March 6, 2023

Alan Davidson
Assistant Secretary for Communications and Information and
NTIA Administrator
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Submitted via www.regulations.gov

Subject: NTIA Privacy, Equity, and Civil Rights Request for Comment, Docket Number NTIA-2023-0001

Dear Assistant Secretary Davidson:

On behalf of The Leadership Conference on Civil and Human Rights and its Media and Telecommunications Task Force, we write in response to the National Telecommunications and Information Administration's (NTIA) request for comments (RFC) on Privacy, Equity, and Civil Rights.[1] The Leadership Conference, a coalition charged by its diverse membership of more than 230 national organizations to promote and protect the rights of all persons in the United States, and its Media/Telecommunications Task Force, work to ensure that civil and human rights, equal opportunity, and democratic participation are front and center in communications and technology policy debates.

We appreciate NTIA's commitment to protecting the American public in the age of artificial intelligence (AI) and its recognition that there are entrenched disparities in our laws, infrastructure, systems, and public polices that have denied equal opportunity to individuals and communities. We are particularly encouraged by NTIA's leadership in advancing the administration's AI Bill of Rights.[2] In these comments, we discuss how privacy, equity, and civil rights are connected; describe the harms to underserved and marginalized communities caused by commercial data collection practices and use of that data in AI systems; offer solutions based on already existing principles on the use of data and emerging technologies that can be used as guides in addressing the harms experienced by underserved and marginalized communities; and discuss the need to implement those principles in concrete

---

[1] National Telecommunications and Information Administration, Department of Commerce, 88 FR 3714, January 20, 2023.
[2] https://www.whitehouse.gov/ostp/ai-bill-of-rights/; Oct. 4, 2022.

ways and why legislators and regulators must create enforceable rules to hold companies that develop or deploy AI accountable.

Introduction

Technological progress must promote equity and justice as it enhances safety, economic opportunity, and convenience for everyone. Technology, if designed and managed appropriately, has the potential to expand economic equality and to identify and mitigate instances of bias and discrimination, but far too often, people who are subject to historical and ongoing discrimination face disproportionate surveillance and bear the brunt of harms created or amplified by new technologies, including in decision-making that relies on technology that creates new, or exacerbates existing, harms.

We appreciate NTIA's recognition that data may be used to make decisions about individuals based on "real or perceived demographic characteristics such as age, sex, or race." In the advertising context, like the example cited in the RFC, use of AI to deliver digital ads means that some ads may reach certain groups while ignoring others. The RFC further recognizes that "the datasets they use may reflect current or historic inequities and the algorithms [can] unintentionally replicate those biases or others" and make individuals "vulnerable to discrimination."[3] The advertising context is but one real-life scenario. The same potential for bias and discrimination exists across uses of technology in other areas, including housing, health care, education, employment, the criminal-legal system, and credit and lending. In general, some personalization AI algorithms being used for marketing can be intrusive to personal privacy, can serve as proxies that discminate against consumers on the basis of characteristics protected under civil rights statutes like the Fair Housing Act, and can limit upward economic mobility.

In a welcome development, NTIA — along with other agencies, state governments, and Congress — is now addressing the issues of privacy, equity, and civil rights. The proliferation of emerging AI technologies, and the potential for adverse impact on individuals, particularly in underserved or marginalized communities, is real. The multitude of "AI Principles" adopted by advocacy groups, industry associations, individual companies, the administration, and other governments is evidence of a consensus not only that there are potential harms, but that measures must be taken to address and prevent those harms.

The questions posed in the RFC lead to the following conclusions:

1. Privacy rights are civil rights.
2. The harms of bias and discrimination caused using AI driven by personal data are well-documented across industry sectors.
3. The persistence of AI bias and the harmful impact of AI-based decision-making, especially on underserved and marginalized communities, merits action to mitigate these serious risks. Risk mitigations should come through the implementation of the AI Bill of Rights[4] and subsequent Executive Order on *Advancing Racial Equity and Support for Underserved Communities*

---

[3] Id. at 3716.
[4] Blueprint for an AI Bill of Rights - OSTP - The White House; Oct. 4, 2022.

Through the Federal Government (Equity EO)[5] and regulatory and legal frameworks to manage those risks.

4. Any privacy framework must also reduce harms. Needed protections include data minimization, assessing AI for risks, like bias, preventing or mitigating any bias found, identifying use cases where use of AI should be prohibited, transparency and explainability, community engagement, providing for data security, closing any gaps with existing civil rights laws, and strong enforcement.

5. It is critical to take a holistic approach in addressing privacy, equity, and civil rights. From its concept and design to deployment, use, and monitoring, AI systems require thoughtful and collaborative approach. At each point in the AI development process, there is a potential for bias to be inserted or thwarted. For example, we must ensure that entities developing or deploying AI provide notices and disclosures in the language of users. They also need to consider the potential impact of the technologies they create or use on all communities that may be subject to an AI system, including communities of color and LGBTQ+, Muslim, Native American, and disability communities.

6. While new protections are needed in many cases, regulators should use their existing authorities under current statutes — like the Fair Credit Reporting Act, the Equal Credit Opportunity Act, and the Fair Housing Act — to protect the rights of individuals generally to advance equity.

SPECIFIC QUESTIONS

Framing: Privacy, equity, and civil rights are connected.

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

We urge regulators and legislators to create enforceable rules of the road to hold companies accountable for their collection and use of data and development and deployment of AI. The civil rights and equity implications of AI systems are now well-documented. When AI, driven by data, is biased, using those systems can exacerbate existing harms, often disportionately impacting communities of color and other marginalized groups. This is why privacy rights are civil rights.

Currently, there is a lack of transparency and explanation of how decisions involving AI are made, including what data are being used in that decision-making. Sometimes the people using AI to make decisions have little understanding of how the technology works. As AI is used across various sectors, those designing, deploying, and using technology fueled by personal data should be responsible for doing so in ways that are not biased and discriminatory. The only way to assess the impact of technology is to look at the system and understand the contexts in which it could be used. From there, a diverse team of AI

---

[5] [Executive Order on Further Advancing Racial Equity and Support for Underserved Communities Through The Federal Government - The White House](#); Feb. 16, 2023.

solution developers and deployers[6] can determine where the system should not be used, whether it is fit for specific purposes it is developed for, and evaluate the potential impact of the solution on underserved and marginalized communities.

We need both new protections and existing protections to mitigate AI risks. New protections should be codified in laws and regulations; where necessary, gaps in existing laws should be closed. It should be made clear with guidance that existing civil rights laws, including antidiscrimination laws, apply in the digital world regardless of whether AI is being used.

This protection framework should include:

- **Civil rights protections:** With data-driven AI systems becoming more ubiquitous, those systems should not result in discriminatory outcomes or exacerbate existing biases related to protected characteristics.
- **Privacy protections:** Companies should minimize the data they collect; there should be clear permissible and impermissible purposes for collecting, sharing, and using personal data; discriminatory collection and use of personal data should be prevented; and rules should provide for transparency and explainability.
- **Impact assessments:** Impact assessments enable companies to identify biases and mitigate harm on communities and individuals, including marginalized communities and communities of color. Companies should be required to assess their algorithms on a cadence consistentith the rate at which they develop and deploy new solutions.
- **Audits:** Companies should evaluate the algorithms to identify potential discriminatory impacts and biases before those algorithms are deployed, during field testing, and after they are put into use.

Impact of Data Collection and Processing on Marginalized Groups

Question 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?

There is a growing record of patterns and practices of data collection and use across sectors that harm individuals, particularly the most marginalized communities. The use of algorithms, fueled by an individual's personal information both from data collected and inferred, has led to reproducing patterns of

---

[6] Michael Akinwumi, Lisa Rice and Snigdha Sharma, "Purpose, Process and Monitoring: A new framework for auditing algorithmic bias in housing and lending", National Fair Housing Alliance, February 7, 2022. https://nationalfairhousing.org/wp-content/uploads/2022/02/PPM_Framework_02_17_2022.pdf.

discrimination[7] in recruiting,[8] housing,[9] education,[10] finance,[11] mortgage lending,[12] credit scoring,[13] health care,[14] vacation rentals,[15] ridesharing,[16] and other services. Private companies are developing and offering technologies that use data in ways that can discriminate, or disproportionately harm communities of color, when they are inaccurate. Products and services such as facial recognition,[17] including in-store facial recognition,[18] cell phone location data tracking,[19] background checks for employment,[20] and credit

---

[7] Milner, Yeshimabeit. & Traub, Amy. "Data Capitalism and Algorithmic Racism." *Data for Black Lives. Demos.* May 17, 2021.
https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf

[8] Bogen, Miranda. & Rieke, Aaron. "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias." *Upturn.* December 10, 2018
https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf

[9] Schneider, Valerie. "Locked Out By Big Data: How Big Data, Algorithms and Machine Learning may Undermine Housing Justice." *Columbia Human Rights Law Review.* Fall, 2020.
https://blogs.law.columbia.edu/hrlr/files/2020/11/251_Schneider.pdf

[10] Quay-de la Vallee, Hannah. & Duarte, Natasha. "Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data." *Center for Democracy & Technology.* August 12, 2019.
https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/

[11] Bartlett, Robert et al. "Consumer-Lending Discrimination in the FinTech Era." *UC Berkeley.* November, 2019.
https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf

[12] Olick, Diana. "A troubling tale of a Black man trying to refinance his mortgage." *CNBC.* Aug 19, 2020.
https://www.cnbc.com/2020/08/19/lenders-deny-mortgages-for-blacks-at-a-rate-80percent-higher-than-whites.html

[13] Rice, Lisa. & Swesnik, Deidre. "Discriminatory Effects of Credit Scoring on Communities of Color." *Suffolk University Law Review.* January 17, 2014.
https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/3/1172/files/2014/01/Rice-Swesnik_Lead.pdf

[14] Obermeyer, Ziad et al. "Dissecting racial bias in an algorithm used to manage the health of populations." *Science.org.* Oct 25, 2019.
https://www.science.org/doi/10.1126/science.aax2342

[15] Edelman, Benjamin et al. "Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment." *American Economic Association.* April, 2017.
https://www.aeaweb.org/articles?id=10.1257/app.20160213

[16] Ge, Yanbo et al. "Racial and Gender Discrimination in Transportation Network Companies." *NATIONAL BUREAU OF ECONOMIC RESEARCH.* October, 2016.
https://www.nber.org/system/files/working_papers/w22776/w22776.pdf

[17] Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It," *The New York Times.* Jan 18, 2020.
https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[18] Wimbley, Randy. and Komer, David. " Black teen kicked out of skating rink after facial recognition camera misidentified her." *FOX 2 Detroit.* July 16, 2021.
https://www.fox2detroit.com/news/teen-kicked-out-of-skating-rink-after-facial-recognition-camera-misidentified-her

[19] Valentino-DeVries, Jennifer et al. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." *The New York Times.* Dec 10, 2018.
https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[20] *Henderson v. Source for Public Data, 540 F. Supp. 3d 539 (E.D. Va. 2021).* May 19, 2021
https://casetext.com/case/henderson-v-source-for-public-data

The Leadership
Conference

scoring[21] have had harmful impacts on communities of color. Commercial data practices can facilitate the surveillance of and discrimination against communities of color, both by packaging and selling data to law enforcement in ways that allow them to circumvent warrant requirements and by selling biased technologies for law enforcement use.[22] One example is cell phone location data tracking. It has become common for law enforcement to rely on cell tower data in criminal prosecutions. Although a warrant is usually obtained, the data can be inaccurate, and the use of unreliable information from private companies in prosecutions can have grave consequences.[23] With no legal requirements in place to assess how data is used, evaluate the potential impact of the AI system, test or audit it, there is nothing to prevent or stop adverse consequences until after harm has occured.

Other examples of how commercial data affected underserved and marginalized groups includes the NFHA Facebook settlement case and NFHA Redfin Case. In the Facebook case, NFHA and other plaintiffs asserted that Facebook's advertising platform contained pre-populated lists that allowed advertisers to place housing, employment, and credit ads that could "exclude" certain protected groups, such as African Americans, Hispanics, and Asian Americans.[24] This historic settlement involved sweeping changes to Facebook's paid advertising platform and resolves five separate legal claims that alleged Facebook's platform unlawfully enabled advertisers to target housing, employment, and credit ads to Facebook users based on race, color, gender, age, national origin, family status, and disability.[25]

The NFHA Redfin settlement was a result of a complaint filed by NFHA and another fair housing organization that alleged Redfin's minimum home price policy had a substantial adverse impact on buyers and sellers of homes in predominantly non-White communities based on race and national origin.[26] The complaint alleged that Redfin offered no services in non-White zip codes at a disproportionately higher rate than in White zip codes in Baltimore, MD; Chicago, IL; Detroit, MI; Kansas City, MO/KS; Long Island, NY; Louisville, KY; Memphis, TN; Milwaukee, WI; Newark, NJ; and Philadelphia, PA. The lawsuit was brought after NFHA and nine other fair housing organizations conducted a lengthy investigation. The fair housing organizations alleged that Redfin's minimum home price policy violated the Fair Housing Act by discriminating against sellers and buyers of homes in communities of color. NFHA and the other plaintiffs alleged that policies that limit or deny services for homes priced under certain values can perpetuate racial segregation and contribute to the racial wealth gap. These settlements are expected to serve as cautionary tales to entities practicing commercial data collection and processing

---

[21] Rice, Lisa. & Swesnik, Deidre. "Discriminatory Effects of Credit Scoring on Communities of Color." *Suffolk University Law Review.* January 17, 2014.
https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/3/1172/files/2014/01/Rice-Swesnik_Lead.pdf
[22] https://www.naacpldf.org/wp-content/uploads/LDF-Comment-on-FTC-Rulemaking-on-Commercial-Surveillance-Data-Security27.pdf.
[23] https://washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html.
[24] https://nationalfairhousing.org/wp-content/uploads/2022/01/2018-06-25-NFHA-v.-Facebook.-First-Amended-Complaint.pdf
[25] https://nationalfairhousing.org/wp-content/uploads/2022/01/FINAL-SIGNED-NFHA-FB-Settlement-Agreement-00368652x9CCC2.pdf
[26] https://nationalfairhousing.org/wp-content/uploads/2022/04/FINAL-Joint-Statement-NFHA-v.-Redfin-00492531x9CCC2.pdf?eType=EmailBlastContent&eId=465cbcfb-2c3b-4a11-aed7-99f358d743e4

practices without thought of how it may affect underserved or marginalized communities more frequently or severely than other populations.

In some cases, the potential uses of a new technology might not be fully known or its potential harms not identified. It is vital to ensure that the technology is not harmful prior to putting it into uses where it could have a harmful impact. A recent example is ChatGPT, a generative AI system that is based on large language models that are known to be biased and discriminatory toward underserved and marginalized communities.[27] While in its early stages, ChatGPT has been found to provide inaccurate results,[28] sexist responses, and biased responses.[29] The technology merits further assessment and testing. Potentially impacted communities should be consulted. In some use cases, the technology may be inappropriate, and its use should be prohibited like what is being proposed by the European Union.[30]

Question 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?

Without safeguards to ensure AI technology does not cause new or aggravate existing inequalities, data may be used in ways that discriminate. Some contexts warrant rigorous scrutiny because of their potential to cause disproportionate harm or enable discrimination, including:

- **Use that can limit economic opportunity**. AI-based decisions have led to jobseekers steered towards lower paying jobs, jobseekers losing access to available jobs, which employees are chosen for layoffs,[31] whether a potential homebuyer receives a mortgage, or whether a borrower is given a loan or credit.
- **Advertising**. Researchers examined Facebook's algorithms to find new audiences for advertisers, which permitted racial and ethnic bias.[32]
- **Policing and public safety**. "Flock" cameras, which give individuals the power to surveil license places, can be a tool of mass surveillance.[33]

---

[27] Okerlund, Johanna, et al. *What's in the Chatterbox? Large Language Models, Why They Matter, and What We Should Do About Them*. Apr. 2022, https://stpp.fordschool.umich.edu/sites/stpp/files/2022-05/large-language-models-TAP-2022-final-051622.pdf.

[28] Ian Bogost, "ChatGPT is Dumber than You Think," The Atlantic (Dec. 7, 2022), https://www.theatlantic.com/technology/archive/2022/12/chatgpt-openai-artificial-intelligence-writing-ethics/672386/.

[29] A tweet thread on the social ills of language models or generative AI including ChatGPT may be found here, https://twitter.com/datawumi/status/1625816934918029313?s=20

[30] Luca Bertuzzi, "AI Act: EU Parliament's crunch time on high-risk categorisation, prohibited practices", EURACTIV, Feb 7, 2023. https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-parliaments-crunch-time-on-high-risk-categorisation-prohibited-practices/

[31] *AI is starting to pick who gets laid off*, Pranshu Verma, The Washington Post (February 20, 2023 at 7:00 am). https://www.washingtonpost.com/technology/2023/02/20/layoff-algorithms/.

[32] Zang, Jinyan. "Solving the problem of racially discriminatory advertising on Facebook." Brookings.ed. October 19, 2021. https://brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/

[33] https://www.aclu.org/news/privacy-technology/how-to-pump-the-brakes-on-your-police-departments-use-of-flock-mass-surveillance-license-plate-readers.

- **Health care**. For example, access to reproductive health care and the general type or level of health care someone receives have been decided by AI.
- **Use of proxies**. Any industry where data is used as a proxy for protected characteristics is risking discrimination. Additional scrutiny is required whenever AI is used to make a decision about someone's life. Given the well-documented harms, AI should not be the deciding factor in these situations. A data-minimization framework will help to support harm-reduction.
- **Housing advertisement**. For example, where Facebook's advertising platform contained prepopulated lists that allowed advertisers to place housing and credit ads in a way that could include certain protected groups such as African Americans or Hispanics despite the Fair Housing Act, which requires fairness in how certain ads are made available to people.
- **Disability discrimination**. Both the Department of Justice and the Equal Employment Opportunity Commission have issued guidance putting employers on notice that using automated hiring tools driven by AI can put them at risk of engaging in disability discrimination. This is just one example of AI having difficulty capturing the disability experience.

Specific communities may also face harm from the use of their data. These harms were most recently highlighted in comments filed in 2022 for the Federal Trade Commission's (FTC) *Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security*[34]:

- For Asian Americans and other communities of color, the harms of automated decision-making practices are especially magnified for those who have Limited English Proficiency (LEP) or have been historically monitored and surveilled.[35]
- Latino and other marginalized communities face potential harms from commercial data surveillance, as well as dangers posed by unregulated or inadequately enforced laws related to commercial data practices to civil rights and individual privacy.[36]
- The commercial collection and personal use of data exacerbate economic racial discrimination and bias. Other examples include the collection and use of personal health data in ways that systematically discriminate against Black patients. Law enforcement use of commercial data disproportionately targets the Black community with over-policing.[37]
- Commercial surveillance and weak data security harm Muslims and all individuals. Muslims and other minority groups need protections from surveillance based on faith, religiosity, or other community-specific characteristics.[38]

---

[34] Federal Trade Commission *Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security*, 87 FR 51273, August 22, 2022.

[35] Comments of the Asian Americans Advancing Justice (AAJC), https://www.regulations.gov.comment/FTC-2022-0053-1068, FTC Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security.

[36] Comments of UnidosUSA, https://www.regulations.gov/comment/FTC-2022-0053-1146, FTC Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security.

[37] Comments of the Black Women's Roundtable, https://www.regulations.gov/comment/FTC-2022-0053-1203, FTC Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security.

[38] Comments of Muslim Advocates, htts://www.regulations.gov/FTC-2022-0053-1168, FTC Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security.

- Data can fuel algorithmic processing, which is harmful to communities of color, women, low-income communities, and communities with disabilities. Rules are needed to minimize the amount of information collected that could eliminate some of the biases and unfair practices that are derived from the use of predictive algorithms.[39]
- Automated decision-making systems can exacerbate inequities, bias, and discrimination. Policymakers must prevent the harms caused by commercially developed technologies, particularly those that leverage large amounts of sensitive data, which are used by law enforcement in ways that discriminate against communities of color.[40]

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?

The current regulatory and legal landscape is inadequate. There is a need for a new framework and multi-pronged approach to protect privacy and civil rights and prevent potential harms from the use of AI and other emerging technologies:

- **Federal:** There is currently no comprehensive federal law that directly addresses current data practices or contemplates future commercial surveillance and the harm those uses of data can have on privacy and civil rights.
- **State:** While several states, like California, have passed privacy legislation, those laws lack necessary civil rights protections. In addition, the laws only apply to citizens of the state of entities doing business in the state.
- **Regulatory:** There are scant regulatory frameworks that address the use of AI. While some agencies, like the Consumer Financial Protection Bureau (CFPB), are exploring various industry sectors, how technology and data are being used, and considering which protections are needed, more work needs to be done. All agencies need to undertake efforts to assess the landscape and propose a framework for addressing potential harms. The Federal Trade Commission (FTC) should also proceed with its rulemaking on privacy and civil rights.[41]

We need a comprehensive federal privacy law that includes strong civil rights protections. In addition to broadly protecting data privacy, the law should advance civil rights by prohibiting discriminatory uses of personal data and mandate measures to prevent biased outcomes. There should be strict limits on how one company can share an individual's data, like biometric data, with others[42] or retain such data for future use. The law should also include a requirement for solution providers and users to test algorithms for bias, allow companies to only collect, use, or share as much data as is necessary to provide services consumers

---

[39] Comments of the National Urban League, https://www.regulations.gov/FTC-2022-0053-0916, Federal Trade Commission Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security.

[40] Comments of the NAACP Legal Defense and Educational Fund, Inc. (LDF), https://www.regulation.gov/FTC-2022-00531135, Federal Trade Commission Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security.

[41] Federal Trade Commission *Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security*, 87 FR 51273, August 22, 2022.

[42] One example is Clearview AI. Clearview AI relied on data from third-party social media platforms to fill its image databases without the consent of the platforms' users.

The Leadership
Conference

expect, and mandate companies to be transparent about the use of AI and explain how algorithmic decisions are made.

We also need to close gaps in existing civil rights laws to contemplate the use of emerging technologies like AI and machine learning, especially in areas that have direct impact on individuals, like credit and lending, housing, employment, education, health care, public benefits, and justice.

The Lawyers' Committee for Civil Rights Under Law (LCCRUL) comments filed in the FTC's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security captured the gaps and shortcomings of existing civil rights laws, which did not contemplate the digital era and ubiquitous use of technologies like AI[43]:

- Existing anti-discrimination laws have many gaps and limitations, such as Title II of the Civil Rights Act of 1964, exclude retail stores or have unresolved questions about how they apply to online businesses.[44]
- The Fair Housing Act and Title VII apply to specific sectors like housing and employment, respectively, but may not cover new types of online services used to match individuals to these opportunities. To give a few examples, under current federal civil rights statutes it would be legal for an online business to charge higher prices to women or to refuse to sell products to Christians.[45]
- A service provider could use discriminatory algorithms to look for workers to target for recruitment so long as the provider does not meet the definition of an "employment agency" under Title VII.[46]
- Some federal civil rights laws are not comprehensive in the classes they protect. Sections 1981 and 1982 of the Civil Rights Act of 1866, and Title VI of the Civil Rights Act of 1964, only apply to race and national origin.[47] Title II additionally applies to religion.[48] But these core statutes do not apply to sex.[49] The scope of classes protected by Section 1985,[50] which prohibits conspiracies against civil rights and has been used to combat commercial discrimination,[51] is unsettled.[52]

---

[43] https://www.lawyerscommittee.org/wp-content/uploads/2022/11/LCCRUL-FTC-Privacy-Comments.pdf
[44] See 42 U.S.C. § 2000a.
[45] See id. § 1981 (prohibiting discrimination in commerce solely on the basis of race and national origin); 42 U.S.C. § 2000a (prohibiting discrimination in public accommodations, but not retail stores, and omitting sex as a protected characteristic).
[46] See generally Miranda Bogen & Aaron Rieke, Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias, Upturn (2018), https://www.upturn.org/reports/2018/hiringalgorithms/.
[47] 42 U.S.C. §§ 1981, 1982, 2000d.
[48] Id. § 2000a.
[49] Title IX extends anti-discrimination protections similar to Title VI to sex discrimination, but only in the context of education. 20 U.S.C. § 1681.
[50] 42 U.S.C. § 1985.
[51] See, e.g., Washington v. Duty Free Shoppers, 696 F. Supp. 1323 (N.D. Cal. 1988).
[52] See, e.g., Bray v. Alexandria Women's Health Clinic, 506 U.S. 263 (1993) (scope of protected classes undecided); United Bhd. of Carpenters & Joiners of Am., Loc. 610, AFLCIO v. Scott, 463 U.S. 825 (1983) (1985(3) scope is undecided, but it does not apply to conspiracies against union organizers).

The Leadership
Conference

- In general, federal civil rights laws may not always cover discrimination against LGBTQ+ people, although the Supreme Court has held that discrimination "because of sex" includes discrimination on the basis of sexual orientation or gender identity.[53]
- Many existing federal civil rights statutes also apply only to intentional discrimination and do not apply to disparate impact. Sections 1981 and 1982, as well as Title II, apply only to intentional discrimination.[54] The Fair Housing Act, Title VII, and the Equal Credit Opportunity Act (ECOA), among other statutes, apply to disparate impact.[55] The federal government can administratively enforce Title VI to address disparate impacts, but private litigants can only bring intentional discrimination claims.
- There are also sectors that lack comprehensive sector-specific civil rights laws akin to the Fair Housing Act or ECOA. For example, Title IX addresses sex discrimination in educational opportunities receiving federal funding,[56] but there is no comprehensive antidiscrimination statute specific to education. Likewise, while the Fair Housing Act, ECOA, and regulations from the Department of Health and Human Services can apply to some forms of insurance discrimination, there is no general civil rights law specific to insurance.
- It is unclear whether existing laws will apply at all to discrimination in many new online-only economies related to online gaming, influencers, streamers, and other creators. The scope of ECOA's application to novel online financial products is also unclear.

Solutions: Principles on the use of data and emerging technologies exist and can be used as guides in addressing the harms experienced by underserved and marginalized communities. But the time has come to implement those principles in concrete ways.

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?

Advocacy organizations, commercial companies and tech firms, industry associations and standards bodies, and governments have each developed sets of principles on these issues over the last few years. They all share common elements, including the need to address harms like bias, transparency, assessments and testing, as well as data protections and security. Enough time, research, and experience has occurred to provide a path for more concrete measures to ensure harms are addressed and mitigated. We highlight several principles below that should inform this work.

---

[53] See Bostock, 140 S.Ct. 1731.

[54] Gen. Bldg. Contractors Ass'n v. Pennsylvania, 458 U.S. 375, 391 (1982) (Section 1981); Daniels v. Dillard's, Inc., 373 F.3d 885, 888 n.4 (8th Cir. 2004) (Section 1982); Joseph v. Metro. Museum of Art, No. 1:15-CV-9358-GHW, 2016 WL 3351103, at *2 (S.D.N.Y. June 15, 2016), aff'd, 684 F. App'x 16 (2d Cir. 2017) (Title II).

[55] See Texas Dep't of Hous. & Cmty. Affs. v. Inclusive Communities Project, Inc., 576 U.S. 519, 545 (2015) (Fair Housing Act); Griggs v. Duke Power Co., 401 U.S. 424, 431 (1971) (Title VII); Michael Aleo & Pablo Svirsky, Foreclosure Fallout: The Banking Industry's Attack on Disparate Impact Race Discrimination Claims Under the Fair Housing Act and the Equal Credit Opportunity Act, 18 B.U. Pub. Int. L.J. 1, 62 n.467 (2008) (ECOA) (collecting cases).,

[56] See 20 U.S.C. § 1681.

The Leadership
Conference

Civil Rights Principles for the Era of Big Data

In 2014, a coalition of civil rights and media justice groups released the "Civil Rights Principles for the Era of Big Data"[57] calling on the U.S. government and businesses to respect and promote equal opportunity and equal justice in the development and use of data-driven technologies. These principles, along with the Obama White House's subsequent reports on big data, highlighted the need for rules of the road for the private and public institutions whose decisions can protect or deny civil and human rights.

Today, while the terminology has shifted from "big data" to "AI" and "biometrics," the issues remain the same and the threats that technology can pose to civil rights have only grown. Recognizing this increased urgency, on October 21, 2020, The Leadership Conference joined dozens of leading civil rights and technology advocacy organizations in updating the Civil Rights Principles for the Era of Big Data. Of relevance to this inquiry, the principles propose a set of civil rights protections that can serve as a guide, including:

Ending High-Tech Profiling

Surveillance technologies are empowering governments and companies to collect and analyze vast amounts of information about people. Too often, these tools are deployed without proper safeguards, or are themselves biased. In some cases, surveillance technologies should simply never be deployed. In other cases, clear limitations and robust auditing mechanisms are needed to ensure that these tools are used in a responsible and equitable way. Law should hold both the government and private actors accountable for abuses.

Ensuring Justice in Automated Decisions

Statistical technologies, including machine learning, inform important decisions in areas such as employment, health, education, lending, housing, immigration, and the criminal-legal system. Decision-making technologies too often replicate and amplify patterns of discrimination in society. These tools must be judged not only by their design but also, even primarily, by their impact — especially on communities that have been historically marginalized. Transparency and oversight are imperative to ensuring that these systems promote just and equitable outcomes. In many cases the best outcome is to not use automated tools in high-stakes decisions at all.

Preserving Constitutional Principles

Enforcement of constitutional principles such as equal protection and due process must keep pace with government use of technology. Search warrant requirements and other limitations on surveillance and policing are critical to protecting fundamental civil rights and civil liberties, especially for communities who have been historically marginalized and subject to disproportionate government surveillance.

---

[57] https://www.civilrightstable.org/civil-rights-principles-for-the-era-of-big-data/

Moreover, governments should not compel companies to build technologies that undermine basic rights, including freedom of expression, privacy, and freedom of association.

Ensuring that Technology Serves People Historically Subject to Discrimination

Technology should not merely avoid harm, but actively make people's lives better. Governments, companies, and individuals who design and deploy technology should strive to mitigate societal inequities. This includes improving access to the internet and addressing biases in data and decision-making. Technologies should be deployed in close consultation with the most affected communities, especially those who have historically suffered the harms of discrimination.

Defining Responsible Use of Personal Information and Enhancing Individual Rights

Corporations have pervasive access to people's personal data, which can lead to discriminatory, predatory, and unsafe practices. Personal data collected by companies also often end up in the hands of the government, either through the direct sale of personal data or through data-driven systems purposely built for the government. Clear baseline protections for data collection, including both primary and secondary uses of data, should be enacted to help prevent these harms.

Making Systems Transparent and Accountable

Governments and corporations must provide people with clear, concise, and easily accessible information on what data they collect and how it is used. This information can help equip advocates and individuals with the information to ensure that technologies are used in equitable and just ways. Any technology that has a consequential impact on people's lives should be deployed with a comprehensive, accessible, and fair appeals process with robust mechanisms for enforcement. Governments and corporations must be accountable for any misuse of technology or data. When careful examination reveals that a new, invasive technology poses threats to civil rights and civil liberties, such technology should not be used under any circumstance.

The AI Bill of Rights

In October 2022, the White House issued a blueprint for an "AI Bill of Rights,"[58] which calls for AI systems to be safe and effective, to not be biased or discriminatory, and to provide notice and explanation, human alternatives to technology, and recourse mechanisms. The AI Bill of Rights also recognizes that, in some instances, just because technology is available doesn't mean it should be used. More recently, the National Institute of Standards and Technology (NIST) published a Risk Management Framework for AI (RMF).[59] The RMF provides a framework for how those designing and using AI can determine whether

---

[58] Blueprint for an AI Bill of Rights | OSTP | The White House; Oct. 4, 2023.

[59] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), January, 2023, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.PDF.

the system is fit for purpose, assess potential outcomes, test and monitor, and other measures, including ensuring that the system does not result in biased or discriminatory outcomes.

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

There are some specific measures that all agencies should take to advance privacy, equity, and civil rights in response to the problems outlines in the RFC, including:

- Ensure ongoing and robust community engagement, including with civil rights groups. This includes requiring community input before technologies are deployed and involving them in continued monitoring and oversight.
- Incorporate multilingual needs.
- Use independent audits and continuous testing and monitoring to ensure accountability.
- Recognize the importance not just of design choices, but the need to assess and test throughout the development and deployment of emerging technologies.
- Adopt regulations and support legislation to codify needed protections. Industry codes of conduct can have limited, little, or no real impact, as they are voluntary, unenforceable, and can be lacking in specificity.

Agencies should also build on what the administration has already done:

- Agencies must implement the AI Bill of Rights.
- Agencies should move forward with meeting the requirements of the February 2023 Executive Order on *Advancing Racial Equity and Support for Underserved Communities Through the Federal Government.* The EO places the following specific requirements on agencies:

    - Directs agencies to produce an annual public Equity Action Plan that assesses and includes actions to address barriers to underserved communities in accessing benefits.
    - Strengthens requirements for agencies to build and resource Agency Equity Teams, including designating senior leaders to be accountable for implementing the equity mandates.
    - Calls for strengthening agencies' Offices of Civil Rights, including ensuring those offices have capacity and resources to fulfill their mandates.
    - Requires agencies to improve the "quality, frequency, and accessibility of community engagement," including consulting with impacted communities. Community engagement is critical to ensure that newly crafted policies meet people's needs.
    - Supports implantation of agencies' Equity Action Plans through budget requests to Congress.
    - Directs agencies to contribute to building wealth and opportunity in rural and urban communities through locally led development.

The Leadership Conference

- o Directs the Interagency Working Group on Equitable Data to facilitate better collection, analysis, and use of demographic data to advance equity, and to regularly report to the public.
- o Instructs agencies to focus their civil rights authorities on "emerging threats" to civil rights, including algorithmic discrimination.
- o Calls on agencies to improve access for people with disabilities and improve language access, recognizing that all impacted communities should be considered by the agencies as they move forward with their Equity Action Plans.
- o Requires agencies to look at their own use of artificial intelligence and to use those systems in ways that advance equity.

Conclusion

It is now well-recognized that commercial data practices can lead to disparate impacts and outcomes for marginalized or disadvantaged communities. As AI systems continue to proliferate, if left unsupervised, with no determinations of bias or discrimination of those systems on communities, no requirements to mitigate those biases, lack of transparency, or without prohibitions where an AI system should not be used, the harmful consequences already experienced by individuals will not only continue but will also likely grow. NTIA's work can and must contribute to addressing those challenges.

Thank you for considering these views. If you have any questions about the issues raised in these comments, please contact Anita Banerji, senior director of the media & tech program, at banerji@civilrights.org; Jonathan Walter, policy counsel, at walter@civilrights.org; or Frank Torres, civil rights technology fellow, at torres@civilrights.org.

Sincerely,

The Leadership Conference on Civil and Human Rights
Color of Change
Common Cause
Communications Workers of America (CWA)
Japanese American Citizens League
Lawyers Committee for Civil Rights Under the Law
National Disability Rights Network (NDRN)
National Fair Housing Alliance
National Urban League
Sikh American Legal Defense and Education Fund (SALDEF)
UnidosUS
United Church of Christ Media Justice Ministry