CHAMBER OF PROGRESS

February 28, 2023

Alan Davidson
Assistant Secretary for Communications and Information & NTIA Administrator
National Telecommunications and Information Administration
1401 Constitution Avenue NW
Washington, DC 20230

Re: Privacy, Equity, and Civil Rights Request for Comments, Docket No. 230103-0001

Dear Assistant Secretary Davidson:

Chamber of Progress appreciates the opportunity to submit a response to the call by National Telecommunications and Information Administration (NTIA) for public comments to Docket No. 230103-0001.[1] Our comments will focus on a number of questions within the Request for Comment (RFC).

Chamber of Progress is a new progressive tech industry group fighting for public policies that will build a fairer, more inclusive country in which all people benefit from technological leaps. Our partner companies include a diversity of social media, online marketplace, and other consumer-facing platforms, but our partner companies do not have a vote or veto over our positions.

Introduction

Data collection and use makes possible free services that consumers have come to enjoy, such as the ability to chat, connect, and navigate the physical world. One survey of Internet users found that 89% would be willing to pay for WhatsApp ($2.38 per month), 78% would pay for Google Maps ($3.48 per month), and 72% would pay for YouTube ($4.20 per month).[2] A different study found that consumers would have to be paid $17,500 to give up search engines for a year.[3]

[1] Privacy, Equity, and Civil Rights Request for Comment, 88 Fed. Reg. 3714, 3718 (Mar. 6, 2023).
[2] Michael Guta, *Could Businesses Charge for Apps? Maybe, Survey Says*, Small Bus. Trends (Aug. 8, 2019), https://smallbiztrends.com/2019/08/willing-to-pay-for-free-apps.html.
[3] The Data Team, *How much would you pay to keep using Google?,* The Economist (Apr. 25, 2018), https://www.economist.com/graphic-detail/2018/04/25/how-much-would-you-pay-to-keep-using-google.

As these surveys show, although popular sites may be able to charge consumers for such services, removing the option to access them free of charge would disproportionately impact lower-income households who may not have the same resources to pay for services as wealthier households.[4]

In fact, consumers make informed choices to share their data every day, so that they can reap the benefits of an information society. They share their precise location data with ride-sharing apps, their biometric data for authentication and security purposes, and their health, wellness, and fitness data with step-counting, sleep, and heart-rate apps that allow them to lead healthier lives.

We recognize that algorithms are the backbone of innovation. Companies use them to make supply chains more efficient,[5] to make machines safer,[6] and to power modern conveniences.[7]

But despite the importance of algorithms in improving our lives, we have seen instances where data collection and algorithmic processing can exacerbate discrimination against protected classes. These include reports of biased algorithms in the following sectors:

- **Criminal justice:** Academics have found bias in algorithms used to predict recidivism, which judges used to use to determine whether to grant bail.[8] These biases could lead to Black defendants getting bail less often than similarly-situated White defendants.

- **Health care:** One algorithm designed to improve health care access for high-risk patients used health care costs as a proxy for health

---

[4] Ashley Johnson, *Banning Targeted Ads Would Sink the Internet Economy*, Info. Tech. & Innovation Foundation (Jan. 20, 2022), https://itif.org/publications/2022/01/20/banning-targeted-ads-would-sink-internet-economy/.

[5] Kaushik Pal, *How Machine Learning Can Improve Supply Chain Efficiency*, Techopedia (last updated July 27, 2022), https://www.techopedia.com/2/31846/trends/big-data/how-machine-learning-can-improve-supply-chain-efficiency.

[6] Truki Alsuwian, Rana Basharat Saeed & Arslan Ahmed Amin, *Autonomous Vehicle with Emergency Braking Algorithm Based on Multi-Sensor Fusion and Super Twisting Speed Controller*, 12 Applied Sciences 8458 (Aug. 24, 2022), https://doi.org/10.3390/app12178458.

[7] MIT Laboratory for Info. & Decision Sys., *New Smart Thermostat Algorithm Can Learn Optimal Temperature Thresholds Within a Week*, SciTechDaily (Jan. 3, 2021), https://scitechdaily.com/new-smart-thermostat-algorithm-can-learn-optimal-temperature-thresholds-within-a-week/.

