Comments of Consumer Reports
In Response to the
National Telecommunications and Information Administration
Request for Comment On
Privacy, Equity, and Civil Rights

By

Matt Schwartz, Policy Analyst
Justin Brookman, Director of Technology Policy

March 6, 2023

CR Consumer Reports®

Consumer Reports[1] appreciates the opportunity to provide feedback on the National Telecommunication and Information Administration's (NTIA) Request for Comment on Privacy, Equity, and Civil Rights. We thank NTIA for initiating this proceeding and for its other efforts to investigate the effects of invasive commercial data practices.

We describe our views on the intersections between privacy, equity and civil rights in detail below in the course of providing answers to NTIA's questions posed in the Request for Comment.

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

<u>a. Is "privacy" the right term for discussing these issues? Is it under-inclusive? Are there more comprehensive terms or conceptual frameworks to consider?</u>

<u>b. To what degree are individuals sufficiently capable of assessing and mitigating the potential harms that can arise from commercial data practices, given current information and privacy tools? What value could additional transparency requirements or additional privacy controls provide; what are examples of such requirements or controls; and what are some examples of their limitations?</u>

Consumers currently possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they collect and process that information (so long as they note their behavior somewhere in their privacy policy). As a result, consumers' every move is constantly tracked and often combined with offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is sold as a matter of course, is used to deliver targeted advertising, facilitates differential pricing, and enables opaque algorithmic scoring—all of which can lead to disparate outcomes along racial and ethnic lines.

At the same time, spending time online has become integral to modern life, with many individuals required to sign-up for accounts with tech companies because of school, work, or simply out of a desire to connect with distant family and friends. As we expect most commentators will tell you, the current "notice and choice" regime, in which consumers are

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

expected to read extensive privacy policies and make “all or nothing” decisions about whether to use an online service or app, makes it impossible for consumers to meaningfully participate in the market while protecting their privacy. Even if consumers had the time to read every privacy policy and statement, they would in most cases come away with woefully incomplete information. Such policies tend to be vague and expansive, designed to protect a company from liability rather than inform privacy-conscious consumers. In many cases, the companies themselves have not decided to whom data will be sold and the purposes for which it will be used. It is impossible for consumers to assess the cost of a loss of control over their personal information, or to determine a value and “trade” their data for goods or services.

The solution to this problem is not simply better privacy policies. Even if such policies contained complete and understandable information, no consumer has the capacity or would want to process such policies for every website, app, and service they use and make discrete choices about their personal privacy. Even asking consumers to manage cookie settings on individual pages is overly burdensome and impractical; expecting consumers to read hundreds of different privacy policies is absurd. Simply put, privacy policies are not a useful mechanism for providing information to consumers.

That said, privacy policies may still play some role in a privacy regulation regime. While consumers should not be expected to read privacy policies in the ordinary course of business, they can still provide simple and clear instructions to consumers on how to exercise privacy rights such as the right of access. Moreover, privacy policies can serve another role in providing detailed information to regulators, advocates, researchers, and journalists to ensure that information practices of the biggest companies are consistent with the principles of data minimization and other privacy requirements.

As detailed in our Model State Privacy Act, Consumer Reports recommends a bifurcated approach to privacy policies: (1) all companies should provide a short, accessible, and clear description on how consumers should exercise privacy rights and (2) the largest and most sophisticated companies should provide detailed information about their data processing activities to create transparency and external accountability for what they do with personal data.[2] For the latter function, privacy policies should thus function more like SEC filings — providing detailed information to the most sophisticated audiences but which no ordinary consumer is expected to read or understand. However, the mandate to provide this information to the public will still serve as a meaningful check on companies who might otherwise prefer that questionable data processing go unnoticed.

It is extremely difficult for even sophisticated consumers to understand how companies collect, use, process, and retain data. Most data processing is functionally invisible to consumers; some first-party data collection may be expected given the nature of a customer interaction. However, what happens to that data on a company’s servers is inscrutable — it may be retained

[2] Consumer Reports, Model State Privacy Act, (Feb. 2021), § 100, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf .

indefinitely, used for unexpected purposes, sold to data brokers, or inadvertently exposed to hackers. Offline data sharing is completely unobservable to consumers. Much online data sharing is facilitated directly by a user's browser — consumers can install a special extension to see which third parties a website is sharing data with. However, few consumers actually take the time to do that. Moreover, these tools are less readily available for mobile platforms, let alone Internet of Things devices such as smart televisions. Even when data collection is technically observable, it may be encrypted by the company; this prevents inspection by outside hackers but also may prevent inspection by the device's owner.

