**Statement**

**of**

**Jennifer Huddleston**

**Senior Fellow in Technology Policy**
**Cato Institute**

**before the**

**AI Task Force**
**United States House of Representatives**
**June 28, 2024**

Representatives Obernolte, Lieu, and attendees,

My name is Jennifer Huddleston, and I am a Senior Fellow in Technology Policy at the Cato Institute. My research focuses primarily on the intersection of law and technology, including issues related to data privacy, free speech, and the governance of emerging technologies, such as artificial intelligence (AI). Therefore, I welcome the opportunity to provide insights around questions regarding data privacy, transparency, and AI.

In this statement, I will focus on the following three key points:

- Policymakers are right to focus on questions regarding data privacy and seek to create certainty for both consumers and innovators around their rights; however, these policies should focus on harm and specific bad actions rather than presuming that all uses of data are equally problematic;
- A highly regulatory approach to data privacy can create problems for the development of AI, especially around issues such as data minimization;
- While transparency can be a good way to assuage consumer concerns, transparency for AI can also raise concerns related to speech and the development of this important technology.

**The Need for Federal Data Privacy Legislation**

As of 2021, more than 80% of both Republican and Democrat voters said Congress should make data privacy a major or top priority.[i] Few other issues related to technology reach anything close to similar numbers. However, given the number of industries — from agriculture to finance to medicine to social media — using data in beneficial and impactful ways, Congress should be careful to not regulate for the mere sake of responding to such requests, but look at underlying

concerns. While seeking to protect consumers from harmful data practices is well intentioned, many policy proposals would also impact free speech, the beneficial uses of data, and further innovation in fields such as AI. With such in mind, policymakers should consider the impacts that privacy regulation could have on these other important values and seek to narrowly tailor any regulation to focus on clearly defined harms.

As of June 2024, 18 states have passed comprehensive data privacy legislation. These laws vary in both their requirements and covered content and risk creating a confusing patchwork for innovators, small businesses, and consumers. Additionally, such an approach comes at significant costs, with one study finding a 50-state patchwork could exceed $1 trillion in compliance cost within 10 years, with at least $200 billion from the impact on small businesses.[ii] Similar to European authorities (that will be discussed more later), some states may seek to apply the existing data privacy rules in ways that could create a patchwork of regulations that not only create costly compliance but, in some cases, could keep beneficial AI technology from being deployed or developed. For example, California's Consumer Privacy Protection Act is currently engaged in rulemaking around automated decision-making technology that would significantly impact AI.[iii] This potential impact on the development of this important technology is just the latest case for federal preemption of the growing patchwork.

While the patchwork of privacy laws is concerning, a federal approach must also consider impacts to the benign and beneficial uses of data in AI and beyond. Too often, policy uses terms like "commercial surveillance" or "dark patterns" to describe not only malicious actions, but benign and beneficial data practices that personalize user experience and provide clarity before canceling a service or ordering a product. But the need to define harm beyond mere collection is

even more important as AI gains prominence so that potentially beneficial applications are not prevented from being developed or deployed merely because they rely on AI.

When it comes to data privacy, it is also important that policymakers consider if there are clear cut harms not only from private actors but also from government abuse, particularly when it comes to AI development and deployment by government agencies. One positive step towards data privacy would be to clarify when and how the government can use the data it collects and when it can request data from private actors.

**Data Privacy Regulation Could Accidentally Prevent AI Deployment and Development**

While some of the concerns about AI might be resolved through improved awareness of data privacy options or laws that apply to malicious actions around data, a stringent approach could have negative consequences that prevent the development or deployment of AI. This is true particularly around requirements for deletion or data minimization that may seem like a best practice in the internet era but could disrupt AI.

AI is, by its nature, reliant on large amounts of data. Many underlying concerns like algorithmic bias are improved by using larger, more diverse data sets. In fact, it may not be data minimization, but the use of even more data — including sometimes sensitive information — that can create more accurate models in areas such as medicine. As University of San Diego Professor Orly Lobel notes in her paper The Law of AI for Good, "But what if the very fact that data is collected brings more health, safety, equality, accuracy, and socially valuable innovation? In other words, what if the tradeoffs are not simply between individual rights and cheaper services, but are also between different fundamental rights?"[iv] Policymakers must carefully consider that while privacy may well be an important right, that right does not exist without

tradeoffs for other rights, including potentially lifesaving innovations. As the late economist Thomas Sowell once noted, "There are no solutions. Only tradeoffs."[v]In many cases, policymakers are best to leave consumers to choose the tradeoffs that best fit their needs and intervene only in cases where harm occurs or is extremely likely to occur, particularly in irreversible ways. But the potential application of data in AI remains not fully known and limitations could prevent beneficial applications along with risky ones.