[8] *See, e.g.*, Deborah Hellman, *Measuring Algorithmic Fairness*, 106 Va. L. Rev. 811, 815 (2020); Jeff Larson, Survya Mattu, Lauren Kirchner & Julia Angwin, *How We Analyzed the COMPAS Recidivism Algorithm*, Pro Publica (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

needs. This meant that the algorithm disproportionately flagged white patients for additional care because they spent more than their equally sick Black counterparts.[9]

- **Employment:** There have been reports of companies using artificial intelligence to score job candidates in ways that replicate existing biases, for example, by training the algorithms on "good" past employees, who may have excluded employees of certain races or genders on a range from one to five stars. The company scrapped the program once it found out that the system was disparately impacting women. This was because the training data set of past applications included more resumes from men.[10]

These outcomes are clearly harmful to consumers, and no one should fear that their data will be used against them to deny them employment, health care, housing, justice, or opportunity. We commend NTIA for undertaking an inquiry focused on the values of civil rights and equity as it relates to privacy protections.

I. Notice and choice must be part of the solution.

The RFC asks, "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?"[11]

While transparency and choice have their challenges, we reject the argument that consumers are somehow passive victims of technology incapable of making meaningful choices.[12] By necessity, choice has to play a role in the digital environment because consumers have legitimately different views about privacy.

According to one survey, 42% of participants registered for certain "club card benefits," even though they knew that data was likely being shared.[13] The

---

[9] Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 SCIENCE 447, 477 (2019).
[10] F.T.C., Big Data: A Tool for Inclusion or Exclusion? 1, 28 (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.
[11] Privacy, Equity, and Civil Rights Request for Comment, 88 Fed. Reg. 3714, 3718 (Jan. 20, 2023).
[12] See Adam Kovacevich, *Want More Humane Technology? Look to the Supermarket*, American Compass (Jun 10, 2021), https://americancompass.org/the-commons/humane-tech-future/.
[13] Survey Shows Consumers Very Willing to Trade Personal Data for Financial Benefits, PR Newswire (Aug. 5, 2020), https://www.prnewswire.com/news-releases/survey-shows-consumers-very-willing-to-trade-personal-data-for-financial-benefits-301106196.html.

results of another survey showed that 39% of participants liked the idea of compensation for data sharing.[14]

Indeed, consumers are not monolithic, as evidenced by the fact that companies often offer users choices between ad-supported content or a "no ads" plan at a higher cost.[15] For example, in 2019, about 70% of Hulu users were utilizing an ad-supported plan, while about 30% were paying more for an ads-free experience.[16] Consumers have fundamentally different approaches towards digital engagement, therefore, choice has to be part of the solution.

When thinking about how a privacy choice framework should work, we can borrow some concepts from food safety and nutrition. For example, just as we implement baseline protections for food safety, there should be baseline privacy protections that consumers should not have to choose (e.g., security of their data, freedom from use of data for discriminatory purposes).

On top of this baseline level of protections, we allow consumers to make choices. We don't require grocery stores to carry only low-fat or low-sodium goods because we feel consumers can't be trusted, despite the very real risks of heart disease from eating high-fat and high-sodium foods. Just as in this example, we should allow consumers to exercise choices about privacy and should focus regulatory efforts on empowering them to make more informed choices.

However, we acknowledge that any framework must address harmful practices:

- **First, deceptive practices must be prohibite**d, while truthful disclosures must be required.

- **Second, privacy defaults could minimize the number of choices** consumers have to make. For example, consumers should not have to make choices about data security or data minimization. Companies should provide these protections regardless, and do not need to clutter disclosures about

[14] *Survey Shows Consumers Very Willing to Trade Personal Data for Financial Benefits*, PR Newswire (Aug. 5, 2020), https://www.prnewswire.com/news-releases/survey-shows-consumers-very-willing-to-trade-personal-data-for-financial-benefits-301106196.html (noting that 39% of participants liked the idea of compensation for data sharing and 20% said they valued product discounts most).
[15] Plans and Prices, *Hulu Help Center* (Sept. 6, 2022), https://help.hulu.com/s/article/how-much-does-hulu-cost#:~:text=Hulu%3A%20Our%20ad%2Dsupported%20plan,movies%20without%20the%20ad%20breaks.
[16] Ben Munson, *Hulu has 82M viewers, and most of them are seeing ads*, Fierce Video (May 30, 2019), https://www.fiercevideo.com/video/hulu-has-82m-viewers-and-most-them-are-seeing-ads.

choices with this information. Nor should consumer choices be cluttered with non-material information about reasonably-expected uses of personal information, such as product fulfillment, product improvement, security, or sharing with service providers.