Consumers who encounter retargeted or surprisingly targeted ads often wonder how companies were able to gain such insights. Even when the source of targeting seems straightforward, consumers cannot know for sure the reason. For example, a recent Consumer Reports study showed that even when manually opting out of cookies on a publisher site, researchers later saw ads from that same company on other sites.[3] However, while it seems likely that the cookie controls on the original site simply did not work, there is no way to know for certain — consumers do not have access to the targeting logic used by marketing companies.

Many companies actively deliberately frustrate efforts of consumers and researchers to hold them accountable for their data practices. For example, researchers at New York University created a tool called Ad Observatory, where they obtained consent from volunteer Facebook users who gave the researchers access to the ads the users were seeing on their newsfeed. This study gave the researchers insight into how political ads were algorithmically targeted to users, and the collected ads were put into a publicly available database for other researchers and journalists to examine.[4] However, in August 2021, Facebook disabled the accounts of the researchers conducting the study, effectively halting their research.[5] As detailed in a recent Consumer Reports white paper, companies can use any number of technical and legal mechanisms to frustrate external research into data practices, including contract terms, computer trespass laws, and intellectual property rights.[6] As a result, it is functionally very difficult to understand how consumers are monitored and tracked online.

[3] Thomas Germain, I Said No to Online Cookies. Websites Tracked Me Anyway., Consumer Reports, (Sep. 29, 2022), https://www.consumerreports.org/electronics-computers/privacy/i-said-no-to-online-cookies-websites-tracked-me-anyway-a8480554809/; see also Justin Brookman et al., Cross-Device Tracking: Disclosures and Measurements, Privacy Enhancing Technologies Symposium (PETS) 2017 (2):133–148, https://petsymposium.org/2017/papers/issue2/paper29-2017-2-source.pdf.

[4] Shirin Ghaffary, People do not trust that Facebook is a healthy ecosystem, Vox, (Aug. 6, 2021),https://www.vox.com/recode/22612151/laura-edelson-facebook-nyu-ad-observatory-social-media-researcher

[5] Lois Anne DeLong, Facebook Disables Ad Observatory; Academicians and Journalists Fire Back, NYU Center for Cybersecurity, (Aug. 21, 2021), https://cyber.nyu.edu/2021/08/21/facebook-disables-ad-observatory-academicians-and-journalists-fire-back/

[6] Nandita Sampath, Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing, Consumer Reports Digital Lab, (Oct. 2022), https://digital-lab.consumerreports.org/2022/10/13/new-paper-opening-black-boxes-addressing-legal-barriers-to-public-interest-algorithmic-auditing/

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?

For the most part, the Consumer Reports does not believe privacy law needs to distinguish between “sensitive” and “non-sensitive” data— instead all data should be subject to strict data minimization requirements. Strong data minimization provisions are our first choice because they prevent consumers from constantly operating from a defensive position where they must determine whether each company that they interact with performs processing activities they consider acceptable or not.
Additionally, given current company data processing capabilities, it is unclear whether there is a truly a meaningful distinction between sensitive and non-sensitive data; plenty of so-called “non-sensitive” personal information, when combined in certain ways, can become sensitive, and companies can often use their vast stores of non-sensitive data to infer sensitive attributes about a person. The Federal Trade Commission has, for example, identified categories such as geolocation[7] and TV viewing[8] as “sensitive” and worthy of greater protection; however, other common categories of data collection — such as web browsing and shopping — can in many cases be at least as if not more revealing about personal behavior.

The boundaries of “sensitive” are also highly dependent on the person and context, which brings to the fore important equity and civil rights considerations. Certain individuals with certain lived experiences may not want certain information about their lives revealed, whereas that same information may be entirely unobjectionable to another person. As such, there are immense challenges in scoping the definition of sensitive information. A common outcome, at least in the case of state privacy laws, is that the sensitive data category (if such a category exists) is under-inclusive.[9]

It may be reasonable to require heightened and prominent notice to consumers when a company is required to process sensitive data in direct service of a consumer request. However, under a strict data minimization regime, such notice would simply be limited to ensuring that consumers understand when sensitive data is operationally necessary; companies will still be fundamentally constrained to only use this data to respond to a consumer request or for one of a narrow set of permitted business purposes.

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

[7] FTC v Kochava, Inc., Complaint for Permanent Injunction and Other Relief, (August 2022) https://www.ftc.gov/system/files/ftc_gov/pdf/1.%20Complaint.pdf

[8] FTC v Vizio and Vizio Inscape, Complaint for Permanent Injunction and Other Equitable and Monetary Relief, (February 2017) https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf

[9] For example, in relation to health information, Virginia’s Consumer Data Protection Act only includes “mental or physical health diagnosis” in its definition of sensitive personal information, leaving reproductive health information uncovered. Code of Virginia, Chapter 53, § 59.1-575, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

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?

