPPA Proposes Regulatory Framework for Automated Decision-making Technology," November 27, 2023.

[13] Jennifer Huddleston, Cato Institute, Testimony Before the Hearing on Privacy, Transparency, and Identity of the House AI Taskforce, 118th Cong., 1st sess., June 28, 2024.

because of uncertainty around their ability to comply with existing facets of data privacy law such as a right to deletion.[14]

As the question notes, however, there are also concerns about how AI policy and particularly state-level AI policy could impact both data privacy and AI regulation at a federal level. Regulation of the development of AI or its use of certain data by states could have an impact beyond a single state's borders. Limitations on the use of certain data in automated decision-making could make it more difficult to build AI tools that can consider various concerns around bias and discrimination or otherwise result in requiring more data collection in the future due to past minimization requirements. As Orly Lobel notes in her paper "The Law of AI for Good," AI is challenging existing frameworks around topics like right to privacy and automated decision-making in cases where automation and data maximization can actually provide better and more accurate opportunities and outcomes.[15]

At this point, over 20 states have passed consumer data privacy frameworks. While the current number of state level AI laws may be small, hundreds of bills are being considered this legislative year. Extending a state patchwork to AI would only be even more problematic for innovators and consumers than the current data privacy patchwork and could derail or deter the development of this important technology.

VI. Accountability & Enforcement

A. Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.

Policymakers should carefully consider the purpose behind data privacy legislation in granting enforcement authority and avoid calls to create a new agency. Data touches nearly all sectors of the economy risking a new digital or data regulator having a significant ability to impact not only technology but many other industries from agriculture to traditional retail as well.[16]

---

[14] Jennifer Huddleston, "The Consequences of Regulation: How GDPR Is Preventing AI," *Cato at Liberty (blog)*, June 22, 2023.
[15] Orly Lobel, "The Law of AI for Good," *Florida Law Review 75*, no. 6 (2023).
[16] Neil Chilson, "Creating a New Federal Agency To Regulate Big Tech Would Be a Disaster," *Washington Post*, October 30, 2019.

Grounding any delegation to an agency in the clearly defined harm and related response would help restrain potential overreach. Many data privacy questions might continue to fall within existing agencies that govern those fields. For more general data concerns, the impetus is typically consumer protection or fraud. For this reason, the Federal Trade Commission has and logically would continue to be the most appropriate enforcer for a general data privacy law.

B. What expertise, legal authorities, and resources are available—or should be made available—to the Federal Trade Commission and state Attorneys General for enforcing such a law?

As mentioned, data is transforming almost every industry and should not be thought of as only a technology industry issue. Any enforcement actions should be based on clear evidence of harm and seek to go after malicious actions not merely benign or even beneficial uses of data that some more privacy sensitive individuals find unnerving. In considering appropriate enforcement and enforcement options, policymakers must be careful to avoid privacy fundamentalism or wrongly maligning all uses of data.[17]

Policymakers should provide clear definitions to enforcement authorities around what constitutes a violation and set up guardrails to prevent potentially deterring positive developments with over-zealous enforcement. Policymakers should also clearly delegate appropriate authority to avoid an agency like the FTC attempting to expand its regulatory role over all facets of the economy that data touches.

If state attorneys general are to be enforcers, it is important to consider how different states might interpret ambiguous terms. As with a state-by-state patchwork, such an enforcement option risks that California and Florida might have significantly different interpretations of the law. This is particularly true if there is a lack of clarity on what is covered by the law and guidance on appropriate enforcement.

[17] Alec Stapp, "Against Privacy Fundamentalism in the United States," *Niskanen Center*, November 19, 2018.

Conclusion

We thank you for the opportunity to submit comments on this important topic and are happy to have further conversations based on the research referenced in this response as well as our other research on this topic as the committee continues to consider the important questions of an appropriate federal data privacy framework that can continue to allow innovation while providing appropriate protections and certainty for both consumers and entrepreneurs.