Billing Code 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Privacy, Equity, and Civil Rights Request for Comment

[Docket No. 230103-0001]

RIN 0660-XC052

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice, Request for Comment.

SUMMARY: The National Telecommunications and Information Administration (NTIA) requests comments addressing issues at the intersection of privacy, equity, and civil rights. The comments, along with information gathered through the three listening sessions that NTIA held on this topic, will inform a report on whether and how commercial data practices can lead to disparate impacts and outcomes for marginalized or disadvantaged communities.

DATES: Written comments must be received on or before 11:59 p.m. Eastern Time on [insert date 45 days after date of publication in the *Federal Register*].

ADDRESSES: All electronic public comments on this action, identified by Regulations.gov docket number NTIA-2023-0001, may be submitted through the Federal e-Rulemaking Portal at www.regulations.gov. The docket established for this rulemaking can be found at www.regulations.gov, NTIA-2023-0001. Click the "Comment Now!" icon, complete the required fields, and enter or attach your comments. Responders should include a page number on

each page of their submissions. Please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. All comments received are a part of the public record and will generally be posted to Regulations.gov without change. All personal identifying information (*e.g.*, name, address) voluntarily submitted by the commenter may be publicly accessible. For more detailed instructions about submitting comments, see the ''Instructions for Commenters'' section at the end of this Notice.

FOR FURTHER INFORMATION CONTACT: Please direct questions regarding this Notice to thall@ntia.gov with "Privacy, Equity, and Civil Rights Request for Comment" in the subject line, or if by mail, addressed to Travis Hall, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725, Washington, DC 20230; telephone: (202) 482-3522. Please direct media inquiries to NTIA's Office of Public Affairs, telephone: (202) 482–7002; email: press@ntia.gov.

SUPPLEMENTARY INFORMATION:

Background and Authority: The National Telecommunications and Information Administration (NTIA) is the President's principal advisor on telecommunications and information policy issues. In this role, NTIA studies and develops policy on the impact of technology and the Internet on privacy. This includes examining the extent to which modern data practices and business models are adequately addressed by the current U.S. privacy protection framework. For example, NTIA helped draft the 2012 "Consumer Privacy Bill of Rights" [1] and the 2014 "Big Data: Seizing

[1]White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy,* (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

Opportunities, Preserving Values"[2] report, and led the 2018 Consumer Privacy Request for Comment.[3] Recently, NTIA filed comments in response to the Federal Trade Commission's (FTC) Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security, supporting the rulemaking and recommending that the FTC adopt strong, comprehensive privacy rules, consider heightened privacy protections for marginalized communities, and address discriminatory algorithmic decision-making.[4]

NTIA has long acknowledged that the contexts of information collection, disclosure, and use are key considerations for privacy policy, and that privacy cannot be reduced to a strict divide of exposure contrasted with secrecy. A vital component of contextual analysis, and one that requires greater attention by policy-makers, is the relative social and economic status of the individual or community subject to commercial data flows. Scholarship has shown that marginalized or underserved communities are especially at risk of privacy violations.[5] This work has demonstrated that not only are these communities often materially disadvantaged regarding

---

[2] White House, *Big Data: Seizing Opportunities, Preserving Values,* (May 2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[3] National Telecommunications & Information Administration, *Request for Comments on Developing the Administration's Approach to Consumer Privacy* (Sept. 25, 2018), https://www.ntia.doc.gov/federal-register-notice/2018/request-comments-developing-administration-s-approach-consumer-privacy.

[4] National Telecommunications and Information Administration ANPR Comment (Nov. 21, 2022), https://www.ntia.doc.gov/files/ntia/publications/ftc_commercial_surveillance_anpr_ntia_comment_final.pdf.

The FTC recently solicited comments on the possibility of promulgating rules to govern commercial surveillance and data security, partly in response to President Biden's request that the agency initiate rulemakings in areas such as "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy." Promoting Competition in the American Economy, Exec. Order No. 14036, 86 Fed. Reg. 36987, Section (r) (iii) (July 9, 2021), https://www.govinfo.gov/content/pkg/FR- 2021-07-14/pdf/2021-15069.pdf.