Many stakeholders involved in the commercial surveillance economy attempt to downplay the harms associated with privacy invasions, including by imagining that the harms of their business model only apply to the smallest possible unit — the individual — and are only worth addressing when the individual demonstrates a financial loss associated with the invasion. The judiciary has largely acquiesced to this line of argumentation.[10] However we have advised the FTC to recognize that unwanted observation, through excessive data collection and use, is harmful in and of itself.[11] That applies both on the individual level, as well as collectively.

One of the most notable privacy invasions of recent memory was the Cambridge Analytica scandal, where the harm extended far beyond those Facebook users and their contacts whose information was harvested without their knowledge. The scandal brought unprecedented attention to the use of microtargeting in elections, foreign influence, and the privacy practices of social media companies. In many ways, Cambridge Analytica contributed to a growing distrust of the electoral process that continues to this day.

Even when a privacy breach doesn't result in an easily observable harm to the public, the inchoately realized dislike of being observed has a chilling effect on public participation and free expression. This has an especially important effect on populations that have been historically marginalized and/or surveilled. Vulnerable communities may feel especially constrained from experimenting with new ideas or adopting controversial positions. In fact, this constant threat of surveillance was the fundamental conceit behind the development of the Panopticon prison: if inmates had to worry all the time that they were being observed, they would be less likely to engage in problematic behaviors.[12] Unfortunately, we see the same principle applied to minority communities in the policing context in the United States, often to deleterious effects on civic engagement.[13]

[10] Ryan Calo, Privacy Harm Exceptionalism, 12 COLO.TECH.L.J. 361, 361 (2014); see also Ryan Calo, Privacy Law's Indeterminacy, 20 THEORETICAL INQUIRIES L. 33, 48 (2019) ("[C]ourts . . . do not understand privacy loss as a cognizable injury, even as they recognize ephemeral harms in other contexts.").

[11] Consumer Reports, Comments on the Federal Trade Commission's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security, (November 21, 2022) https://advocacy.consumerreports.org/wp-content/uploads/2022/11/CR-comments-on-FTC-privacy-ANPRM-combined-2.pdf

[12] Michel Foucault, Discipline and Punish: The Birth of the Prison (1977).

[13] Josh Hendrix et al., The Eyes of Law Enforcement in the New Panopticon: Police-Community Racial Asymmetry and the Use of Surveillance Technology. Surveillance & Society 16(1): 53-68 (2018). https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

The United States was founded on a tradition of anonymous speech. In order to remain a vibrant and innovative society, citizens need room for the expression of controversial — and occasionally wrong — ideas without worry that the ideas will be attributable to them in perpetuity. In a world where increasingly every action is monitored, stored, and analyzed, people have a substantial interest in finding some way to preserve a zone of personal privacy that cannot be observed by others.

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?

While there is a compelling public interest in keeping some types of information publicly available (such as land title records), we do not believe that interest extends to an individual's entire digital footprint. Consumer Reports generally advocates for a stricter definition of "publicly accessible information" than is contained in many state privacy proposals, some of which include "information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information", such as social media posts.[14] For reference, Consumer Reports' Model State Privacy Act defines publicly available information as information that is "lawfully made available from federal, state, or local government records."[15]

f. What is the interplay between privacy harms and other harms that can result from automated decision-making, such as discriminatory or arbitrary outcomes? How should these two issues be understood in relation to one another in the context of equity and civil rights concerns?

In many cases, automated decisionmaking systems, which rely on large stores of data to run, exist on top of a foundation of improperly sourced data. Consumers who did not have the right to object to their personal data being used to train an algorithm are now being evaluated by that same algorithm. Recent settlements at the FTC that use the "algorithmic disgorgement" remedy imply that the Commission is coming to a similar understanding.[16] That improper collection and subsequent usage should be thought of as a civil rights concern of its own, and one that can potentially be addressed through the framework of traditional privacy legislation - such as with strong data minimization requirements, a right to delete, and a right to object to processing.