Europe illustrates how a highly regulatory approach may be an ill-fit for AI deployment and development not because of poor privacy practices, but because of the difficulty in certain compliance requirements. Meta[vi], Google[vii], and ChatGPT[viii] all faced a delay in launching their products in Europe not because of inherent violations of privacy, but because of concerns largely stemming from issues such as how consumer consent was obtained or concerns around questions such as data deletion when a model has already been trained. Questions such as consent and the ability to revoke it may be evolving with AI; however, cumbersome regulations are unable to adapt and can prevent benign and beneficial uses of data in AI. Technology often moves faster than regulation and if regulation is based on today's technology, it can be an ill-fit for the next generation.

With the potential unintended consequences in mind, policymakers must ensure that any approach to data privacy remains flexible to adapt to both future concerns and future technologies and is based on the harms it seeks to prevent rather than presuming all data uses equally problematic. This has traditionally led to sector specific approaches in the US such as HIPAA, COPPA, and Graham-Leach-Bliley. When considering privacy and AI, policymakers should look to ways that maximize consumer choice and innovation in many cases and apply limits to only problematic and malicious uses. They should also consider the government's own

uses of data and how clarity and restrictions might assuage certain civil liberties concerns about AI.

**Transparency Mandates v. Transparency Best Practice**

One common solution to many concerns in both AI and data privacy is to mandate transparency. While transparency may often be a best practice to inform consumers how their data is used, transparency mandates from the government may fail to achieve their goal, not be adaptable to different technologies, or even negatively impact other values like free speech or innovation.

AI and other data users should seek to provide those they collect data on with information to make knowledgeable choices about their privacy preferences. This type of transparency can occur in several different ways depending on the nature of the product. Unfortunately, a policy approach often mandates a certain method of transparency or disclosure that may not fit all products or situations. The best way to provide information about the data used by a program like ChatGPT, for example, may be different from an AI that provides information about potential heart disease from an eye scan.[ix] Many mandates for transparency, however, often treat all uses of AI the same and do not consider the different deployers of what may even be similar models. For example, photosorting software can help individual users identify friends and family, but it can also raise civil liberties concerns when deployed in other scenarios.

Mandated transparency may also not actually improve consumer education around their privacy choices. First, many consumers may grow fatigued and frustrated with the constant pop ups and consents as they do with current cookie pop ups. Second, a government mandate — as opposed to an organic best practice — is more likely to communicate to consumers in ways that are not

seamless with products and in terms they see fit for their audience by focusing on compliance instead.

Finally, mandated transparency in AI is particularly tricky. Often, the ways data is used are of key value to the company. Government transparency mandates could require the disclosure of intellectual property or other competitively valuable information and concerningly set up platforms for pressure from the government to take or not take certain actions.[x]

Many companies will likely provide transparency in response to consumers' expectations and demands. Those who do not may face industry or consumer pressure to do so. Such an approach allows for more flexibility than a regulatory mandate would and raises less concerns about the potential tradeoffs. Where policymakers could consider greater transparency is the government's own deployment of AI as well as any requests that AI companies produce certain data.

**Conclusion**

AI policy is unlikely to resolve underlying questions of data privacy and some concerns about AI may be better understood as continuing concerns about data privacy. A federal data privacy framework could have implications for the development of AI and other current technologies, including tradeoffs for underlying concerns and potentially life-saving applications. Policymakers should consider these potential tradeoffs not only for the internet era but for the innovative uses of data in the AI era. America has traditionally focused on those malicious actors and clear areas of harm while allowing innovation in the benign and beneficial uses of data in a variety of industries. When it comes to AI, continuing such an approach is perhaps even more important.

[i] Sam Sabin, "States Are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data," *Morning Consult*, April 27, 2021.

[ii] Daniel Castro et al., "The Looming Cost of a Patchwork of State Privacy Laws," *Information Technology and Innovation Foundation*, January 24, 2022.

[iii] 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.

[iv] Orly Lobel, "The Law of AI for Good," San Diego Legal Studies Research Paper 23-001, January 30, 2023.

[v] Thomas Sowell Quotes (@ThomasSowell), "There are no solutions, there are only trade-offs," Twitter post, August 23, 2022, 9:58 a.m., https://x.com/ThomasSowell/status/1562076748874907648.

[vi] Foo Yun Chee, "Meta Pauses AI Models Launch in Europe Due to Irish Request," *Reuters*, June 14, 2024.

[vii] Clothilde Goujard, "Google Forced to Postpone Bard Chatbot's EU Launch Over Privacy Concerns," *POLITICO*, June 13, 2023.

[viii] Elvira Pollina, "OpenAI's ChatGPT Breaches Privacy Rules, Says Italian Watchdog," *Reuters*, January 29, 2024.

[ix] National Eye Institute, "AI Can Identify Heart Disease From An Eye Scan," *National Institutes of Health*, January 25, 2022.

[x] Adam Thierer, "The Battle Over AI Regulation Will End in a Big Fight Over Transparency and Audits," *Medium*, April 6, 2024.