[5] Danielle Keats-Citron, *Cyber Civil Rights,* 89 B.U.L. Rev. 61 (2008); Khiara Bridges, *The Poverty of Privacy Rights,* Stanford University Press (2017); Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix Of Vulnerabilities For Poor Americans,* 95 Wash. U.L. Rev. 53 (2017); Alvaro Bedoya, *Privacy As Civil Right,* 50 N.M.L. Rev. 301 (2020); Scott Skinner-Thompson, *Privacy At The Margins,* Cambridge University Press (2020); Sara Sternberg Greene, *Stealing (Identity) From The Poor,* 106 Minn. L. Rev. 59 (2021); Michele Gilman, *Feminism, Privacy, And Law In Cyberspace,* in Oxford Handbook of Feminism and Law in the United States, (Deborah Brake, Martha Chamallas, & Verna Williams eds., 2021); Anita Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform,* 131 Yale L.J.F. 907, 910 (Feb. 20, 2022) ("In pursuit of equitable data privacy, American lawmakers should focus on the experiences of marginalized populations no less than privileged populations").

to the effort required to adequately manage privacy controls, they are often at increased risk of privacy losses or data misuse.[6] Given the real and promised benefits of the digital economy, it is vital that access to digital services not be predicated on increased risk to marginalized and disadvantaged communities, or practices that may undermine trust and therefore adoption.

The Biden Administration has highlighted a national imperative to promote equity and increase support for communities and individuals who have been "historically underserved, marginalized, and adversely affected by persistent poverty and inequality."[7] As stated in Executive Order 14035 on *Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*: "[e]ntrenched disparities in our laws and public policies, and in our public and private institutions, have often denied … equal opportunity to individuals and communities."[8] These observations and the vital need to address them are deeply relevant to modern data collection and processing. In October 2022, the White House Office of Science and Technology Policy released the Blueprint for an AI Bill of Rights identifying "five principles that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence," including "Algorithmic Discrimination Protections" and "Data Privacy."[9] The Administration's Principles for Enhancing Competition and Tech

[6] *Id. See, e.g.,* Laura Moy, *A Taxonomy of Policing Technology's Racial Inequity Problems*, 2021 U. Ill. L. Rev. 139, 185-191 (illustrating how the use of automated employment recruiting tools and automated personalized learning programs for K-12 students can create, reify, and obscure racial inequity); Greene, *supra* note 5 (citing Department of Justice and other data showing high rates of identity theft among low-income individuals, and discussing the severity of the ensuing harms for low-income people in particular); Danielle Citron & Daniel Solove, *Privacy Harms*, 102 B.U.L. Rev. 793, 856 (2021) ("The misuse of personal data can be particularly costly to women, sexual and gender minorities, and non-White people given the prevalence of destructive stereotypes and the disproportionate surveillance of women and marginalized communities in their intimate lives."); *id*. at 857 ("A key aspect of discrimination harms is the unequal frequency, extensiveness, and impact of privacy violations on marginalized people.").

[7] Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, Exec. Order No. 13985, 86 Fed. Reg. 7009 (Jan. 20, 2021), https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01753.pdf.

[8] *Id.*

[9] White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights* (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

Platform Accountability document highlights the imperative to "stop discriminatory algorithmic decision-making" and "restrict excessive data collection and targeted advertising to young people," priorities President Biden also emphasized in his 2022 State of the Union address.[10] President Biden requested that the Federal Trade Commission consider exploring new avenues of protecting the information of consumers seeking reproductive care, and that the Department of Health and Human Services examine how to better protect sensitive information related to reproductive care.[11] This Request for Comment is intended to examine the persistence of discriminatory disparities in the digital economy, and the extent to which the collection, processing, sharing, and use of data can lead to higher risks for some communities, exacerbate structural inequities, or contribute to their erosion.

On December 14-16, 2021, NTIA hosted three listening sessions on privacy, equity, and civil rights, with each session consisting of keynote speakers, a panel of experts, and an opportunity for the public to present their views. The data gathered through this process, along with responses to this Request for Comment, will be used to inform a report on whether and how commercial data practices can lead to disparate impacts for marginalized or disadvantaged communities.

The proliferation of cheap, efficient, and profitable data collection and processing has transformed how we identify, access, and obtain important life necessities and opportunities. Instead of perusing the local newspaper's classified section, a job seeker may now seek potential

[10] The White House, *Readout of White House Listening Session on Tech Platform Accountability* (Sept. 8, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listeningsession-on-tech-platform-accountability; President Joe Biden, *2022 State of The Union Address* (Mar. 1, 2022), https://www.whitehouse.gov/state-of-the-union-2022.
[11] Protecting Access to Reproductive Healthcare Services, Exec.Order No. 14076, 87 Fed. Reg. 42053 (July 13, 2022), https://www.govinfo.gov/content/pkg/FR-2022-07-13/pdf/2022-15138.pdf.

work opportunities through career-focused social networking sites,[12] or be targeted with digital ads for specific opportunities. Smartphone apps have become vehicles for banking, dating, accessing public benefits, and obtaining medical information, among other key societal functions. But even as these new modes of engaging with the world can reduce barriers, they can also calcify old forms of discrimination and introduce new ones.[13] Digital ads for some employment opportunities may be targeted based on real or perceived demographic characteristics such as age, sex, or race, and reach certain groups while ignoring others.[14] Even when digital advertisers do not intend to use discriminatory targeting criteria, the datasets they use may reflect current or historic inequities and the algorithms they use may unintentionally replicate those biases or others—such as untargeted ads for certain types of jobs being delivered disproportionately to men or women.[15] An app that collects and sells location data could reveal

[12] Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn, at 5 (Dec. 10, 2018), https://www.upturn.org/work/help-wanted/ (describing the development of internet job boards).
[13] This Request for Comment discusses related but distinct terms of art. "Disparate impact" refers to facially neutral practices that produce discriminatory outcomes for certain groups, while "disparate treatment" involves discriminatory intent coupled with a discriminatory outcome. Disparate outcomes may or may not constitute discrimination on the basis of certain attributes. Civil rights laws confer protected class status on certain attributes, such as race, gender, sexual orientation, or national origin.
[14] Jeremy B. Merrill, *Google Has Been Allowing Advertisers to Exclude Nonbinary People from Seeing Job Ads*, The Markup (Feb. 11, 2021), https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads; Moy, *supra* note 6, at 186-88; Julia Angwin & Terry Parris, Jr., *Facebook Lets Advertisers Exclude Users by Race,* ProPublica (Oct. 28, 2016), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race; Julia Angwin et al., *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, ProPublica (Nov. 21, 2017). https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin; Ava Kaufman & Ariana Tobin, *Facebook Ads Can Still Discriminate Against Women and Older Workers, Despite a Civil Rights Settlement*, ProPublica (Dec. 13, 2019), https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement; Jon Keegan*, Facebook Got Rid of Racial Ad Categories. Or Did It?,* The Markup (July 9, 2021), https://themarkup.org/citizen-browser/2021/07/09/facebook-got-rid-of-racial-ad-categories-or-did-it.
[15] Latanya Sweeny, *Discrimination in Online Ad Delivery*, 11 ACM Queue 3, 10-29 (2013),https://queue.acm.org/detail.cfm?id=2460278 (finding skewed ad delivery on racial and gender lines of ads for employment and housing opportunities on Facebook, despite neutral targeting parameters); Basileal Imana et al., *Auditing for Discrimination in Algorithms Delivering Job Ads*, World Wide Web Conference '21 (April 2021), https://dl.acm.org/doi/pdf/10.1145/3442381.3450077 (replicating prior findings that ads for employment opportunities on Facebook can be delivered on a skewed demographic basis despite neutral targeting criteria, and

facts about the app user's movements and life that could make them vulnerable to discrimination, such as an LGBTQ+-specific dating app or a Muslim prayer app.[16] These examples demonstrate how debates about consumer privacy necessarily implicate questions about civil rights as the proliferation of tracking, collection, and evaluation technologies enables new forms of profiling, redlining, and exclusion.[17]

Commenters during NTIA's listening sessions raised concerns that data collection and processing can disproportionately harm marginalized and historically excluded communities, such as disabled people;[18] Native or Indigenous people; people of color, including but not limited to Black people, Asian-Americans and Pacific Islanders, and Hispanic or Latinx people; LGBTQ people; women; victims of domestic violence (including intimate partner violence, abuse by a caretaker, and other forms of domestic abuse); religious minorities; victims of online harassment; formerly incarcerated persons; immigrants and undocumented people; people whose primary language is not among the most commonly spoken languages in the United States; children and adolescents; students; low-income people; people who receive public benefits; unhoused people;

identifying the advertiser's choice of advertising objective and choices made by the ad platform regarding ad delivery optimization as additional factors causing the skew); Jinyan Zhang, *Solving the problem of racially discriminatory advertising on Facebook*, Brookings Institution (Oct. 19, 2021), https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/ (summarizing literature and replicating similar findings).

[16] Jon Keegan & Alfred Ng, *Gay/Bi Dating App, Muslim Prayer Apps Sold Data on People's Location to a Controversial Data Broker*, The Markup (Jan. 27, 2022), https://themarkup.org/privacy/2022/01/27/gay-bi-dating-app-muslim-prayer-apps-sold-data-on-peoples-location-to-a-controversial-data-broker.

[17] *See, e.g.,* Federal Trade Commission, *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers* 47 (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf (describing how six surveyed internet service providers collect and use race and ethnicity data; detailing ensuing concerns about potentially discriminatory practices; and situating those concerns in previous digital redlining tactics).

[18] We refer both to "people with disabilities" and "disabled people" throughout this document to reflect the usage of both person-first and identity-first language. *See generally*, National Center on Disability and Journalism, *Disability Language Style Guide,* "Disabled people/people with disabilities," https://ncdj.org/style-guide/#disabledpeople; Research & Training Center on Independent Living, *Acceptable Language Options: A Partial Glossary of Disability Terms*, https://rtcil.org/guidelines#Acceptable (describing and distinguishing person-first and identity-first language).

sex workers, hourly workers, "gig" or contract workers, and other kinds of workers; and other communities or individuals who are vulnerable to exploitation, or have historically been subjected to discrimination.[19]

The listening sessions examined many different components of how data collection and processing can disproportionately harm marginalized or underserved communities. Certain data practices have the potential to replicate and exacerbate existing forms of discrimination. For example, loose oversight of digital marketing policies allowed payday lenders and associated lead generation companies to target low-income communities of color, replicating discriminatory predation that the payday loan industry has long engaged in offline.[20] Members of specific marginalized groups may also be more likely to be subjected to a privacy harm—for example, women, girls, and members of the LGBTQ community experience invasions of sexual privacy at greater rates than do other communities.[21] Marginalized individuals can also experience privacy invasions more severely. For example, privacy invasions such as data breaches and identity theft can be universally costly and time-consuming to address, guard against, and seek justice for. But pursuing redress is often particularly burdensome for low-income victims, and the lack of a

[19] In discussing the disparate impact of privacy invasions on marginalized communities, we are also conscious of this pertinent reminder from Federal Trade Commissioner Alvaro Bedoya: "When we talk about the disparate impact of surveillance, we have to be careful. We must not reinforce the idea that the targets of surveillance are helpless victims. Often, in fact, the "other" is being watched precisely because they are fighting back. And sometimes, they win—and that watching fails and is utterly useless." Alvaro Bedoya, *Privacy As Civil Right,* 50 N.M.L. Rev. 301, 309 (2020);.

[20] Upturn, *Led Astray: Online Lead Generation and Payday Loans* (Oct. 2015), https://www.upturn.org/static/reports/2015/led-astray/files/Upturn_-_Led_Astray_v.1.01.pdf (describing digital ads placed by payday lenders and lead generation companies for exploitative loans—including in jurisdictions where such ads are illegal—despite policies by online platforms ostensibly prohibiting such ads); David Dayen, *Google Said It Would Ban All Payday Loan Ads. It Didn't*, The Intercept (Oct. 7, 2016), https://theintercept.com/2016/10/07/google-said-it-would-ban-all-payday-loan-ads-it-didnt; Jim Hawkins & Tiffany Penner, *Advertising Injustice: Marketing Race and Credit in America*, 70 Emory L.J. 1619, 1624-5 (2021), https://scholarlycommons.law.emory.edu/elj/vol70/iss7/7/ (finding that in two studies of such lenders in the Houston, Texas area, lenders for generally exploitative loan products such as payday loans and auto title loans marketed predominantly to Black and Latino potential customers, while "mainstream" banks predominantly marketed to white potential customers).

[21] Danielle Citron, *Sexual Privacy*, 128 Yale L.J. 1870, 1908-09 (2019).

financial safety net can make the theft more impactful.[22] Finally, the intersectional nature of marginalized identities—i.e., the fact that many individuals have multiple marginalized identities, such as their race or gender, which concurrently affect how they are perceived and treated—compels careful attention to those complexities.[23]

The implications of modern data practices for privacy and civil rights also compel interrogation of the efficacy of legal privacy and civil rights protections. For example, the Health Insurance Portability and Accountability Act's (HIPAA) privacy protections only extend to personally identifiable health information collected by certain categories of entities,[24] which leaves health information that fails to fit that precise description—such as information collected by certain fitness and health apps—without specific protections, despite its sensitivity and inherent potential for abuse.[25] This can create specific risks for workers vulnerable to discrimination based on conditions such as pregnancy or disability.

---

[22] Greene, *supra* note 5, at 5-7.

[23] Katy Steinmetz, *Kimberlé Crenshaw on What Intersectionality Means Today*, Time (Feb. 20, 2020), https://time.com/5786710/kimberle-crenshaw-intersectionality ("We tend to talk about race inequality as separate from inequality based on gender, class, sexuality or immigrant status. What's often missing is how some people are subject to all of these, and the experience is not just the sum of its parts."); Kimberlé Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. Chi. Legal F. 139, 149 (1989) ("The point is that Black women can experience discrimination in any number of ways and that the contradiction arises from our assumptions that their claims of exclusion must be unidirectional. Consider an analogy to traffic in an intersection, coming and going in all four directions. Discrimination, like traffic through an intersection, may flow in one direction, and it may flow in another. If an accident happens in an intersection, it can be caused by cars traveling from any number of directions and, sometimes, from all of them. Similarly, if a Black woman is harmed because she is in the intersection, her injury could result from sex discrimination or race discrimination."); Michele Gilman, *The Class Differential in Privacy Law*, 77 Brooklyn L. Rev. 1389, 1394 (2012) ("The class differential in privacy law results from complex interactions between class, race, and gender. Because poor Americans are disproportionately minority and female, it is impossible to talk about class without taking into account how subordination is linked to race and gender").

[24] Department of Health and Human Services, *The HIPAA Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[25] *See, e.g.,* Drew Harwell, *Is your pregnancy app sharing your intimate data with your boss?*, The Washington Post (April 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think; Stephanie O'Neill, *As Insurers Offer Discounts for Fitness Trackers, Wearers Should Step With Caution*, NPR (Nov. 19, 2018), https://www.npr.org/sections/health-shots/2018/11/19/668266197/as-insurers-offer-discounts-for-fitness-trackers-wearers-should-step-with-cautio.

Other components of the modern digital economy have discriminatory implications that existing civil rights laws do not appear to prevent or address. For example, public accommodations statutes do not always extend to key online spaces such as social networking or gaming sites, meaning that operators of those spaces are not always legally compelled to make their websites accessible to users with disabilities.[26] Websites that are difficult to use, or simply unusable, for users with disabilities prevent those users from accessing information or opportunities in an Internet-dependent world.[27]

The listening sessions also addressed solutions to these difficult problems. Panelists and attendees suggested a range of strategies, such as firmer restrictions on risky data collection and processing activities; more meaningful penalties for data abuses; more impactful remedies for

---

The privacy implications of non-health data from which sensitive health information can be inferred, such as the location data of an app user who visits an abortion clinic or dialysis center, are also concerning. *See, e.g.*, Stuart A. Thompson & Charlie Warzel, *Twelve Million Smartphones, One Dataset, Zero Privacy*, The New York Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html (review of dataset from a location data aggregator included "hundreds of pings in mosques and churches, abortion clinics, queer spaces and other sensitive areas."); Joseph Cox, *Data Broker is Selling Location Data of People Who Visit Abortion Clinics*, Vice (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood ("It costs just over $160 to get a week's worth of data on where people who visited Planned Parenthood came from, and where they went afterwards."); Joseph Cox, *Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live*, Vice (May 5, 2022), https://www.vice.com/en/article/g5qaq3/location-data-firm-heat-maps-planned-parenthood-abortion-clinics-placer-ai.

[26] David Brody & Sean Bickford, *Discriminatory Denial of Service*, Lawyers' Committee For Civil Rights Under Law (Jan. 2020), https://lawyerscommittee.org/wp-content/uploads/2019/12/Online-Public-Accommodations-Report.pdf (finding a range of approaches to how states consider online spaces, with 28 states where coverage is unclear, coverage is unlikely, online sites are explicitly not covered, or lack a state anti-discrimination law altogether); Amanda Beane et al., *Eleventh Circuit Vacates Ruling That Websites Are Not Public Accommodations Under the ADA*, Consumer Protection Review (Jan. 18, 2022), https://www.consumerprotectionreview.com/2022/01/eleventh-circuit-vacates-ruling-that-websites-are-not-public-accommodations-under-the-ada (describing the ambiguity of whether websites constitute places of public accommodations under the ADA).

[27] *See, e.g.,* Rachel Lerman, *Social media has upped its accessibility game. But deaf creators say it has a long way to go*, The Washington Post (Mar. 15, 2021), https://www.washingtonpost.com/technology/2021/03/15/social-media-accessibility-captions; April Glaser, *Blind people, advocates slam company claiming to make websites ADA compliant,* NBC News (May 9, 2021), https://www.nbcnews.com/tech/innovation/blind-people-advocates-slam-company-claiming-make-websites-ada-compliant-n1266720; Sarah Katz, *Twitter Just Rolled Out a Feature That's Inaccessible to Disabled Users,* Slate, https://slate.com/technology/2020/06/twitter-voice-tweets-accessibility.html; Blake Reid, *Internet Architecture and Disability*, 95 Ind. L.J. 591, 593 (May 2020), ("[S]hortcomings in Internet accessibility threaten to deny millions of Americans access to the economic, educational, cultural, and democratic life of the twenty-first century").

victims; and certain kinds of third-party audits for algorithms that use particular categories of data or algorithms that will be deployed in specific contexts. Participants argued that proposals should also account for how data may also be used to reduce discriminatory harms, such as monitoring for or preventing biased outcomes, and connecting marginalized communities to public services.

INSTRUCTIONS FOR COMMENTERS:

In this Request for Comment, we hope to gather information on the intersection of privacy, equity, and civil rights to supplement the information gathered in the listening sessions. Specifically, we seek to gather feedback on how the processing of personal information by private entities creates, exacerbates, or alleviates disproportionate harms for marginalized and historically excluded communities; to explore possible gaps in applicable privacy and civil rights laws; and to identify ways to prevent and deter harmful behavior, address harmful impacts, and remedy any gaps in existing law. We welcome answers to any of the below questions, in whole or in part, as well as input on related issues not specifically addressed in the questions. We also welcome reactions to information we heard at the three listening sessions held in December. Written comments may include references to personal experiences; white papers and reports; legal, historical, sociological, technical, and interdisciplinary scholarship; empirical or qualitative analysis; and any other form of information that commenters deem pertinent to our review.

When responding to one or more of the questions below, please note in the text of your response the number of the question to which you are responding.

NTIA seeks public comment on the following questions:

QUESTIONS:

Framing

1. **How should regulators, legislators, and other stakeholders approach the civil rights and equity implications of commercial data collection and processing?**
    a. Is "privacy" the right term for discussing these issues? Is it under-inclusive? Are there more comprehensive terms or conceptual frameworks to consider?
    b. To what degree are individuals sufficiently capable of assessing and mitigating the potential harms that can arise from commercial data practices, given current information and privacy tools? What value could additional transparency requirements or additional privacy controls provide; what are examples of such requirements or controls; and what are some examples of their limitations?
    c. How should discussions of privacy and fairness in automated decision-making approach the concepts of "sensitive" information and "non-sensitive" information, and the different kinds of privacy harms made possible by each?
    d. Some privacy experts have argued that the collective implications of privacy protections and invasions are under-appreciated.[28] Strong privacy protections for individuals benefit communities by enabling a creative and innovative democratic society, and privacy invasions can damage communities as well as individuals. What's more, many categories of extractive and profitable processing rely on inferences about populations and demographic groups, making a collective

[28] *See* Citron & Solove, *supra* note 6, at 21-22 (noting that "[p]rivacy harms often involve injury not just to individuals but to society" and citing theorization by Joel Reidenberg, Robert Post, Julie Cohen, and Paul Schwartz concerning the societal implications of privacy protections and invasions).

understanding of privacy highly relevant.[29] How should the individual and collective natures of privacy be understood, both in terms of the value of privacy protections; the harms of privacy invasions; and the implications of those values and harms for underserved or marginalized communities?

e. How should proposals designed to improve privacy protections and mitigate the disproportionate harms of privacy invasions on marginalized communities address the privacy implications of publicly accessible information?

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?

g. Civil rights experts and automated decision-making experts have raised concerns about the incongruity between intent requirements in civil rights laws and how automated systems can produce discriminatory outcomes without the intentional guidance of a programmer.[30] How should regulators, legislators, and other stakeholders think about the differences between intentional discrimination and unintentional discrimination on the basis of protected characteristics, such as race or gender? How do data practices and privacy practices affect each?

[29] Salome Viljoen, *A Relational Theory of Data Governance,* 131 Yale L.J. 573, 578 (2021), https://www.yalelawjournal.org/pdf/131.2_Viljoen_1n12myx5.pdf ("[T]he data-collection practices of the most powerful technology companies are aimed primarily at deriving (and producing) population-level insights regarding how data subjects relate to others, not individual insights specific to the data subject. These insights can then be applied to all individuals (not just the data subject) who share these population features. This population-level economic motivation matters conceptually for the legal regimes that regulate the activity of data collection and use; it requires revisiting long-held notions of why individuals have a legal interest in information about them and where such interests obtain.").

[30] *See, e.g.*, Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671 (2014).

Impact of data collection and processing on marginalized groups

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?**
    a. In particular, what are some examples of how such practices differently impact communities including but not limited to: disabled people; Native or Indigenous people; people of color, including but not limited to Black people, Asian-Americans and Pacific Islanders, and Hispanic or Latinx people; LGBTQ people; women; victims of domestic violence (including intimate partner violence, abuse by a caretaker, and other forms of domestic abuse); religious minorities; victims of online harassment; formerly incarcerated persons; immigrants and undocumented people; people whose primary language is not English; children and adolescents; students; low-income people; people who receive public benefits; unhoused people; sex workers, hourly workers, "gig" or contract workers, and other kinds of workers; or other individuals or communities who are vulnerable to exploitation, or have historically been subjected to discrimination?
    b. In what ways do the specific circumstances of people with disabilities—such as the obligation to supply personal information to obtain public benefits or reasonable accommodations, the use of assistive technologies, or the incompatibility of digital services with a disability—create particular privacy interests or risks?
    c. How do specific data collection and use practices potentially create or reinforce discriminatory obstacles for marginalized groups regarding access to key

opportunities, such as employment, housing, education, healthcare, and access to credit?

3. **Are there any contexts in which commercial data collection and processing occur that warrant particularly rigorous scrutiny for their potential to cause disproportionate harm or enable discrimination?**

    a. In what ways can disproportionate harm occur due to data collected or processed in the context of evaluation for credit; healthcare; employment or evaluation for potential employment (please include consideration of temporary employment contexts such as so-called "gig" or contract workers); education, or in connection with evaluation for educational opportunities; housing, or evaluation for housing; insurance, or evaluation for insurance; or usage of or payment for utilities?

    b. Are there particular technologies or classes of technologies that warrant particularly rigorous scrutiny for their potential to invade privacy and/or enable discrimination?

    c. When should particular types of data be considered proxies for constitutionally-protected traits? For example, location data is frequently collected and used, but where someone lives can also closely align with race and ethnicity. In what circumstances should use of location data be considered intertwined with protected characteristics? Are there other types of data that present similar risks?

    d. Does the Internet offer new economic or social sectors that may raise novel discrimination concerns not directly analogous to brick-and-mortar commerce? For example, how should policymakers, users, companies, and other stakeholders think about civil rights, privacy, and equity in the context of online dating apps, streaming services, and online gaming communities?

e. In what ways can government uses of private data that is collected for commercial purposes—for example, through public-private partnerships—produce unintended or harmful outcomes? Are there ways in which these types of public-private partnerships implicate equity or civil rights concerns? What about the collection and sharing of consumer data by private actors for "public safety purposes"?

f. What is the impact of consolidation in the tech and telecom sectors on consumer privacy as it relates to equity and civil rights concerns?

Existing Privacy and Civil Rights Laws

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?

a. With particular attention paid to equity considerations, what kinds of harms have been excluded from recognition or insufficiently prioritized in privacy law and policy?

b. To what extent do privacy and civil rights laws consider the effects of having multiple marginalized identities on a person's exposure to data abuses? How can privacy and civil rights laws incorporate an intersectional approach to privacy and civil rights protections?

c. Are existing privacy and civil rights laws being effectively enforced? If not, how should these deficiencies be remedied?

d. Are there situations where privacy law conflicts with efforts to ensure equity and protect civil rights for these communities? If so, how should those conflicts be addressed?

e. What resources or legal structures exist to identify and remedy wrongful outcomes produced by digital profiles or risk scores, particularly regarding individual or collective outcomes for underserved or marginalized communities?

f. Legislators around the country and across the globe have enacted or amended a number of laws intended to deter, prevent, and remedy privacy harms. Which, if any, of these laws might serve as useful models, either in whole or in part? Are there approaches to be avoided? How, if at all, do these laws address the privacy needs and vulnerabilities of underserved or marginalized communities?

g. Are there any privacy or civil rights laws, regulations, or guidance documents that demonstrate an exemplary approach to preventing or remedying privacy harms, particularly the harms that disproportionately impact marginalized or underserved communities? What are those laws, regulations, or guidance documents, and how might their approach be emulated more broadly?

h. What is the best way to collect and use information about race, sex, or other protected characteristics to identify and prevent potential bias or discrimination**,** or to specifically benefit marginalized communities? When should this occur, and what safeguards are necessary to prevent misuse?

Solutions

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?**

    a. Are these principles reflected in any legislative proposals? If so, what are those proposals, and how might they be improved?

b. What kinds of protections might be appropriate to protect children and teens from data abuses? How might such protections appropriately address the differing developmental and informational needs of younger and older children? Are there any existing proposals that merit particular attention?

c. What kinds of protections might be appropriate to protect older adults from exploitative uses of their data?

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?

e. Considering resources, strategic prioritization, legal capacities and constraints, and other factors, what can federal agencies currently do to better address harmful data collection and practices, particularly the impact of those practices on underserved or marginalized groups? What other executive actions might be taken, such as issuing executive orders?

6. **What other actions could be taken in response to the problems outlined in this Request for Comment include?**

a. What are the most effective ways for policymakers to solicit input from members of underserved or marginalized groups when crafting responses to these problems? What are the best practices, and what are the missteps to avoid?

b. How should legislators, regulators, and other stakeholders incorporate the multilingual needs of technology users in the United States into policy proposals intended to address privacy harms?

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?

d. What role could design choices concerning the function, accessibility, description, and other components of consumer technologies play in creating or enabling privacy harms, particularly as disproportionately experienced by marginalized communities? What role might design play in alleviating harms caused by discriminatory or privacy-invasive data practices?

e. What role should industry-developed codes of conduct play in public policy responses to harmful data collection and processing and the disproportionate harms experienced by marginalized communities? What are the limitations of such codes?

f. How can Congress and federal agencies that legislate, regulate, adjudicate, advise on, or enforce requirements regarding matters involving privacy, equity, and civil rights better attract, empower, and retain technological experts, particularly experts belonging to marginalized communities? Are there any best practices that should be emulated?

Dated: January 17, 2023

Stephanie Weiner
Acting Chief Counsel, National Telecommunications and Information Administration