The outcomes of automated decisionmaking systems also raise civil rights concerns when they are arbitrary or discriminatory, which may call for solutions that divert from traditional privacy law. Consumer Reports' Model State Privacy Act addresses civil rights by including sections

[14] Virginia Code § 59.1-575. https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

[15] Consumer Reports, Model State Privacy Act, (Feb. 2021), § 3 (p)(2), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pd

[16] U.S. v. Kurbo, Inc., and WW International, Inc., Stipulated Order for Permanent Injunction, (March 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/wwkurbostipulatedorder.pdf

prohibiting discrimination in economic opportunities and discrimination in public accommodations under a traditional disparate impact rubric:

> **Discrimination in economic opportunities.**
>
> (a) It is unlawful to process information for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for housing, employment, credit, or insurance, in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of a person or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.
>
> (b) The unlawful processing of personal information based on disparate impact is established under this subsection only if:
>
> (1) A complaining party demonstrates that the processing of personal information causes a disparate impact on the basis of a protected characteristic; and
>
> (2) The respondent fails to demonstrate that the challenged processing of information is necessary to achieve one or more substantial, legitimate, nondiscriminatory interests; or
>
> (3) The complaining party shows that an alternative policy or practice could serve such interests with a less discriminatory effect.
>
> (c) With respect to demonstrating that a particular processing of personal information causes a disparate impact as described in paragraph (a), the complaining party shall demonstrate that any particular challenged component of the processing of personal information causes a disparate impact, except that if the components of the respondent's processing of personal information are not reasonably capable of separation for analysis, the processing of personal information may be analyzed as a whole. Machine learning algorithms are presumed to be not capable of separation for analysis unless respondent proves otherwise by a preponderance of the evidence.
>
> **Discrimination in public accommodations.**
>
> (a) It is unlawful to process personal information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a person or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, or disability.
>
> (b) The standards for disparate impact cases stated in Section 126(b)-(c) shall apply to disparate impact cases with respect to this paragraph.
>
> (c) It is unlawful for any person to:
>
> (1) Withhold, deny, deprive, or attempt to withhold, deny, or deprive, any person of any right or privilege secured by this paragraph;

> (2) Intimidate, threaten, coerce, or attempt to intimidate, threaten, or coerce, any person with the purpose of interfering with any right or privilege secured by this paragraph; or
> (3) Punish or attempt to punish any person for exercising or attempting to exercise any right or privilege secured by this paragraph.[17]

The American Data Privacy Protection Act (ADPPA), which overwhelmingly passed the House Energy and Commerce Committee on a 53-2 bipartisan vote, also included strong civil rights language.[18]

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

Commercial surveillance and processing practices may indeed produce discriminatory outcomes without that being the intention of programmers. For example, the segmentation of consumers into groups for the purposes of targeted advertising may not be explicitly based on protected characteristics such as race and gender identity, though companies may (intentionally or inadvertently) use proxies for these factors that result in unfair treatment. The civil rights language included in Consumer Reports' Model State Privacy Act (see *supra,* Question 1(f)) resolves this issue (at least in part) by honing in on disparate impact, meaning complainants would not need to prove intentional guidance of a programmer to assert a harm. Similarly, Section 5 of the FTC Act and its prohibition on unfair or deceptive acts or practices is not contingent on intentionality. Section 207 (civil rights) of the ADPPA also does not rest on an intentionality provision.

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

[17] Consumer Reports, Model State Privacy Act, (Feb. 2021), §§ 3-126, 3-127, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pd

[18] See Section 207, Amendment in the Nature of a Substitute to the American Data Privacy and Protection Act, https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf

people; people whose primary language is not English; children and adolescents; students; low-income people; people who receive public benefits; unhoused people; sex workers, hourly workers, "gig" or contract workers, and other kinds of workers; or other individuals or communities who are vulnerable to exploitation, or have historically been subjected to discrimination?

b. In what ways do the specific circumstances of people with disabilities—such as the obligation to supply personal information to obtain public benefits or reasonable accommodations, the use of assistive technologies, or the incompatibility of digital services with a disability—create particular privacy interests or risks?

c. How do specific data collection and use practices potentially create or reinforce discriminatory obstacles for marginalized groups regarding access to key opportunities, such as employment, housing, education, healthcare, and access to credit?

There are many, many examples of commercial surveillance and processing practices negatively impacting vulnerable populations and communities historically subjected to discrimination. For example, the Department of Housing and Urban Development has charged Facebook for targeting housing advertisements based on protected categories like race and religion.[19] These targeting systems have also been used to interfere with elections and fuel voter suppression efforts and to carry out disinformation campaigns that undermine public trust.[20] Further, some data brokers provide this information to employers, landlords, and others, while evading the Fair Credit Reporting Act, giving consumers next to no control over these uses.[21] The increasing use of automated decision-making can further exacerbate these problems, as opaque algorithms, often trained on historical data, can perpetuate existing inequalities.[22]

In one recent example, Consumer Reports uncovered evidence that auto insurers were engaging in discriminatory pricing schemes based on educational attainment and employment

[19] Sec'y of Hous. & Urban Dev. v. Facebook, Inc., No 01-18-0323-8, 1, Charge of Discrimination, FHEO No. 01- 18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

[20] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Fed. Trade Comm'n (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billionpenalty-sweeping-new-privacy-restrictions.

