The Balance Between Privacy and Utility  
Position Paper 2

DSE6003 – SU1 2025  
Dr. Yamil Guevara  
Nick Lagoni  
6/22/2025

# Introduction

Dear members of the *House Subcommittee on Innovation, Data, and Commerce,*

Thank you for the opportunity to provide testimony and recommendations on how the Subcommittee should address the conflict between data privacy and utility. The central question facing the Subcommittee on this issue is whether or not data security can be maintained while extracting the most value from available data; as well as which to prioritize, in the event that both utility and privacy cannot be equally focused on. The goal of this report is to explore this conflict and seek to develop a balanced plan to promote both data privacy and utility.

# Privacy vs. Utility

## Maximizing Data Privacy

The threats to consumer data privacy are increasing as technology rapidly accelerates and data is harvested, used, and sold by companies without consumer awareness or understanding (U. S. Government Accountability Office 2022). As these threats accelerate, data protection measures are becoming increasingly important. Data breaches pose a significant risk to individual consumers’ personal information and livelihoods. Additionally, data breaches damage public trust in companies and institutions, both private and public. This represents a risk to the profitability of companies as well as the function of government agencies. Individuals charged with managing data such as Chief Technology Officers have a responsibility to prioritize the secure and protected used of any data under their care, both for the sake of the company or institution and the individual consumers. There is a growing public demand for more protection and control over individual consumer’s data are used, with this demand being directed at both private companies and the government (Arbanas et al. 2023).

## The Economy of Data Utility

Big Data is a major contributor to modern day innovation and business decision-making; the value that Big Data provides has transformed many sectors by empowering them to make accurate and informed decisions (Seghier 2021). This represents a major economic benefit, allowing companies to gain insight into consumer behavior, their own operations, market trends, future needs, and to personalize consumer experiences and advertising. The use of Big Data has also revolutionized health care, improved public services, improved education, and empowered activists and policymakers to address Climate Change (Harvard Online 2024). The ability to leverage the utility of data to its fullest has represented not only economic growth and upheaval but also societal benefits. Limiting the utility of data could diminish the benefits and slow the rapid growth of multiple sectors, including important pillars of society like education and healthcare. Data that is inherently personal to consumers is important for improving services in fields like healthcare and education. Sensitive patient data is used to improve treatment plans, research new disease treatments, prevention, and diagnoses (NEJM Catalyst 2018). While this data is sensitive in nature and personal to those patients, the innovations that have stemmed from it would not be possible without it’s usage.

## Balancing Utility and Privacy

We have established that both the utility and privacy of data are important to both companies and consumers. Maximizing the utility of data represents a potential to revolutionize our society and reach unprecedented levels of growth and productivity, while failing to protect our usage of that data represents a significant risk to individual consumers who are at risk of having their identities stolen, being biased against, and having their personal data stolen by or sold to malicious actors. Companies must be intentional about their use of data and the resources they put into protecting it. It is possible to use data both effectively and securely, and companies have been doing so, self-regulating to avoid reputational damages while maximizing utility. The Subcommittee has a responsibility to find a way to establish what has been best-practice into codified and enforceable law.

# Recommendations

## National Standard for Data Privacy

While there are potent data privacy protections in place at the state level, more specifically in the California Consumer Privacy Act, the national standard for data protection is comparatively lacking. There is currently no single, comprehensive federal law governing data protection. Instead, consumers are protected by a patchwork of federal laws for specific data types and use cases (i.e., the Health Insurance Portability and Accountability Act, the Family Education Rights and Privacy Act) and state and local legislation. The U.S. is inconsistent compared to a governing body like the European Union, which has one of the most robust and unified pieces of data privacy legislation, the General Data Protection Regulation. Adoption of a single robust federal law like the EU’s GDPR would additionally promote global data protection, as foreign businesses that deal with the U.S. find it more straightforward and efficient to comply with the most strict requirements, rather than selectively applying data protection policies (Rustad and Koenig 2019). This is known as the “Brussels Effect” and has been seen already from the implementation of the GDPR. However, The U.S. represents a significant player in the global data economy and thusly holds sway over the global big data ecosystem (Rustad and Koenig 2019, Chakravorti et al. 2019). There is a growing desire for legislation to force the issue of privacy by consumers as well, so this would be a publicly popular initiative (Arbanas et al. 2023).