- Third, **industry should be able to test disclosure methods with support from the federal government.** In fact, there are examples of industry and the federal government working together to test disclosures to provide guidance to industry about what works and what doesn't. For example, the Federal Trade Commission (FTC) initially studied mortgage disclosures in 2007, revealing that the prototype disclosures developed for the study "significantly improved consumer recognition of mortgage costs."[17] The FTC also led the interagency group that studied privacy disclosures under the Gramm-Leach-Bliley Act.[18] And the Consumer Financial Protection Bureau studied a redesign of mortgage closing documents.[19] Safe harbors for disclosure formats supported by this type of consumer testing should be supported.

II. Sensitive and non-sensitive data must be treated differently.

The RFC asks, "How should discussions of privacy and fairness in automated decision-making approach the concepts of 'sensitive' and 'non-sensitive' information, and the different kinds of privacy harms made possible by each?"[20]

We recognize that not all data is the same and thus, regulators and policymakers should not treat all data the same. We have three suggestions in this regard.

First, we urge regulators and policymakers to allow easy access to deidentified data, the use of which can offer many societal benefits. The clearest

---

[17] F.T.C. Bureau of Economics, Executive Summary of Improving Consumer Mortgage Disclosures: An Empircal Assessment of Current and Prototype Disclosure Forms (Jun. 2007), https://www.ftc.gov/sites/default/files/documents/reports/improving-consumer-mortgage-disclosures-empirical-assessment-current-and-prototype-disclosure-forms/p025505mortgagedisclosureexecutivesummary.pdf.

[18] See U.S. Gov't Accountability Office, Consumer Privacy: Better Disclosures Needed on Information Sharing by Banks and Credit Unions, GAO-21-36 (Oct. 2020), https://www.gao.gov/assets/gao-21-36.pdf.

[19] Consumer Fin. Protection Bureau, Testing "Know Before You Owe" Mortgage Forms (Nov. 20, 2013), https://files.consumerfinance.gov/f/201311_cfpb_factsheet_kbyo_testing.pdf.

[20] Privacy, Equity, and Civil Rights Request for Comment, 88 Fed. Reg. 3714, 3718 (Mar. 6, 2023).

case is research, where data can be used to help change society in fields like medicine and human rights.

Second, regulations should incentivize the collection of less sensitive data, where possible. For example, if regulations were to treat precise geolocation and IP-based location data the same, companies would have little incentive to avoid collecting precise geolocation.

The FTC's case against Flo, a health app that provides menstruation tracking, illustrates the point with respect to sharing of sensitive data. As discussed in the complaint, Flo tracked "Custom App Events," records of user interactions unique to the Flo App, such as user entry of menstruation dates.[21] As the complaint explains, Custom App Events can be used to improve functionality and identify which features are likely to interest new users.[22]

Flo could have accomplished these purposes by associating a Custom App Event with a particular activity internally (i.e., user entry of menstruation dates), but only sharing a generic name with its analytics provider, such as "Custom App Event 1," ensuring that it would not be sharing sensitive health data about the individual.[23] A distinction between sensitive and non-sensitive data could incentivize companies to collect and share less sensitive data, which would help better protect consumer privacy.

Third, although we believe that there should be heightened protections for sensitive data, this alone will not be enough to protect consumers where companies may utilize non-sensitive data categories as a proxy for sensitive data in order to avoid the heightened requirements. This is why regulations should also distinguish between sensitive and non-sensitive *uses* of data.

For example, a prohibition on collection of race information could be both underinclusive and overinclusive in resolving policy concerns. It would be underinclusive in the sense that, while companies may refrain from collecting race information explicitly, they may use proxies to infer race information. It could be overinclusive in that companies may want to collect race information, either explicitly or by proxy, in order to self-test their algorithms to make sure that they don't have a disparate impact on a particular race. An absolute

[21] Complaint at ¶ 18, In the Matter of Flo Health (F.T.C. Jun. 22, 2021) (No. 192 3113).
[22] Complaint at ¶ 18, In the Matter of Flo Health (F.T.C. Jun. 22, 2021) (No. 192 3113).
[23] Complaint at ¶ 20, In the Matter of Flo Health (F.T.C. Jun. 22, 2021) (No. 192 3113).

prohibition on collecting this information would make it much more difficult to discover discrimination and remedy it.[24]

In short, equally important to categorizing data into sensitive and non-sensitive buckets is limiting sensitive uses of data without consumer consent. Rather than relying solely on distinctions between sensitive and non-sensitive data, regulations could encourage risk assessments that focus on use cases. One could look to the model of Data Protection Impact Assessments (DPIAs) under the GDPR as inspiration.