[21] Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA, Fed. Trade Comm'n (June 12, 2012), https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-chargescompany-allegedly-marketed; Big Data, A Big Disappointment for Scoring Consumer Credit Risk, Nat'l Consumer Law Ctr. at 26 (Mar. 2014), https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf

[22] See Erin Simpson & Adam Conner, How to Regulate Tech: A Technology Policy Framework for Online Services, Ctr. for Am. Progress (Nov. 16, 2021) (discussing the extensive literature on civil rights harms caused by automated decision-making systems, biometric surveillance, amplification of civil-rights suppressing content, and reification of prejudice), https://www.americanprogress.org/article/how-toregulate-tech-a-technology-policy-framework-for-online-services/.

data they had collected from consumers.[23] These factors disproportionately penalize drivers of color and working-class people, often costing them hundreds of dollars per year.

Consumer Reports has also written about the use of race as a variable in medical algorithms, which can determine eligibility for critical services, such as risky treatments or organ transplants.[24] One paper found that Black patients were assigned lower-risk scores than white patients, even when they were equally sick; the algorithm used data about patients' historical healthcare costs to make decisions, and Black patients were routinely spent less on, which the scientists speculated is due to systemic barriers to healthcare access.[25] While many hospitals have dropped race as a consideration in medical algorithms, citing a lack of evidence, many still use them, often without the patient knowing their race was a consideration in the clinical decisionmaking process.[26]

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?

<u>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?</u>

Algorithms are increasingly used to supplement or replace human decisionmaking, and in some cases they are touted as being more objective and thorough than a human decisionmaker.[27] However, an algorithm is only as good as the engineer who designs it and the data it is trained on—human error, including biased data collection methods and the type of algorithm that is chosen by the engineer, can also cause bias. No algorithm will ever be perfect, because a model is a simplified version of real-world events. Most algorithms make mistakes — or are

[23] Chuck Bell, CR investigates how auto insurers are using drivers' education and occupation to set premiums, (January 28, 2021) https://advocacy.consumerreports.org/research/report-effects-of-varying-education-level-and-job-status-on-online-auto-insurance-price-quotes/

[24]Kaveh Waddell, Medical Algorithms Have a Race Problem, Consumer Reports, (September 18, 2020), https://www.consumerreports.org/medical-tests/medical-algorithms-have-a-race-problem/

[25] Heidi Ledford, "Millions Affected by Racial Bias in Health-Care Algorithm," Nature 574 (October 31, 2019): 608-609, https://media.nature.com/original/magazine-assets/d41586-019-03228-6/d41586-019-03228-6.pdf.

[26]Kaveh Waddell, Medical Algorithms Have a Race Problem, Consumer Reports, (September 18, 2020), https://www.consumerreports.org/medical-tests/medical-algorithms-have-a-race-problem/

[27] Rebecca Heilweil, "Artificial intelligence will help determine if you get your next job," Vox, (December 12, 2019), https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen; Sendhil Mullainathan, "Biased Algorithms Are Easier to Fix Than Biased People," The New York Times, (December 6, 2019), https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html.

more accurate on certain groups than others[28] — due to these errors during the design process. This can cause real harm when the algorithm is used by a government, school, workplace, or even a landlord.[29]

In the employment context, some AI companies are developing algorithms that are intended to help human resources departments narrow down job applicants or monitor/encourage productivity in the workplace. Companies like HireVue have been criticized for incorporating facial and other analysis into their video interviewing software which monitors the applicant's expressions, their tone of voice, perceived traits like "enthusiasm," eye contact, and their word choice. After much pushback from civil rights groups including an official complaint to the FTC from the Electronic Privacy Information Center, the company discontinued their facial analysis component of their software. HireVue is not the only company using biometrics to assess job applicants; other companies like Interviewer.AI and MyInterview assess candidates' faces, body language, and/or voices and rank candidates perceived characteristics like "sociability," "humility," and "positive attitude."

In another use-case, landlords have used automated tenant screening reports (which include an algorithmically generated score) to make determinations about potential tenants.[30] In the criminal justice system, risk assessments have been used to, among other things, quantify a defendant's future risk of misconduct to determine whether they should be incarcerated before their trial.[31]

Companies like these are typically not required to disclose how their algorithms work, how they trained them, what issues they identified with their technology, and what steps they took to mitigate harm.[32] Furthermore, people usually do not know how the algorithm works on others, so it could be difficult for them to even identify whether they were discriminated against (for example, a woman who is rejected for a job by a resume-screening algorithm may not know that it allowed a man of similar experience to pass through).

(See supra Question 2(c) above for examples of data processing harms related to the provision of housing and insurance.)

[28] The National Institute of Standards and Technology found that certain facial recognition algorithms were more likely to misidentify Asian and African American faces relative to Caucasians. "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," National Institute of Standards and Technology: News, (December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[29] There are entire books written about these issues, such as Weapons of Math Destruction by Cathy O'Neil (Crown Publishing Group, 2016) and Race After Technology by Ruha Benjamin (Polity, 2019).

[30] Kaveh Waddell, "How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times," Consumer Reports, (March 11, 2021), https://www.consumerreports.org/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-toughtimes-a2331058426.

[31] Alex Chohlas-Wood, "Understanding risk assessment instruments in criminal justice," Brookings Institution, (June 19, 2020), https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice.

[32] Hannah Bloch-Wehba, "Transparency's AI Problem," Knight First Amendment Institute at Columbia University, (June 17, 2021), https://knightcolumbia.org/content/transparencys-ai-problem.

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

As mentioned above (supra Question 3a), data processing use-cases that contribute to legal or other substantial decisionmaking typically warrant extra scrutiny. Existing regulatory frameworks and proposals in the United States that address algorithmic accountability tend to do so in cases where the algorithm contributes to decisionmaking that has a legal or similarly significant effect, such as provision of credit, employment, housing, or educational opportunities. Justifications for such proposals tend to reveal a concern with a lack of transparency and human accountability commensurate with the magnitude of the decisions being made.

Rather than focus on specific technologies or classes of technologies, Consumer Reports' Model State Privacy Act focuses on discrimination through data processing that contributes to provision of public accommodations and economic opportunities.[33]

Biometrics, for a combination of reasons involving both the underlying data being collected (which are both unique to a person and, in many cases, immutable) and the questionable technologies utilizing them, also present a particularly risky use-case. Companies designing AI-powered tools exploit biometric features including faceprints, retina eye scans, or an individual's gait or gestures in order to attempt to predict certain characteristics about the individual. At worst, some of these technologies revive pseudoscientific racism which has been debunked many times over. These technologies can exclude people from opportunities or mark them as a threat or "high-risk" in a particular situation based on little or fraudulent evidence.[34] Unlike with a particular piece of information, individuals cannot simply “delete” their biometric information to prevent companies from using it.

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?

As mentioned above (supra Question 2(c)), educational attainment and occupation can be used as proxies for constitutionally-protected traits, resulting in economic harm to historically marginalized communities.

[33] Consumer Reports, Model State Privacy Act, (Feb. 2021), §§ 3-126, 3-127, https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pd

[34] Seth Colaner, "AI phrenology is racist nonsense, so of course it doesn't work," VentureBeat, June 12, 2020, https://venturebeat.com/business/ai-weekly-ai-phrenology-is-racist-nonsense-so-of-course-it-doesnt-work/

While some types of data are more capable of serving as proxies on their own due to historical injustices (i.e. location data), another risk that increases along with the ability of firms to process enormous data sets is the risk of businesses combining many small data points to create a profile for a person that reveals or exploits protected traits. Moreover, even when there is no intention to discriminate, black box algorithms can produce discriminatory results by replicating patterns of inequity that are already present in societal data inputs. This segmentation is often done through algorithms that are inherently difficult for external observers to test and hold accountable — especially when companies take affirmative measures to frustrate researchers testing for potential bias. For these reasons, Consumer Reports advocates for strict data minimization requirements in privacy laws, rather than attempts to identify and put enhanced guardrails around particularly risky data.

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? As the nature of discrimination and technologies that perpetuate it evolve, it is important for policymakers to be able to rely on flexible standards that proscribe discrimination in whichever form it appears. That's why we advocate for privacy laws that include language that forbids data-driven discrimination outright or using a disparate impact test (see supra Question 1(f)).

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

So long as companies retain market power and legal leeway to collect excessive amounts of consumer information with relatively little friction, the incentive to find profitable secondary uses for that information will exist (including uses unexpected or unanticipated by the consumer). That is why comprehensive privacy laws should include strict data minimization standards that with limited exceptions prevent businesses from using data for any other purpose other than to provide the service requested by the consumer (see supra Questions 1(b), 5(a) 5(e)).

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?

Market structure plays an important role in the current data ecosystem. Without policy interventions, the harms to consumers, especially those in vulnerable communities, will continue as the market is broken and will not self-correct. The current online market is dominated by giant online platforms like Facebook and Google that profit from commercial surveillance. In practice, this means that consumers have few alternatives, even when dominant firms do not appropriately weigh equity and civil rights concerns into their collection and processing activities.

