ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

Before the

National Telecommunications Information Administration

Washington, D.C.

In the Matter of:	)	
	)	
	)	
	)	Docket No. 230103-0001
Privacy, Equity, and Civil Rights	)	
	)	
	)	
	)	

March 6, 2023

CONTENTS

Introduction 2
Unintended Consequences of Privacy Regulation 2
Recommendations 4
Conclusion 6

INTRODUCTION

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA) request for public comment concerning privacy, equity, and civil rights.[1] ITIF is a nonprofit, non-partisan public policy think tank based in Washington, D.C., committed to articulating and advancing pro-productivity, pro-innovation, and pro-technology public policy agendas around the world that spur growth, prosperity, and progress.

UNINTENDED CONSEQUENCES OF PRIVACY REGULATION

2. *Are there specific examples of how commercial data collection and processing practices may negatively affect underserved or marginalized communities more frequently or more severely than other populations?*

Data privacy regulation intended to protect consumers can have unintended consequences. In its request for comment, NTIA focuses on how data collection and processing may negatively affect underserved or marginalized communities. Yet these groups would also suffer the greatest harm from overly broad or burdensome privacy regulation.

For example, any regulation that bans or limits targeted advertising will disporportinately negatively impact low-income individuals. Targeted advertising is the backbone of the modern Internet economy, enabling higher ad revenues, which in turn alows a wide variety of businesses, big and small, to offer their services for free or a reduced price. While this practice does require online services to collect relevant data on user behavior in order to tailor advertisements to each user's needs and interests, contrary to popular misconceptions, it rarely involves online services sharing the data they have collected with third parties.[2]

Instead, online services sell the opportunity for advertisers to target certain demographics. The advertiser pays the online service to show an ad to users who are more likely to click on it and potentially buy the advertiser's product or service or support the advertiser's cause. This benefits all parties involved: advertisers reach specific

[1] "Privacy, Equity, and Civil Rights Request for Comment," National Telecommunications and Information Administration, January 20, 2023, https://www.federalregister.gov/documents/2023/01/20/2023-01088/privacy-equity-and-civil-rights-request-for-comment.

[2] Daniel Castro, "Congress Needs to Understand How Online Ads Work to Pass Privacy Legislation," ITIF, March 2, 2023, https://itif.org/publications/2023/03/02/congress-needs-to-understand-how-online-ads-work-to-pass-data-privacy-legislation/.

audiences more easily than ever before, online services gain a source of revenue, and users have access to free online services and see ads that are more relevant to them.[3]

Regulation banning targeted ads, as well as overly broad privacy regulation that limits online services' ability to collect enough data in order to target ads to their users, would likewise harm all parties involved: advertisers would have more difficulty reaching specific audiences, online services would lose a source of revenue, and as businesses that relied on targeted advertising to offer certain services for free or at a reduced price would have to start charging or raise their prices, users would either have to pay those prices or stop using those services.

Wealthier individuals and households have more resources to afford to pay for online services. The consumers who would suffer the most in an Internet economy without targeted ads, or with less effective targeted ads, are low-income consumers. In the United States, there is a correlation between race and socioeconomic status, with white and Asian households earning more on average than black, Hispanic or Latino, American Indian or Alaska Native, and Pacific Islander households over the 2014 to 2016 period, according to the Bureau of Labor Statistics.[4]

In regulating privacy to advance civil rights for marginalized communities, the U.S. government should avoid provisions that would harm the very populations it is trying to protect. Not only does the current ad ecosystem lower the costs of online services for consumers, it also provides an easy source of funding for app developers from marginalized communities and allows business owners from marginalized communities to connect with new or existing customers.

Similarly, privacy regulation that fails to strike the right balance on privacy and overly restrict the forms of data organizations can collect and the way organizations can use data will negatively impact marginalized communities by exacerbating the existing data divide, the social and economic inequalities that result from a lack of data collection or use about certain individuals or communities.[5]

Much of the discussion around privacy focuses on preventing harm from data collection and use, which is a necessary goal, but a more balanced view would also prioritize maximizing the benefits of data collection and use. Virtually every American industry collects many different forms of data—including data on individuals—to inform decisions and streamline processes in ways that benefit not only those industries, but also the public. For example, the healthcare industry uses data to discover new treatments, cures, and prevention methods. Data collection was crucial in tracking and responding to the COVID-19 pandemic—a notable example being the relatively swift discovery and testing of effective vaccines—while gaps in available data and inconsistent data sharing at times impeded the United States' response.[6]

---

[3] "How Do Online Ads Work?" (ITIF, November 2021), https://www2.itif.org/2021-online-advertising.pdf.

[4] Reginald A. Noël, "Race, Economics, and Social Status" (Bureau of Labor Statistics, May 2018), https://www.bls.gov/spotlight/2018/race-economics-and-social-status/pdf/race-economics-and-social-status.pdf.

[5] Gillian Diebold, "Closing the Data Divide for a More Equitable U.S. Digital Economy" (Center for Data Innovation, August 2022), https://www2.datainnovation.org/2022-closing-data-divide.pdf.

[6] Chuck Curran, "Improving Public Health Data Collection and Sharing After COVID-19," O'Neill Institute, February 17, 2022, https://oneill.law.georgetown.edu/improving-public-health-data-collection-and-sharing-after-covid-19/.

There are many other examples of data collection and use for the public good, from responding to climate change to improving public safety.[7] Inequitable data collection would lead to inequitable outcomes for marginalized communities. Compare a school district that collects relevant data on student outcomes to one that does not. The former school district will be better equipped to make informed decisions when designing curricula and tailoring programs to students' needs. As a result, students in that district are more likely to achieve higher educational outcomes, which will put them on the path to success in their post-secondary education and careers. Similar gaps could form in the financial and healthcare sectors as more public and private services rely on data to make better decisions.

