

March 6, 2023

Ms. Stephanie Weiner
Acting Chief Counsel
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: NTIA– 2023–0001

Dear Ms. Weiner:

This letter is submitted on behalf of Business Roundtable, an association of chief executive officers of America’s leading companies. As major employers in every state, Business Roundtable CEOs lead companies that support 37 million American jobs and almost a quarter of U.S. GDP. Our companies—who represent every sector of the U.S. economy, including technology, communications, retail, financial services, health, public safety and security, manufacturing, hospitality, insurance and others—rely on data and data-driven processes and solutions every day to deliver, improve and market innovative products and services across the United States and around the world. Consumer trust and confidence are essential elements of our businesses and our relationship with our customers, including customers from disadvantaged communities.

We appreciate the opportunity to participate in the Request for Comment (the “Request”) released by the National Telecommunications and Information Administration (“NTIA”) on January 20, 2023, relating to whether and how commercial data practices can lead to disparate impacts and outcomes for marginalized or disadvantaged communities.¹ NTIA issued the Request with the laudable goal of examining how privacy may intersect with considerations of justice for marginalized or disadvantaged communities, and determining what solutions may be appropriate.

Introduction

Business Roundtable member companies take data privacy and security very seriously. Our companies also understand that many American consumers may not feel in control of their personal data and how it is collected, used, shared, and protected, and that this concern may be greater in marginalized communities.

¹ Department of Commerce, NTIA, Privacy, Equity and Civil Rights Request for Comment, 88 Fed. Reg. 3,714 (Jan. 20, 2023).

Consistent with consumer expectations and responsible business practices, our member companies already undertake significant efforts to limit the collection, use, and sharing of consumer data, and to protect the security of such data. For example, our member companies maintain robust data privacy and security compliance programs, implement internal and external privacy policies, provide consumers with meaningful notice and opportunities for consent, and train employees to emphasize the importance of keeping their customers' data confidential and secure. In addition, Business Roundtable member companies are at the forefront of responsible innovation, developing and implementing best practices regarding how new technologies such as artificial intelligence ("AI") should be utilized by businesses in ways that mitigate the potential for unfair bias.

In January 2022, Business Roundtable launched the "Roadmap for Responsible Artificial Intelligence," an initiative to guide the responsible development and use of AI.²

The [Roadmap](#) provides a set of principles to guide businesses as they implement Responsible AI and reflects the perspectives and real-world experiences of companies from every sector of the economy, including AI developers, deployers and end users. Alongside the Roadmap, Business Roundtable also released a set of policy recommendations to encourage AI governance, oversight and regulation that build public trust in AI while enabling innovation and promoting continued U.S. leadership. Additionally, Business Roundtable recently published a collection of case studies demonstrating the many ways that companies are leveraging AI and data to operationalize Responsible AI principles and directly benefit consumers and communities.³

Business Roundtable believes that the goals articulated in the Request would be most effectively achieved through the enactment of comprehensive federal privacy legislation that provides Americans, including disadvantaged communities, with data privacy and security protections that apply throughout the United States, for which Business Roundtable has strongly advocated.⁴ A national, uniform consumer privacy law would ensure that consumers in California are provided the same privacy protections as those in New Hampshire, an outcome which cannot be achieved through a state-by-state approach or a federal rulemaking that would not apply holistically to the entire internet ecosystem.

In terms of the key attributes of a national privacy framework, NTIA should carefully consider whether certain proposals, including restrictive data minimization, collection limitations or external audits would restrict beneficial uses of consumer data or divert resources that could be used to benefit consumers, including those from disadvantaged communities. Many businesses

² Business Roundtable, Roadmap for Responsible AI (Jan. 26, 2022), <https://www.businessroundtable.org/policy-perspectives/technology/ai>.

³ Business Roundtable, Business Roundtable Companies Put AI Recommendations into Practice (Jan. 25, 2023), <https://www.businessroundtable.org/ai-innovation-at-work-putting-principles-into-practice>

⁴ Business Roundtable, Framework for National Privacy Legislation (Dec. 6, 2018), <https://www.businessroundtable.org/policy-perspectives/technology/privacy>.

rely on consumer data to provide valuable products and services on which consumers have come to rely, and that restrictive rules might prohibit. For example:

- Financial services firms and their customers rely on superior data-enabled fraud detection tools that help prevent millions of unauthorized transactions every year. The accuracy of fraud tools is data-driven, which is why such tools have been granted exemptions under the Gramm-Leach-Bliley Act (“GLBA”).
- Health care innovations that improve patient outcomes are enabled through data collection and exchange consistent with prevailing restrictions under the Health Information Portability and Accountability Act⁵ (“HIPAA”).
- Energy companies collect and analyse data to assist consumers and enterprises in optimizing energy efficiency and reducing carbon footprints.
- The cybersecurity community leverages security data to provide effective, real-time cybersecurity security solutions.
- Retail firms use customer data to manage customer loyalty and rewards programs, and to ensure that inventories track changing customer demand.

Regardless of sector, a national framework for data-driven technologies, including AI, should focus on principles-based requirements which provide a flexible approach that can evolve as the technologies evolves.

NTIA’s Request addresses important societal questions, and policymakers will take NTIA’s recommendations seriously. Our hope is that these recommendations reflect solutions that will ensure a community’s data rights are not affected by state boundaries and take into account the beneficial uses of consumer data. In the sections that follow, we provide answers to specific questions posed in the Request.

I. Comprehensive Privacy Legislation is the Only Viable Solution to Ensure That All Communities Are Afforded Equal Privacy Protections.

Question 1. How should regulators, legislators, and other stakeholders approach the civil rights and equity implications of commercial data collection and processing?

Question 4. How do existing laws and regulations address the privacy harms experienced by underserved or marginalized groups? How should such laws and regulations address these harms?

Question 5. What are the principles that should guide the Administration in addressing disproportionate harms experienced by underserved or marginalized groups due to commercial data collection, processing, and sharing?

⁵ Pub. L. 101-191.

To promote privacy and equity with respect to online data collection, NTIA should recommend that the Biden Administration vigorously pursue comprehensive privacy legislation that creates a single national standard rather than separate and misaligned agency rulemakings that would simply add yet another inconsistent set of guidelines, recommendations or requirements that would exacerbate the disparities in privacy rights we see today. There is a pressing need for clear and comprehensive privacy requirements that protect all consumers and provide certainty to businesses.

The United States is home to a growing patchwork of privacy laws, which vary depending on where an American lives and the type of data at issue. The U.S. national privacy regime is comprised of a growing number of state-level privacy laws (currently enacted in California, Virginia, Colorado, Utah, and Connecticut), a variety of topic- and sector-specific federal statutes (*e.g.*, HIPAA, the Fair Credit Reporting Act, the Children’s Online Privacy Protection Act, GLBA), and case-by-case Federal Trade Commission (“FTC”) and State Attorneys General enforcement of federal- and state-law prohibitions on unfair or deceptive acts and practices. The existing U.S. system by its nature creates different privacy rights for similarly situated Americans based on their state of residence, the type of data at issue and whether a company with which the consumer interacts is targeted for enforcement. This haphazard approach only exacerbates existing disparities by fragmenting privacy rights across geographies and jurisdictions.

Administrative actions without comprehensive legislation will not solve this problem. For example, the FTC recently began a rulemaking process on “commercial surveillance.”⁶ Because the FTC Act itself does not preempt state privacy or consumer-protection laws, an FTC rule here in the absence of new legislation likely would not create a holistic national framework. As a result, the FTC’s new requirements would exist alongside—and perhaps in tension with—the myriad other privacy requirements already in place. Consumers will be forced to engage with increasingly complex privacy notices and choices, and likely will be confused about the applicability of the FTC’s rules as compared to state and federal laws. Further, consumers with greater means will be more likely to navigate this system successfully in the event of privacy violations, identity theft or other issues, leaving individuals from marginalized communities further behind.

Rulemaking in this space also could present companies of all sizes with difficult compliance issues that negatively affect consumers. For example, companies in the health and medical fields have well-established privacy and security practices and procedures governed by statutes such as HIPAA; adding new or different requirements will only burden the numerous entities that comply with this law and the rules promulgated thereunder every day. On data security, many companies look to the cybersecurity, privacy and AI risk management frameworks published by the National Institute of Standard and Technology (“NIST”)⁷ and the various

⁶ FTC, Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022).

⁷ NIST, Cybersecurity Framework, <https://www.nist.gov/cyberframework>.

recommendations made by the Department of Homeland Security's cybersecurity arm, the Cybersecurity and Infrastructure Security Agency ("CISA"). Data security requirements that deviate from recommendations made by NIST and CISA will not only complicate compliance but may also reduce the effectiveness of corporate data security programs.

A national consumer privacy law would strengthen protections for consumers in communities across the country, recognizing that consumers' digital lives and experiences are not restricted by state boundaries, while offering Congress the opportunity to harmonize new requirements with the other federal obligations under which companies operate.

Business Roundtable understands that crafting sound data privacy requirements is a difficult endeavour, and that many competing interests must be weighed against each other while ensuring that all Americans benefit from the digital economy. But only Congress can create one nationwide framework. Thus, our recommendation is that NTIA should encourage Congress to continue its work towards forging lasting compromises and legally sustainable requirements in this area.⁸

II. Overly Broad Rules Regarding Data Minimization, Purpose Limitations, Automated Decision-making and Requirement of External Audits Could Prohibit Many Practices that Benefit Consumers and are Essential to Business Operations

Question 1.f. What is the interplay between privacy harms and other harms that can result from automated decision-making, such as discriminatory or arbitrary outcomes? How should these two issues be understood in relation to one another in the context of equity and civil rights concerns?

Question 5.d. In considering equity-focused approaches to privacy reforms, how should legislators, regulators, and other stakeholders approach purpose limitations, data minimization, and data retention and deletion practices?

Question 6.c. What roles should third-party audits and transparency reporting play in public policy responses to harmful data collection and processing, particularly in alleviating harms that are predominantly or disproportionately experienced by marginalized communities? What priorities and constraints should such mechanisms be guided by? What are the limitations of those mechanisms? What are some concrete examples that can demonstrate their efficacy or limits?

NTIA is appropriately evaluating how new, concrete proposals might help consumers in disadvantaged communities. However, in considering approaches such as data minimization,

⁸ Business Roundtable, Comment on the American Data Privacy and Protection Act (September 30, 2022), [Business-RoundtableCommentsOnTheAmericanDataPrivacyandProtectionAct9.30.22.pdf](#)

purpose limitations, restrictions on automated decision-making or requiring external audits, NTIA should support a risk-based approach that carefully considers the many benefits that consumers enjoy because of products or services that rely on analysis of consumer data. Overly restrictive rules regarding data collection and use risk eliminating the many benefits consumers currently enjoy, undermining whatever other gains NTIA might hope to achieve.

Responsible collection and use of consumer data enables companies to innovate and improve the efficacy and efficiency of existing products and services.⁹ There is no denying that there is a direct relationship between data and the outcomes of automated decision systems. It is critical that these systems are trained on robust and sound data, which helps to maximize consumer protections while ensuring beneficial uses. Companies can tailor offerings to customers' unique needs and preferences, improve customer service and strengthen the security of consumer services. Some of these beneficial data uses are integral to business operations and to the consumer experience. And some technologies still in the nascent stages of development, such as automated decision-making, may halt development in the United States if regulators impose undue restrictions, particularly if competitor nations are not similarly restrictive.

Specific examples collected from Business Roundtable member companies regarding these practices clarify some of the harm that could come if regulators were to adopt broad restrictions requiring data minimization and narrow purpose limitations:¹⁰

Health care. Analysis of personal data and other information is essential to making advances in medicine and medical services for patients. Personal data can propel prevention and diagnoses of health conditions and accelerate development of medical technologies, allowing rapid advances in general medical knowledge, facilitating precision medicine and saving patient lives. Companies pursue these significant benefits while protecting the privacy of individuals through use of certain technologies and processes, such as deidentification, pseudonymization and anonymization, transparency, and preference management—some of which are required by existing health privacy laws. Grouping health data (including data linked to a confirmed medical device) and data used for purposes of medical research, innovation, and patient-centric support with other types of non-health-related commercial data for the purpose of regulation would adversely impact innovation, care delivery and research, all of which are critical for providing lower cost health care services in historically disadvantaged communities.

⁹ See *infra* n. 2.