Under the GDPR, companies need to assess the impact of data processing when such use is "likely to result in a high risk to the rights and freedoms of natural persons."[25] These types of assessments may ensure that more sensitive data types receive heightened protection while also discouraging companies from using labels to hide from regulation. And of course, to the extent that assessments are required, they should be proportional to the size of a business and amount and sensitivity of data it collects, consistent with the principles outlined at the outset of this comment.

III. Mitigating certain categories of harm must be a priority for regulators.

The RFC asks, "What is the interplay between privacy harms and other harms that can result from automated decisionmaking, such as discriminatory and arbitrary outcomes?" [26] We believe that harms in this context may fall into several categories.

First, there is no question that lax privacy practices, particularly with respect to security, can cause injury to consumers in the form of fraudulent charges and identity theft, as described in greater detail below.

Second, lax privacy practices can lead to physical injuries, including risks associated with harassment and stalking. For example, in its most recent case against a stalkerware app, the FTC noted that "stalkers and abusers [] use the

[24] *See* Stephanie S. Gervasi et al., *The Potential For Bias In Machine Learning And Opportunities For Health Insurers To Address It*, 41 Health Info. Tech. (Feb. 2022), https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2021.01287 (stating that "[d]ata on members' race and ethnicity could enhance medical management programs and facilitate audits for possible racial bias in both algorithmic output and care management outreach.).
[25] GDPR Art. 35, ¶ 1.
[26] Privacy, Equity, and Civil Rights Request for Comment, 88 Fed. Reg. 3714, 3718 (Mar. 6, 2023).

information obtained via monitoring to perpetuate stalking and abusive behaviors, which cause…physical harm, including death."[27]

Third, use of data to discriminate against protected classes or deny people opportunities is harmful. Many have made the link between privacy and civil rights,[28] in part due to the potential for discrimination based on data. For example, "digital redlining," where ads for housing or certain financial products are shown only to consumers of particular races or genders, can perpetuate economic and racial disparities.[29]

Finally, although we would have concerns about regulations or legislation creating restrictions based on speculative emotional harms, we do believe in protections against very tangible harms that are created when matters concerning someone's private life are disclosed in a way that would be "highly offensive to a reasonable person"[30] By focusing on this type of conduct, subjective harms are excluded. In fact, by focusing on public disclosure of "private" facts, it excludes disclosure of information that is in the public interest, such as online reviews of business establishments.

This framework may be helpful for the regulators in considering the types of non-traditional harms it should focus on. This type of harm already has a history of being the subject of FTC enforcement, such as the following:

1. Cases involving collection, use, and disclosure of sensitive health information without adequate notice and consent[31]
2. Non-consensual sexual adult imagery and stalkerware cases[32]

---

[27] *See, e.g.*,Complaint at ¶ 22, *In the Matter of Support King, LLC* (F.T.C., Aug. 26, 2021) (No. 192 3003) ("Stalkers and abusers then use the information obtained via monitoring to perpetuate stalking and abusive behaviors, which cause . . . physical harm, including death."); Complaint at ¶ 23, *In the Matter of Support King, LLC* (F.T.C., Aug. 26, 2021) (No. 192 3003) ("Stalking victims experience financial loss both directly and indirectly.").

[28] *See, generally,* Alvaro Bedoya, *Privacy as Civil Right*, 50 N. Mex. L. Rev 301 (2020); Danielle Citron, The Fight for Privacy (2022); Scott Skinner-Thompson, Privacy at the Margins (2020).

[29] *Cf., Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising*, Dept. of Justice (Jun. 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known; Lauren Feiner, *DOJ settles lawsuit with Facebook over allegedly discriminatory housing advertising*, CNBC (Jun. 21, 2022), https://www.cnbc.com/2022/06/21/doj-settles-with-facebook-over-allegedly-discriminatory-housing-ads.html.