Certain forms of privacy regulation would exacerbate these existing challenges by making it more difficult for organizations to collect and use data. Data minimization, which requires organizations to collect no more data than is necessary to meet specific needs, would negatively impact organizations that do not know which data will be valuable when initially deciding what data to collect, and would also limit organizations' ability to analyze data in the development of new products and services. Similarly, purpose specification, which requires organizations to disclose to users the purposes for which they are collecting data and not use this collected data for any other reasons, would limit innovation, as organizations could not reuse collected data for new purposes or apply data analytics to collected data.

Privacy regulation specifically designed to protect marginalized communities by limiting the amount of data organizations can collect on them or the ways organizations can use that data would directly exacerbate the digital divide. This, in turn, would widen existing gaps in financial, educational, and healthcare outcomes for members of marginalized communities. Policies that give users greater control over their data, including the right to access, port, delete, and rectify their data, would be more beneficial. Then users could see any gaps in the data collected about them and rectify inaccurate data.

RECOMMENDATIONS

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

While overly broad privacy regulation will impose significant costs on American businesses and the economy, ultimately harming consumers, targeted regulation would address actual privacy harms with minimal costs.[8] ITIF research conducted in 2019 estimated that a broad federal privacy law that mirrors key provisions in Europe's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA)

[7] Colin Cunliff, Ashley Johnson, and Hodan Omaar, "How Congress and the Biden Administration Could Jumpstart Smart Cities With AI" (March 2021), https://www2.itif.org/2021-smart-cities-ai.pdf; Ashley Johnson, Eric Egan, and Juan Londoño, "Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms" (January 2023), https://www2.itif.org/2022-police-tech-future.pdf.

[8] Ashley Johnson and Daniel Castro, "Maintaining a Light-Touch Approach to Data Protection in the United States" (ITIF, August 2022), https://www2.itif.org/2022-light-touch-data-protection.pdf.

would cost the U.S. economy approximately $122 billion per year, whereas a more focused, but still effective national data privacy law would cost about $6 billion per year, around 95 percent less.[9]

Effective regulation should take the form of comprehensive federal data privacy legislation that creates a single standard for all Americans and American businesses. Federal privacy legislation that preempts state laws would save American businesses as much as $1 trillion over 10 years in duplicative compliance costs from following 50 different state privacy regimes.[10] It would also ensure that all Americans have the same privacy protections, instead of those protections changing depending on where an individual lives.

A data privacy law would establish greater regulatory certainty than not only the existing patchwork of state privacy laws but also alternative regulatory approaches, such as FTC rulemaking.[11] Congress has been working over the past several years to reach compromises on a number of key privacy issues, resulting in multiple bipartisan bills, most notably the American Data Privacy and Protection Act (ADPPA).[12] Although this process has been slow, if Congress does pass a federal privacy law in the near future, these years of deliberation and compromise will produce a law that stands the test of time.

FTC rulemaking, on the other hand, is more likely to pass along party lines, representing only one side of the privacy debate. When party power inevitably shifts, new rulemaking is likely to change the regulatory landscape. For businesses, the cost of overhauling their privacy practices in order to maintain compliance with changing privacy regulation every few years would add up to much more than a single set of new rules coming from Congress.

Finally, insofar as privacy regulation creates standards for AI and automated decisionmaking, this regulation should take an outcome-based approach, rather than a process-based one. The goal of privacy regulation to advance equity and civil rights should be to prevent discriminatory outcomes, regardless of the process used to obtain those outcomes. Overall, privacy regulation should address concrete consumer harms, rather than hypothetical ones. This means considering specific steps to target the harms consumers are most likely to face, including discrimination. Outside of passing a federal privacy law, Congress should address concerns about unlawful discrimination by conducting a review of civil rights protections and closing any gaps in laws or enforcement capabilities.[13] The solution is not to collect less data, but to ensure more enforcement of existing anti-discrimination laws.

---

[9] Alan McQuinn and Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law" (ITIF, August 2019), https://itif.org/sites/default/files/2019-cost-data-privacy-law.pdf.

[10] Daniel Castro, Luke Dascoli, and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws" (ITIF, January 2022), https://www2.itif.org/2022-state-privacy-laws.pdf.

[11] Ashley Johnson and Aurelien Portuese, "FTC Announcement on 'Commercial Surveillance' Highlights the Need for Federal Data Privacy Legislation," ITIF, August 17, 2022, https://itif.org/publications/2022/08/17/ftc-announcement-highlights-the-need-for-federal-data-privacy-legislation/.

[12] "H.R.8152 - American Data Privacy and Protection Act," Congress.gov, accessed March 2, 2023, https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[13] Alan McQuinn and Daniel Castro, *A Grand Bargain on Data Privacy Legislation for America* (ITIF, January 2019), https://www2.itif.org/2019-grand-bargain-privacy.pdf.

Importantly, an outcome-based approach should acknowledge that different types of data have different levels of privacy and equity concerns. Distinguishing between sensitive and nonsensitive personal data and creating different levels of data protection for these tiers would provide the most stringent protections where they are needed most while reducing costs for organizations that handle nonsensitive personal data and enabling greater innovation using this nonsensitive data.

CONCLUSION

NTIA's request for comment accurately reflects the need to consider the impact of regulation on marginalized communities. Most of the discussion surrounding privacy and civil rights focuses on the impact of a lack of privacy regulation, and there is in fact a pressing need for a federal data privacy standard, but there is also a potential negative impact if such a standard is overly broad or includes certain provisions that would harm consumers or worsen the data divide. The federal government should consider the unintended consequences for those communities it aims to protect via privacy regulation.

Thank you for your consideration.

Ashley Johnson
Senior Policy Analyst