This market power is persistent, not temporary. As a recent G7 communique notes:

> "There are certain common features present in many digital markets which often lead to firms gaining a large and powerful position. These features may tend to increase market concentration, raise barriers to entry, and strengthen the durability of market power. These common features include: (i) network effects; (ii) multi-sided markets; and (iii) the role of data. This can cause markets to 'tip' in favour [sic] of one or a small number of large firms."[35]

The harmful effects of this market power are widespread, as the largest online platforms operate across the digital ecosystem providing a variety of online services and connected devices. Invasive data collection is an important contributor to this market power and is also widespread as these giant online platforms can and do collect data from all the different services they provide.

In addition to collecting data directly from their own audiences and users, Google and Facebook also have an unmatched ability to collect data from third parties. The UK's CMA reports that multiple studies have found that Google tags are found on over 80% of the most popular websites, and Facebook's between 40-50% of the most popular websites. On mobile apps, Google has SDKs in over 85% of the most popular apps on the Play Store, and Facebook has again the second highest prevalence with SDKs in over 40% of the same.[36]

The unmatched advantage of the largest platforms (particularly Google and Facebook) to collect data gives them a competitive advantage in not just in personally targeted advertising but also in providing verification and attribution services to advertisers. This superior ability to provide feedback to advertisers based on their ability to collect data on how the largest variety and number of users interact with the largest variety and number of targeted ads creates a data driven cycle which helps the largest platforms maintain their dominance.

Evidence reviewed by the UK CMA suggests these capabilities to personally target advertising generate higher revenues for both online platforms and publishers compared to other less intrusive forms of advertising like contextual advertising when both are available. The potential loss of short-term revenues and the persistent dominant position and monopoly profits that platforms like Facebook and Google generate from personalized targeted advertising means the

[35] Compendium of approaches to improving competition in digital markets, G7 Germany, 12 October 2022. With contributions from Competition Bureau Canada; Autorité de la Concurrence, France; Bundeskartellamt, Germany; Autoritá Garante della Concorrenza e del Mercato, Italy; Japan Fair Trade Commission; UK Competition and Markets Authority, US - Federal Trade Commission and Department of Justice; European Commission Directorate-General for Competition; Australian Competition and Consumer Commission; Competition Commission of India; Competition Commission South Africa; and Korea Fair Trade Commission.

[36] Market Study Final Report, The role of data in digital advertising, Online platforms and digital advertising, United Kingdom Competition and Markets Authority, (Jul. 1, 2020), Appendix F, ¶ 43, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report.

incentives, in the absence of any policy intervention, are skewed to continuing commercial surveillance practices and this is the current market equilibrium we are all stuck in. There is limited scope for alternative more privacy friendly business models like subscription-based models to challenge the status quo.

4. How do existing laws and regulations address the privacy harms experienced by underserved or marginalized groups? How should such laws and regulations address these harms?

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

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

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

As mentioned above (supra Question 1(d)), non-monetary and group harms have often been ignored in privacy law and jurisprudence. Leading privacy scholars have recently attempted to expand the understanding of privacy harms, producing a typology that includes physical, economic, reputational, psychological, autonomy, discriminatory, and relationship harms, recognizing that in each category, vulnerable communities can experience a greater degree of harm.[37] In general, considerations of civil rights and equity are newer to the privacy discourse. Existing sectoral privacy laws, for example the Health Information Portability and Accountability Act (HIPAA) Privacy Rule and the Gramm-Leach-Bliley Act (GLBA), do not restrict covered entities from engaging in discriminatory data practices.

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 narrow cases where such efforts could theoretically conflict with privacy laws, such as the offering of scholarships aimed at historically disadvantaged groups. Privacy law should be written to allow for this type of discrimination designed to remedy historical wrongs. Any such provision should include robust safeguards to prevent secondary uses of information collected to mitigate historical biases.

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?