¹⁰ Business Roundtable has produced numerous reports that highlight positive uses of consumer data and other benefits that could be potentially jeopardized by the FTCs rulemaking here. See, e.g., Business Roundtable, *Business Roundtable Roadmap for Responsible Artificial Intelligence* (Jan. 2022), https://s3.amazonaws.com/brt.org/Business_Roundtable_Artificial_Intelligence_Roadmap_Jan2022_1.pdf; Business Roundtable, *Putting Data to Work* (2015), <https://s3.amazonaws.com/brt.org/archive/reports/BRT%20PuttingDataToWork.pdf>.

Financial Services. Credit and payment systems rely on deidentified and securely stored consumer data to provide an array of core services to customers. Critical security functions like fraud prevention, anti-money laundering and cybersecurity protections depend on data-driven technologies to be effective and accurate. Financial services firms also leverage data to better serve historically underserved communities.

Energy. Many energy companies are heavily regulated by state and federal agencies, and routinely collect and use customer data to improve services and achieve energy efficiency and emission reduction goals. For example, consumer data related to energy usage (e.g., via smart thermostats) allows energy providers to offer customers personalized options for how to reduce energy use and expenditures. Smart thermostats also can help identify whether a consumer's HVAC system is working by comparing home temperatures to weather data. Data obtained from connected devices is used to improve commercial building efficiency, helping companies across sectors meet their net-zero-carbon emission goals. These efficiencies drive energy savings, lower costs and emissions reductions that directly benefit marginalized communities which often experience the harshest climate impacts.

Cybersecurity. Cybersecurity companies regularly leverage security data, including IP addresses, device and network information, URLs/domains, session data, threat intelligence data and other telemetry data for the purposes of security research, services and solutions, such as incident prevention, detection and response. Restricted access to such security data can have serious and significant impacts on our collective real-time cybersecurity defense, particularly at a time when cyber attacks are becoming increasingly sophisticated and automated.

Communications. Companies that offer communications services to consumers use data in many of the ways other companies do—to offer new and improved services to customers and to improve user experience. But these companies also regularly use consumer data to perform vital and basic business functions such as maintaining network operations, identifying and repairing infrastructure problems, and diagnosing and remedying service issues. These day-to-day operations are pivotal for improving network reliability and availability in historically disadvantaged areas to further narrow the digital divide.

Retail. Consumer data is vital to understanding customer needs, including whether new features might be beneficial, more convenient or more relevant to consumers. Indeed, algorithmic decision-making is an additional, vital tool that companies use to improve the consumer experience by enabling self-service portals, addressing consumer preferences and speeding customer service. As a result, companies can provide consumers with a more personalized experience and offer consumers products and services based on their preferences. Depending on what restrictions might be contemplated by regulators, retail firms, particularly in the food services sector, might not be able to implement key business processes such as automated inventory management or integrated loyalty programs. These barriers could

prevent retail firms from being able to recognize and tailor services to unique customer needs, presenting equity challenges for underserved communities.

E-Commerce. Anonymized consumer data also allows companies to improve the customer experience through updating key features of retail webpages. For example, measuring click-through rates on various pieces of content enables retailers to optimize their content. Location-based personalization allows companies to increase the accuracy of their advertising by showing only products that are available in the consumer's city or state, simplifying the online experience and tailoring offerings to match community preferences and needs.

Advertising. Companies use consumer information to help connect consumers with products or services that suit their interests, providing additional information that helps consumers make more informed choices. Many brands rely on customer data that they obtain from their own customers, using that information to provide more-relevant products and services to their customers. Strict limitations on using customer information to show targeted advertising to potential new customers ultimately would harm consumers and competition, as advertising would revert to the antiquated "spray and pray" model that (a) inundates consumers with information irrelevant to their consumption priorities and (b) drives up the cost of customer acquisition for companies. These limitations could affect the ability for companies to engage with and provide meaningful, customized services to individuals in historically underserved areas.

Conclusion

Business Roundtable shares NTIA's desire to protect consumers—especially those from marginalized communities—from unscrupulous privacy and security practices. This goal can be achieved in a meaningful way for all consumers only through federal legislation that establishes one national standard that provides strong, consistent consumer privacy rights throughout the United States.

For these reasons, we urge NTIA to work with Congress to forge a lasting legislative compromise on these important issues, and to provide greater clarity to regulators, industry and consumers, with respect to the scope of the government's privacy and data security authority. We would be happy to discuss these comments or any other matters you believe would be helpful. Please contact Paul Jackson, Vice President, Business Roundtable, at pjackson@brt.org or (202) 467-5269.