## Subsidizing Privacy Innovations

The federal government could provide grants and subsidies to companies and institutions that show initiative when it comes to protecting consumer data. This could come in the form of tax incentives for companies that meet higher protection standards or grants for developing new data anonymization techniques and Privacy-Enhancing Technologies (PETs). Previous similar funding opportunities have been provided, such as the Privacy-Preserving Data Sharing in Practice (PDaSP) grant from the National Science Foundation, (National Science Foundation 2024).

## Collaboration with the Federal Communications Commission

While the Subcommittee is already a valuable resource for regulating data privacy, there needs to be a dedicated body that investigates alleged violations or concerns and enforces the legislation passed. This structure exists already in the Privacy and Data Protection Task Force within the FCC. Any legislation planned by the Subcommittee should include a place for feedback from the FCC on issues they have faced under current regulations, common violations they see, and tools they require to be able to best enforce data privacy.

## Public-Private Collaboration

The Subcommittee should establish regular focus groups or roundtable discussions where public and private stakeholders can come together to express their needs and work towards a common solution on data protection and privacy. The world of Big Data is perpetually evolving, and the needs of businesses and consumers will evolve at that same rate. The Subcommittee should build a living framework to continuously assess and reform legislation, with the input of stakeholders from both sides of the issues, in order to remain balanced between data privacy and utility.

# Conclusion

As explored in this report, both the effective use of data and the proper protection of data privacy are imperative as we navigate the digital era. Emphasizing data utility represents a powerful driving force for economic growth, scientific research, and healthcare optimization. Companies and the government have a responsibility to moderate the use of personal data, as improper or unprotected use represents a risk to individual consumers, companies, and even national security. A unified, federal law on data privacy is becoming a necessity for proper data use and protection in the United States. *The Subcommittee on Innovation, Data, and Commerce* should prioritize the federalization of data privacy legislation, while incorporating input from stakeholders to create a living process for data protection and utilization going forward. Combined with incentives for data excellent privacy practices and PET innovation, the Subcommittee has the opportunity to provide a robust framework for secure and effective data use across all industries, promoting significant growth, safely.

# References

Arbanas, J., P. Silverglate, S. Hupfer, J. Loucks, P. Ranab, and M. Steinhart. 2023, September 5. Consumer data privacy and security | Deloitte Insights. https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html.

Chakravorti, B., A. Bhalla, and R. S. Chaturvedi. 2019, January 24. Which Countries Are Leading the Data Economy? Harvard Business Review.

Harvard Online. 2024, February 28. Pros and Cons of Big Data | Harvard Online. https://www.harvardonline.harvard.edu/blog/pros-cons-big-data.

National Science Foundation. 2024, June 27. Privacy-Preserving Data Sharing in Practice (PDaSP). https://www.nsf.gov/funding/opportunities/pdasp-privacy-preserving-data-sharing-practice/506327/nsf24-585.

NEJM Catalyst. 2018. Healthcare Big Data and the Promise of Value-Based Care. Catalyst Carryover 4.

Rustad, M. L., and T. H. Koenig. 2019. Towards a Global Data Privacy Standard. Florida Law Review 71:365.

Seghier, M. L. 2021. An active human role is essential in big data-led decisions and data-intensive science. F1000Research 10:1127.

U. S. Government Accountability Office. 2022, September 13. Consumer Data: Increasing Use Poses Risks to Privacy | U.S. GAO. https://www.gao.gov/products/gao-22-106096.