[30] *See* Restatement (Second) of Torts § 652D.

[31] *See, e.g.,* Complaint, In the Matter of Flo Health, Inc. (F.T.C. Jun. 22, 2021) (No. 192 3113).

[32] See, *e.g.*, Complaint, In the Matter of Support King, LLC (F.T.C. Dec. 21, 2021) (No. 192 3003); Complaint, In the Matter of Retina-X Studios, LLC (F.T.C. Mar. 27, 2020) (No. 172 3118); F.T.C. v. EMP Media, Inc. (D. Nev., Jun. 15, 2018) (No. 2:18-cv-00035-APG-NJK).

3. Cases involving unauthorized video surveillance of individuals[33]

We believe that a "public disclosure of private facts" standard to be more impactful rather than the more nebulous "reputational injury," "emotional distress," or "dignity interests of the individual." It is well grounded in an existing body of the law and can be a helpful reference, as regulators and lawmakers consider the scope of non-tangible harms they seek to address.

IV. A right to cure provides one pathway to mitigate unintentional discrimination.

The RFC asks, "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?"[34]

One policy pathway to address the legitimate concern around automated systems that produce discriminatory outcomes without the intentional guidance of a programmer is to incentivize rigorous processes and iteration to eliminate biases and not focus solely on outcomes.

Consider the example of social entrepreneurs that want to develop an algorithm to reduce racial bias in higher education. The goal of eliminating bias drives their mission, they hire diverse experts to test the algorithm across different vectors (e.g., age, gender, disability, etc.), and their testing does not unearth bias. Assume further that, after release of the algorithm, it gets used in ways that could not have been reasonably foreseen at the time of testing, and it is discovered that certain uses may create bias against older students. Imposing immediate liability on the company would chill social entrepreneurs from trying to build more bias-free systems.

Indeed, this is not a hypothetical scenario: Companies like Zillow are developing remote home appraisal tools that have the potential to reduce racial bias against Black and Latino homeowners.[35] Rules that demand perfect outcomes are likely to stifle interest in developing socially-beneficial algorithms. Instead, we suggest incentivizing innovation in this area by exploring the possibility of a right to cure, where a company has implemented strong processes to detect and mitigate bias.

---

[33] *See, e.g.,* Complaint, In the Matter of TRENDnet, Inc. (F.T.C. Feb. 7, 2014) (No. 122 3090).
[34] Privacy, Equity, and Civil Rights Request for Comment, 88 Fed. Reg. 3714, 3718 (Mar. 6, 2023).
[35] Debra Kamin, *Remote Appraisals of Homes Could Reduce Racial Bias*, N.Y. Times (Mar. 21, 2022), https://www.nytimes.com/2022/03/21/realestate/remote-home-appraisals-racial-bias.html.

Similarly, privacy-protective policies should make sure companies are not penalized for iterating on their algorithms. Most companies don't want their algorithms to yield discriminatory outcomes, period. But they may fear that testing for those outcomes and iterating on them could open them up to liability. To encourage this kind of testing, companies should have the opportunity to cure and remediate any discoveries of discriminatory outcomes. Further policies could encourage safe harbors for companies that publicly publish their initial findings for vetting by public organizations.

Indeed, in the health care example discussed above, the bias was discovered after a public paper about the algorithm was released, and the creators implemented changes to correctly target health care resources toward sicker populations, while reducing bias by 84 percent.[36] Any Rule should make sure that companies are not incentivized to bury their heads in the sand and ignore reports of bias for fear of liability if bias comes to light.

In sum, virtually every privacy regulation in the US and abroad includes some form of consumer choice. We can't see a world where there could be effective privacy regulation without allowing for some differences among consumer preferences.

Thank you for your leadership on this important issue. We are available for any further questions.

Sincerely,

Koustubh "K.J." Bagchi
Senior Director, Technology Policy

[36] Rebecca Kelly Slaughter, *Algorithms and Economic Justice*, 23 Y. J. L. & Tech. 1, 17 (2021) ("Notably, when the researchers identified the flaw, the algorithm's manufacturer worked with them to mitigate its impact, ultimately reducing bias by 84 percent–exactly the type of bias reduction and harm mitigation that testing and modification seeks to achieve."), available at https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf.