epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

National Telecommunications and Information Administration

on

Privacy, Equity, and Civil Rights Request for Comment

88 Fed. Reg. 3,714

March 6, 2022

The Electronic Privacy Information Center (EPIC) submits these comments in response to The National Telecommunications and Information Administration (NTIA) Privacy, Equity, and Civil Rights Request for Comment posted on January 20, 2023.[1] NIST is soliciting comments that, together with information collected from three listening sessions, will be used to create a report on "whether and how commercial data practices can lead to disparate impacts and outcomes for marginalized or disadvantaged communities."

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus on public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC has consistently advocated for privacy as a human right, particularly focusing on how privacy issues impact vulnerable communities.[3] We are pleased to continue that work by contributing to this comment opportunity and engaging in further discussion with NIST on how current technology and business practices impact marginalized and vulnerable communities.

---

[1] Privacy, Equity, and Civil Rights Request for Comment, Fed. Reg. 88 Fed. Reg. 3,714 (Jan. 20, 2023), https://www.federalregister.gov/documents/2023/01/20/2023-01088/privacy-equity-and-civil-rights-request-for-comment.

[2] EPIC, *About Us* (2023), https://epic.org/about/.

[3] EPIC, *AI and Human Rights: Criminal Legal Systems* (2022), https://epic.org/issues/ai/ai-in-the-criminal-justice-system/; EPIC, *EPIC Urges DC Council to Pass Algorithmic Discrimination Bill* (Sept. 23, 2022), https://epic.org/epic-urges-dc-council-to-pass-algorithmic-discrimination-bill/; Comments of EPIC, *HUD's Implementation of the Fair Housing Act's Disparate Impact Standard*, Department of Housing and Urban Development (Oct. 18, 2019), https://epic.org/apa/comments/EPIC-HUD-Oct2019.pdf; EPIC, AI & Human Rights (2023), https://epic.org/issues/ai/; Comments of EPIC on the EEOC's Draft Strategic Enforcement Plan for 2023-2027 (Feb. 9, 2023), https://epic.org/documents/comments-of-epic-on-the-eeocs-draft-strategic-enforcement-plan-for-2023-2027/.

In the interest of providing comprehensive and helpful feedback, we have structured our responses to each question by listing the question and subsection, responding directly to the question and subsection in bold, and providing additional references and resources relevant to our responses in a bullet-point list after each response. In some instances, we have left out a subsection where we believed our response to be duplicative of a previous response.

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?

   Privacy is an important aspect of evaluating civil rights and equity harms of commercial data collection and processing. NTIA should also evaluate how those harms impact equity, justice, and fairness and incorporate conceptual frameworks like commercial surveillance, abusive data practices, informational asymmetry, and digital deception.

   - EPIC's Comments for FTC's ANPR on Commercial Surveillance & Data Security: *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystems*[4]
     - Introduction (p. 1)
     - Data Minimization (p. 30)
     - Notice and Transparency (p. 152)
     - Dark Patterns & Digital Deception (p. 216)
   - EPIC and Consumer Reports Data Minimization White Paper: *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*[5]

   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 requirement or controls; and what are some examples of their limitations?

   Most notice and consent or transparency requirements cannot be fully effective, on their own, to mitigate harms from commercial data practices. Many of these practices are too

[4] Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security, https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf [hereinafter *EPIC FTC Comments on Commercial Surveillance*].
[5] EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf [hereinafter *EPIC and Consumer Reports Data Minimization White Paper*].

complex and numerous for even the most sophisticated consumer to understand and meaningfully consent to, and consumers can also be harmed by data processing activities that are unvetted or undisclosed.

- EPIC FTC Comments on Commercial Surveillance
    - Data Minimization (p. 30)
    - Automated Decision-Making Systems (p. 67)
    - Notice and Transparency (p. 152)
    - Dark Patterns & Digital Deception (p. 216)

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?

The concepts of sensitive and non-sensitive data often overlap. Data can become sensitive when used together or cross-referenced with unique persistent identifiers, data linkable to an individual device, non-aggregated data, and other mechanisms that can be used to identify an individual. Discussions of privacy and fairness in automated decision-making contexts can also benefit from considering the harm, use, and risk of data instead of its inherent sensitivity.

- EPIC FTC Comments on Commercial Surveillance
    - Scope of Covered Data (p. 24)
    - Automated Decision-Making Systems (p. 67)
- Daniel J. Solove, *Data is what Data Does: Regulating Use, Harm and Risk Instead of Sensitive Data,* 116 Northwestern Univ. L. Rev. (Forthcoming) (Jan. 11, 2023), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.

d. Some privacy experts have argued that the collective implications of privacy protections and invasions are under-appreciated. 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 understanding of privacy highly relevant. 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?

Individual rights are not sufficient to protect privacy unless paired with systemic policy interventions like substantive limits on data collection. A narrow focus on individual privacy harms can exclude collective privacy harms that affect entire groups and communities.

- EPIC FTC Comments on Commercial Surveillance
    - Notice and Transparency (p. 152)

- Woodrow Hartzog, *What is Privacy? That's the Wrong Question,* 88 Univ. of Chicago L. Rev. 1677 (Nov. 29, 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3970890.

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?

Such proposals should be attentive to the ability to derive sensitive inferences from publicly available data. It is important that de-identified data is clearly defined and differentiated from personal data such that it would be impossible to connect de-identified data to an individual.

- EPIC FTC Comments on Commercial Surveillance
  - Scope of Covered Data (p. 24)
- Colorado Privacy Act § 6-1-1303(11) (only data that cannot reasonably be used to infer information about or otherwise be linked to an identified or identifiable individual or device linked to that individual may be considered de-identified data and parties using de-identified data must make commitments to use and maintain the data solely in de-identified form).
- California Consumer Protection Act § 1798.148(c) (requires a contract in place for any sale or licensing of deidentified information that includes specific provisions prohibiting reidentification).
- American Data Privacy and Protection Act (ADPPA) § 2(10) (2022) (mandates that de-identified data cannot identify or be linked or reasonably linkable to an individual or individual's device, regardless of whether information is aggregated).

g. Civil rights experts and automated decision-making experts have raised concerns about the incongruity between the requirements in civil rights laws and how automated systems can produce discriminatory outcomes with the intentional guidance of a programmer. 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 and gender? How do data practices and privacy practices affect each?

Automated decision-making systems can facilitate, exacerbate, and cause various harms including bodily harm, loss of liberty, loss of opportunity, financial harms, dignitary harms, and discriminatory harms. The outputs of these systems should be evaluated by their impact—for example, through design analysis or disparate impact analysis.

- EPIC FTC Comments on Commercial Surveillance
  - Automated Decision-Making Systems (p. 67)
  - Discrimination (p. 109)
- EPIC Screened & Scored in D.C. Report[6]

[6] EPIC, *Screened & Scored in D.C.* (2022), https://epic.org/screened-scored-in-dc/.

- EPIC amicus brief in *Gonzalez v. Google*[7]

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?

Commercial data collection and processing practices can cause various harms to marginalized groups and other populations, including where commercially collected data is subject to automated decision-making systems. The impacts of these systems are especially acute for marginalized communities, fostering discrimination and inequities in employment, government services, healthcare, and education.

- Anita Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J.F. 907, 913-28 (Feb. 20, 2022), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon.
- Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018)
- Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com., 117th Cong. (2022) (testimony of David Brody), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents /Testimony_Brody_CPC_2022.06.14.pdf.
- Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793, 855–59 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
- EPIC comments to the FCC on Securus Technology and inmate calling services[8]

[7] Brief for EPIC as Amicus Curiae, *Gonzalez v. Google*, LLC, No. 21-1333 (U.S. Dec. 7, 2022).
[8] EPIC, *Comments to the FCC on Securus Technologies, LLC's Petition for Waiver of the Inmate Calling Services Per-Minute Rate Requirement,* 86 Fed. Reg. 70,427 (Jan. 7, 2022), https://epic.org/documents/epic-comments-on-securus-technologies-petition-for-prison-phone-services-alternative-pricing-scheme/.

b. In what ways to 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?

Ensuring accessibility is vital to providing the benefits of various technologies to people with disabilities. People with disabilities can have unique digital needs, including assistive technologies. There are also unique harms that arise from the incompatibility of digital services with a disability. For example, algorithms are often fail to account for the diversity of disabled people.

- CDT report, *Centering Disability in Technology Policy*[9]
- EPIC FTC Complaint re: HireVue[10]
- EPIC D.C. Attorney General Complaint re: Online Test Proctoring[11]

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?

Certain data collection and use practices—including targeted advertising, customer acquisition, and customer evaluation—can create and perpetuate discrimination and unfair treatment of marginalized groups.

- EPIC FTC Comments on Commercial Surveillance
    - Automated Decision-Making Systems (p. 67)
    - Discrimination (p. 109)
- EPIC Screened & Scored in D.C. Report
- EPIC Buy Now, Pay Later Comments[12]
- Danielle Keats Citron & Daniel J. Solove, Privacy Harms, 102 B.U.L. Rev. Online 793 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
- Calli Schroeder & Cobun Keegan*, Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms*, 15 J. L. Econ. & Pol'y 1, 27 (2018),

[9] Henry Claypool, Claire Carey, Alexander C. Hart, & Linnea Lassiter, *Centering Disability in Technology Policy: Issue Landscape and Potential Opportunities for Action,* Center for Democracy & Technology & American Association of People with Disabilities (Dec. 2021), https://cdt.org/wp-content/uploads/2021/12/centering-disability-120821-1326-final.pdf.

[10] *Complaint and Request for Investigation, Injunction, and Other Relief, In the Matter of HireVue, Inc.,* EPIC submitted to the FTC (Nov. 6, 2019), https://epic.org/documents/in-re-hirevue/.

[11] *Complaint and Request for Investigation, Injunction, and Other Relief, In the Mattr of Online Test Proctoring Companies Respondus, Inc.; ProctorU, Inc.; Proctorio, Inc.; Examity, Inc.; and Honorlock, Inc.,* EPIC submitted to the Attorney General of the District of Columbia (Dec. 9, 2020), https://epic.org/documents/in-re-online-test-proctoring-companies/.

[12] EPIC, *Comments of the Electronic Privacy Information Center to the Consumer Financial Protection Bureau, Request for Comment and Notice, Re: market Monitoring Buy Now, Pay Later,* 87 Fed. Reg. 3,511 (Mar. 25, 2022), https://epic.org/wp-content/uploads/2022/03/EPIC-Comments-CFPB-BNPL-2022-03-25.pdf [hereinafter *EPIC's Buy Now, Pay Later Comments*].

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4204208.

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?

Disproportionate harm can result from data collection and processing, targeted advertising, and the use of certain automated decision-making systems. Many of these tools are used without disclosure or due diligence, harming individuals in healthcare, banking, employment, and educational settings.

- EPIC FTC Comments on Commercial Surveillance
  - Automated Decision-Making Systems (p. 67)
  - Discrimination (p. 109)
- EPIC FTC Complaint re: HireVue
- EPIC Screened & Scored in D.C. Report
- EPIC Buy Now, Pay Later Comments

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

Commercial uses of biometric technologies, including face recognition and "emotion detection," warrant heightened scrutiny for their potential to enable discrimination and cause privacy harms. Not only do these technologies implicate sensitive biometric information; their use in commercial settings is often unavoidable and may not be disclosed to consumers.

- EPIC FTC Comments on Commercial Surveillance
  - Automated Decision-Making Systems (p. 67)
- EPIC NIST Comments re: AI Risk Management Framework[13]

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?

[13] EPIC, *Feedback of the Electronic Privacy Information Center to the National Institute of Standards and Technology Regarding the Artificial Intelligence Risk Management Framework: Second Draft* (Sept. 28, 2022), https://epic.org/epic-submits-additional-feedback-on-nist-ai-risk-management-framework/.

Proxy discrimination can arise in data collection, data analysis, and automated decision-making. Mass commercial surveillance and profiling can reveal, and risk discrimination against, protected traits. This data can include location data, health information, employment data, and credit or financial data. Additionally, automated decision making-systems can perpetuate proxy discrimination.

- EPIC FTC Comments on Commercial Surveillance
  - Data Minimization (p. 30)
  - Automated Decision-Making Systems (p. 67)
  - Discrimination (p. 109)
- Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 Iowa L. Rev. 1257 (2020), https://perma.cc/SC2T-8RHN.
- EPIC letter to FTC about Airbnb automated decision-making system[14]

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?

Commercial surveillance practices pose challenges to civil rights, privacy and equity that are distinct from brick-and-mortar commerce. Consumers do not have the ability to meaningfully consent to mass data collection, surveillance, or the effect of automated decision-making systems fueled by that data. These commercial surveillance and algorithmic decision-making systems disproportionately harm marginalized communities.

- EPIC FTC Comments on Commercial Surveillance
  - Data Minimization (p. 30)
  - Automated Decision-Making Systems (p. 67)
  - Discrimination (p. 109)
  - Privacy of Minors (p. 167)
  - Dark Patterns & Digital Deception (p. 216)
- FTC Enforcement Action against Fortnite video game maker Epic Games[15]

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

[14] *Supplemental Letter: In re Airbnb,* EPIC Letter to FTC (Aug. 18, 2022), https://epic.org/documents/supplemental-letter-in-re-airbnb/.
[15] *In the Matter of Epic Games, Inc., a corporation,* FTC Agreement Containing Consent Order, File No. 192 3202 (Dec. 19, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations.

equity or civil rights concerns? What about the collection and sharing of consumer data by private actors for "public safety purposes"?

There are many examples of government using commercial data or automated decision-making systems fueled by commercial data. Without notice and consent, many government offices use risk assessments or other automated tools to screen and score people, often implicating equity and civil rights concerns. Additionally, public safety agencies and police have used inaccurate facial recognition systems, and ICE has contracted with LexisNexis for invasive surveillance.

- EPIC, Coalition Call for ICE to Cancel Contract with LexisNexis for Invasive Surveillance Databases[16]
- EPIC Screening & Scoring Project
- EPIC Campaign to Ban Face Surveillance[17]
- EPIC urges the FTC to adequately disclose affiliate relationships, like between Amazon Ring and law enforcement organizations[18]

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?

Consolidation in the tech and telecom sectors has eroded consumer privacy and stifled innovation. The more dominant a company becomes, the greater its ability to surveil consumers and amass personal information. This concentration of data relates to equity and civil rights concerns through privacy issues and the profiling and tracking that enables discriminatory targeted advertising, and redlining.

- EPIC Statement on the Digital Advertising Ecosystem[19]
- Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018) (technological redlining)

[16] *EPIC, Coalition Call for ICE to Cancel contract with LexisNexis for Invasive Surveillance Databases,* EPIC (Feb. 23, 2023), https://epic.org/epic-coalition-call-for-ice-to-cancel-contract-with-lexisnexis-for-invasive-surveillance-databases/.
[17] EPIC, *Ban Face Surveillance*, https://epic.org/campaigns/ban-face-surveillance/.
[18] *Comments of the Electronic Privacy Information Center to the Federal Trade Commission, Advanced Notice of Proposed Rulemaking and Request for Comment on Reviews and Endorsements,* 87 Fed. Reg. 67,425 (Jan. 9, 2023), https://epic.org/documents/epic-comments-on-ftc-advanced-notice-of-proposed-trade-regulation-rule-on-use-of-reviews-and-endorsements/.
[19] EPIC Statement, *Understanding the Digital Advertising Ecosystem and the Impact of Data Privacy and Competition Policy,* 116th Cong., S. Comm. on the Judiciary (May 20, 2019), https://epic.org/documents/understanding-the-digital-advertising-ecosystem-and-the-impact-of-data-privacy-and-competition-policy/.

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?

Disparate impacts of privacy abuses have been insufficiently recognized and prioritized in privacy law and policy. Examples of this can be seen in housing algorithms discriminating against the poor and people of color, discriminatory patterns in employment algorithms, and the reduced accuracy of facial recognition on individuals with darker skin tones or non-binary gender presentation. In addition, highly sensitive inferences can be drawn about an individual and used to profile them without the individual ever directly disclosing such information.

- EPIC FTC Comments on Commercial Surveillance
  - Data Minimization (p. 30)
  - Automated Decision-Making Systems (p. 67)
  - Discrimination (p. 109)
  - Notice and Transparency (p. 152)
  - Privacy of Minors (p. 167)
  - Dark Patterns & Digital Deception (p. 216)
- EPIC Screened & Scored in D.C. Report
- Anita Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J.F. 907 (Feb. 20, 2022), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon.
- Danielle Citron & Daniel Solove, *Privacy Harms,* 102 B.U.L. Rev. Online 793 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf[20]

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?

While both civil rights laws and privacy laws may identify multiple categories of information as sensitive (race, ethnicity, sexuality, religion, etc.), intersectionality is rarely specifically addressed by law. But the challenges of intersectional discrimination are real. For example, in a discrimination suit, an individual may have limit their claims to one marginalized identity rather than multiple in order to avoid confusing or overwhelming a judge or jury. A strong privacy approach to intersectionality should consider how each additional marginalized identity can multiply the risk of harms to an individual..

- EPIC FTC Comments on Commercial Surveillance

[20] Particularly pages 855-59, which discuss discrimination harms as a privacy harm, and page 818, which discusses the risk of mass data collection allowing for unanticipated and unwanted inferences on individuals.

    - Discrimination (p. 121-123)
- Renee Shelby, Jenna Imad Harb, & Kathryn Henne, *Whiteness in and through data protection: an intersectional approach to anti-violence apps and #MeToo bots,* Internet Policy Rev. 10.4 (Dec. 7, 2021), https://policyreview.info/articles/analysis/whiteness-and-through-data-protection-intersectional-approach-anti-violence-apps.
- Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Procs. of Machine Learning Res. 77–91 (2018), http://proceedings.mlr.press/v81/buolamwini18a.html.

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

Much like privacy laws themselves, the enforcement of privacy and civil rights laws in the U.S. is an uneven patchwork subject to the variable resources and priorities of different agencies and officials. This patchwork means that privacy and civil rights are inconsistently enforced against and may fall through the cracks in areas with busy or under resourced enforcement bodies. Approaches that could allow for more effective and consistent enforcement include a private right of action and a single agency tasked with enforcement.

- EPIC Screened & Scored in D.C. Report
- Hearing on Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security[21]
- EPIC FTC Comments on Commercial Surveillance
    - The FTC and the Data Protection Crisis (p. 7)
- Complaint for Injunctive Relief, *EPIC v. FTC*[22]
- EPIC: The U.S. Urgently Needs a Data Protection Agency[23]

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?

There may be cases where privacy law conflicts with equity and safety issues for marginalized communities, such as where privacy laws would prevent recording or dissemination of videos showing threats or attacks. These risks must be weighed against the threat of surveillance, monitoring, and algorithmic discrimination to those same communities.

[21] *Hearing on Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security*, House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce, U.S. House of Representatives (June 14, 2022), https://epic.org/documents/hearing-on-protecting-americas-consumers-bipartisan-legislation-to-strengthen-data-privacy-and-security/.
[22] *Complaint for Injunctive Relief,* EPIC v. FTC, No. 1:18-cv-00942 (Apr. 20, 20218), https://epic.org/wp-content/uploads/foia/ftc/facebook/EPIC-v-FTC-Complaint.pdf.
[23] EPIC, *The U.S. Urgently Needs a Data Protection Agency*, https://epic.org/campaigns/dpa/.

- Renee Shelby, Jenna Imad Harb, & Kathryn Henne, *Whiteness in and through data protection: an intersectional approach to anti-violence apps and #MeToo bots,* Internet Policy Rev. 10.4 (Dec. 7, 2021), https://policyreview.info/articles/analysis/whiteness-and-through-data-protection-intersectional-approach-anti-violence-apps.
- EPIC FTC Comments on Commercial Surveillance
    - Data Minimization (p. 30)
    - Automated Decision-Making Systems (p. 67)
    - Discrimination (p. 109)
    - Notice and Transparency (p. 152)
    - Privacy of Minors (p. 167)
    - Dark Patterns & Digital Deception (p. 216)
- ADPPA Section 207

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?

Algorithmic transparency is one of the most effective approaches to identifying and remedying wrongful outcomes, particularly for marginalized communities and individuals. Additional measures include mandating algorithmic impact assessments and regular audits, requiring algorithm developers and users to explain design choices, and pursuing lawsuits to address and mitigate bias and harmful impacts.

- EPIC Screened & Scored in D.C. Report
- EPIC, *EPIC v. CBP (Analytical Framework for Intelligence)*[24]
- EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)*[25]
- EPIC FTC Comments on Commercial Surveillance
    - Automated Decision-Making Systems (p. 67)

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?

A variety of foreign privacy laws, including the GDPR, APPD, DDPA, LGPD, PDPL, and FPA, recognize certain types of data as more sensitive and subject to additional protections. These include race, religion, sexual orientation, and other characteristics. These designations are helpful, but do not alone fully address or prevent privacy harms to marginalized communities—particularly those that may stem from less explicit targeting, such as inferences or algorithms. Other laws fall short by excluding

[24] *Complaint for Injunctive Relief,* EPIC v. U.S. Customs and Border Protection, Case 1:14-cv-01217-RBW (July 18, 2014), https://epic.org/documents/epic-v-cbp-analytical-framework-for-intelligence/.
[25] *Complaint for Injunctive Relief,* EPIC v. U.S. Department of Justice, Civ. Action No. 17-410 (Mar. 7, 2017), https://epic.org/documents/epic-v-doj-criminal-justice-algorithms/.

government activity from the scope of regulation and still allowing for surveillance and tracking through mass algorithmic data collection, as in the PIPL.

- The EU's General Data Protection Regulation (GDPR)
- Denmark's 2000 Act of Processing Personal Data (APPD) and Danish Data Protection Act (DDPA)
- Brazil's Lei Geral de Proteçao de Dados (LGPD)
- Chile's Personal Data Protection Law (PDPL)
- Australia's Federal Privacy Act (FPA)
- American Data Privacy and Protection Act (ADPPA) Section 207
- Biometric Information Privacy Act (BIPA)
- China's Personal Information Protection Law (PIPL)
- EPIC Comments on UK Draft Updated Surveillance Camera Code of Practice[26]

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?

While a variety of approaches have been proposed to prevent and remedy privacy harms inflicted on marginalized communities, an ideal approach would explicitly mandate antidiscrimination actions and monitoring. This would include regular audits to ensure there is no discrimination in results of policies and actions and ideally would include a concentrated effort to engage communities that may be harmed to understand and mitigate those harms. In addition, there must be robust and consistent enforcement against privacy violators, particularly for violations disproportionately harm vulnerable communities.

- EPIC: The U.S. Urgently Needs a Data Protection Agency
- EPIC and Consumer Reports Data Minimization White Paper
- White House OSTP, *Blueprint for an AI Bill of Rights*[27]
- Jessica L. Roberts, *Protecting Privacy to Prevent Discrimination*, 56 Wm. & Mary L. Rev. 2097 (2015), https://scholarship.law.wm.edu/wmlr/vol56/iss6/4.
- Nicol Turner Lee, Paul Resnick, and Genie Barton, "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms," The Brookings Institution (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

[26] *Comments of the Electronic Privacy Information Center to the United Kingdom Biometrics and Surveillance Camera Commissioner Regarding the Draft Updated Surveillance Camera Code of Practice,* ICO (Sept. 8, 2021), https://epic.org/epic-urges-uk-surveillance-commissioner-to-foreground-privacy-ban-facial-recognition-in-updates-to-surveillance-camera-code/.

[27] White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

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?

In cases where information about race, sex, or other protected characteristics must be gathered to identify and prevent bias or to specifically benefit marginalized communities, that information must be gathered with the full knowledge and consent of the individuals. In addition, the use of that information must be strictly limited to the specific purpose for which it was collected and it must not be shared with other parties for any other purpose.

- Jessica L. Roberts, *Protecting Privacy to Prevent Discrimination*, 56 Wm. & Mary L. Rev. 2097 (2015), https://scholarship.law.wm.edu/wmlr/vol56/iss6/4.
- EPIC FTC Comments on Commercial Surveillance
    - Data Minimization (p. 30)
    - Automated Decision-Making Systems (p. 67)
    - Discrimination (p. 109)
    - Notice and Transparency (p. 152)
    - Dark Patterns & Digital Deception (p. 216)

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?

Principles like data minimization, transparency, accuracy, and fairness are reflected in federal and state level proposals, including the Facial Recognition Moratorium, Algorithmic Accountability Act, ADPPA and various state data protection laws. Centering these principles can address the disproportionate harms that marginalized groups face in the current commercial surveillance environment.

- ADPPA §207
- Algorithmic Accountability Act
- Facial Recognition Moratorium

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?

A robust data minimization framework is necessary to protect minors from data abuses online. In particular, personal data of minors should only be collected, processed, or

transferred where strictly necessary. Other protections include a ban on targeted advertising and evidence-based policymaking that considers the unique harms that minors face online.

- EPIC FTC Comments on Commercial Surveillance
  - Data Minimization (p. 30)
  - Privacy of Minors (p. 167)

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

Older adults can face exploitation, fraud, and bias online. Where consent is required for data collection or automated decision-making systems, the consent mechanism should be in plain language that all individuals—including older adults—can understand. Oversight is necessary to combat discrimination in automated decision-making systems, as these systems can be based on biased data sets that exclude older adults. Finally, older adults deserve protection against data brokers that compile lists or information about older adults that are vulnerable to fraud or exploitation.

- AARP FTC Comments on Commercial Surveillance[28]
- *Data Brokers, Elder Fraud, and Justice Department Investigations*[29]

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?

Overcollection and misuse of personal information harms millions of consumers. Legislators and regulators should center data minimization as an equity-focused approach to address these issues. A business should not collect, use, retain or transfer a consumer's personal information beyond what is reasonably necessary and proportionate to achieve the primary purpose for which it was collected, which must be consistent with consumer expectations and the context in which the data was collected.

- EPIC FTC Comments on Commercial Surveillance
  - Data Minimization (p. 30)

e. Considering resources, strategic prioritization, legal capacities and constraints, and other factors, what can federal agencies currently do to better address harmful data collection

[28] *Comments of the AARP to the FTC Re: Trade Regulation Rule on Commercial Surveillance and Data Security,* ANPR R111004 (Nov. 21, 2022), https://www.aarp.org/content/dam/aarp/politics/advocacy/2022/11/aarp-ftc-surveillance-data-security-anprm-11-21-22.pdf.

[29] Alistair Simmons & Justin Sherman, *Data Brokers, Elder Fraud, and Justice Department Investigations,* LawFare (July 25, 2022), https://www.lawfareblog.com/data-brokers-elder-fraud-and-justice-department-investigations.

practices, particularly the impact of those practices on underserved or marginalized groups? What other executive actions might be taken, such as issuing executive orders?

Federal agencies can consider procurement rules, data storage and privacy technologies, and enforcement actions to address harmful data collection and storage practices.

- EPIC FTC Comments on Commercial Surveillance
  - The FTC's Authority (p. 12)
- *EPIC*: What the FTC Could be Doing (But Isn't) To Protect Privacy[30]
- *EPIC*: Privacy, Surveillance, and AI in the FY'23 National Defense Authorization Act[31]

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

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?

Third-party audits and impact assessments are important tools to evaluate and address harms of commercial surveillance and automated decision-making systems. However, reliance on notice and choice mechanisms and deference to industry-backed self-regulation have failed to blunt the impact of harmful data collection. Third party-audits and impact assessments should be paired with meaningful limits on data collection and requirements that automated-decision making systems not be used without first demonstrating that they are effective, accurate and free from impermissible bias.

- EPIC FTC Comments on Commercial Surveillance
  - Data Minimization (p. 30)
  - Automated Decision-Making Systems (p. 67)
  - Notice and Transparency (p. 152)
- Canadian Algorithmic Assessment Tool[32]

---

[30] *What the FTC Could Be Doing (But Isn't) to Protect Privacy: The FTC's Unused Authorities,* EPIC Report (June 2021), https://epic.org/documents/epic-ftc-unused-authorities-report-june2021-2/.
[31] Chris Baumohl, John Davisson, Jake Wiener, & Ben Winters, *Privacy, Surveillance, and AI in the FY'23 National Defense Authorization Act (NDAA),* EPIC (Jan. 26, 2023), https://epic.org/privacy-surveillance-and-ai-in-the-fy23-national-defense-authorization-act-ndaa/.
[32] *Algorithmic Impact Assessment Tool*, Government of Canada, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html.

- Washington State Senate Bill 5116[33]

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 disproportionately experienced by marginalized communities? What role might design play in alleviating harms caused by discriminatory or privacy-invasive data practices?

Deceptive design tactics have become increasingly sophisticated, manipulating users and causing harm by undermining consumer autonomy and subverting privacy choices. With respect to the privacy of minors, California has enacted the Age Appropriate Design Code, and other states have introduced similar bills addressing privacy and autonomy harms to minors online.

- EPIC FTC Comments on Commercial Surveillance
  - Dark Patterns & Digital Deception (p. 216)
- California Age-Appropriate Design Code[34]

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?

Self-regulation has failed to meaningfully protect and address the impact of harmful data collection. Notice and choice mechanisms are particularly ineffective; the burden should not be on consumers to avoid harms in an increasingly complex data collection and processing ecosystem. Instead of relying on ineffective self-regulation, NTIA should encourage a data minimization framework in line with reasonable expectation of consumers, addressing overcollection and out-of-context secondary uses of personal data.

- EPIC FTC Comments on Commercial Surveillance
  - Data Minimization (p. 30)
  - Notice and Transparency (p. 152)

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

[33] Substitute Senate Bill 5116, State of Washington 67th Legislature, 2021 Regular Session S-0744.2 (Feb. 8, 2021), https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5116-S.pdf?q=20210209103349.

[34] California Age-Appropriate Design Code Act, California Legislature AB-2273 (2021-2022), https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false.

attract, empower, and retain technological experts, particularly experts belonging to marginalized communities? Are there any best practices that should be emulated?

Government should focus its resources on oversight, enforcing uniform standards and requirements to address the privacy, equity and civil rights issues stemming from commercial surveillance.

- EPIC FTC Comments on Commercial Surveillance
  - Data Minimization (p. 30)
  - Automated Decision-Making Systems (p. 67)
- EPIC Comments on the National Security Commission on Artificial Intelligence AI[35]

CONCLUSION

We applaud NIST's attention to technology and business practices that disparately impact marginalized and historically excluded communities, and we hope that these comments have assisted in identifying harms and proposing steps to mitigate them in the future. In particular, we note that (i) the NTIA should encourage specific requirements, such as mandating oversight and implementing data minimization standards, rather than allowing for industry self-regulation that does not adequately address the listed harms; (ii) the onus to avoid harms cannot rest on consumers; and (iii) transparency (including algorithmic transparency and mandatory risk and impact assessments) is a key component of meaningful oversight. We look forward to NIST's report on these matters.

Respectfully Submitted,

/s/ *Suzanne Bernstein*
Suzanne Bernstein
EPIC Law Fellow

/s/ *Calli Schroeder*
Calli Schroeder
EPIC Senior Counsel &
Global Privacy Counsel

/s/ *Jake Wiener*
Jake Wiener
EPIC Counsel

[35] *Comments of the Electronic Privacy Information Center to the National Security Commission on Artificial Intelligence,* 85 Fed. Reg. 32,055 (Sept. 30, 2020), https://epic.org/wp-content/uploads/apa/comments/EPIC-comments-to-NSCAI-093020.pdf.