[37] Danielle Citron and Daniel Solove, “Privacy Harms,” (February 18, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222

Short of a disparate impact analysis or data leak, it can be difficult for individuals and researchers to identify or remedy wrongful algorithmically generated decisions. While consumers have rights to challenge algorithms in certain narrow use-cases, such as in the credit reporting context, usually this is not the case. In many cases, individuals may not even realize they have been subjected to algorithmic risk scoring, profiling, or decisionmaking. On the business side, a growing corpus of scholarship has found that human overseers, even when technically empowered to intervene in automated processes, often cannot do so effectively.[38] This can occur for a multitude of reasons, but perhaps most vexingly of all is the "black box" problem, where a human may technically consider the data used in the processing and have the authority to change a result once the processing occurs, but simply possesses no understanding of how the automated process arrived at the conclusion that it did. This problem plagues even the most technically-attuned humans in the loop, including engineers of the systems themselves, and will only worsen as automated processes become more sophisticated.[39]

Consumer Reports advocates for algorithms to be auditable.[40] Before we can regulate algorithms effectively, both regulators and the public need to know how they work, how they arrive at their conclusions, and to what extent they perpetuate discrimination and other harms. Mandatory, independent, and standardized third-party audits for companies whose algorithms pose significant legal effects are vital for maintaining civil rights as more processes that affect our lives become automated. This could be done by either government agencies or private companies that have been accredited through a process specified by government agencies that enforce particular laws. For example, the Department of Housing and Urban Development would need to design what an audit should look like to examine algorithms covered under the Fair Housing Act and would need to accredit private auditing companies to carry out these audits, or perform the audits internally.

In addition to laws that require companies using AI to undergo independent, rigorous third-party audits, public interest researchers can play a vital role in uncovering the harms caused by algorithmic decision-making. We've advocated for several policy solutions to make public interest auditing easier.[41]

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

[38] See, e.g., Brennan-Marquez, Kiel and Susser, Daniel and Levy, Karen, Strange Loops: Apparent versus Actual Human Involvement in Automated Decision-Making (October 2, 2019). 34 Berkeley Technology Law Journal 745–771 (2019), https://ssrn.com/abstract=3462901
[39] Will Knight, The Dark Secret at the Heart of AI, MIT Technology Review, (April 11, 2017), https://www.technologyreview.com/2017/04/11/5113/the-dark-secret-at-the-heart-of-ai/
[40] Nandita Sampath, "Opening Black Boxes: Adressing Legal Barriers to Public Interest Algorithmic Auditing," Consumer Reports, (October 2022), https://digital-lab-wp.consumerreports.org/wp-content/uploads/2022/10/CR_Algorithmic_Auditing_Final_10_2022VF2.pdf
[41] Ibid.

at all, do these laws address the privacy needs and vulnerabilities of underserved or marginalized communities?

See above (supra Question 1(f)) for discussion on the relevant civil rights language included in Consumer Reports Model State Privacy Act, as well as the ADPPA.

None of the five comprehensive privacy laws recently enacted by state legislatures contains anti-discrimination language as strong as that included in our Model State Act or ADPPA. While state laws and proposals typically ban discriminating against consumers who utilize their rights under a given bill (often leaving massive loopholes related to the provision of so-called bona-fide loyalty programs), they do not ban discrimination through data processing.

As a general point, it is useful to consider Europe's experience with the GDPR, where a combination of confusing and vague language with weak enforcement has hamstrung the law's effectiveness in meaningfully constraining unwanted data practices. United States policymakers should learn from the history of the GDPR and commit to writing clear and precise rules and backing them up with robust enforcement.

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?

See above (*supra* Questions 1(f), 4(f)) for discussion on the relevant civil rights language included in Consumer Reports Model State Privacy Act, as well as the ADPPA.

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?

See above (*supra* Question 4(d)).

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?

Aside from anti-discrimination language referenced earlier (*supra* Questions 1(f), 4(f-h)), the key principles for addressing data driven harms experienced by underserved or marginalized groups (as well as the general population) are data minimization and purpose limitation. Consumers shouldn't bear the burden of securing their own privacy, but existing privacy laws typically require consumers to either opt in or opt out of the disclosure of their data. In practice, this means consumers must contact hundreds, if not thousands, of different companies in order to fully protect their privacy. This disproportionately harms individuals who do not have the extra time or social capital necessary to navigate complicated business opt-out processes, leaving them especially vulnerable to invasions of privacy. Privacy laws should forbid data collectors from using data for purposes other than that for which was specifically requested by the consumer.

While many state proposals nod toward data minimization, they often only limit data processing to any purpose listed by a company in its privacy policy — instead of to what is reasonably necessary to fulfill a transaction — which means that companies can include an exhaustive list of processing purposes and essentially do whatever they want with the data. None of the five current comprehensive state privacy laws include a true data minimization provision.[42] At the federal level, Section 101 of ADPPA does include a strong data minimization provision.[43]

We also recommend that any data minimization provision include the principle of non-retaliation: such laws should prohibit businesses from providing differential treatment to consumers who opt out of or do not consent to targeted offers, or the sale of information about customer habits to third-party data brokers. Consumers will be less likely to exercise their privacy rights if businesses charge them for doing so. Charging consumers for privacy would also have a disparate impact on the economically disadvantaged and members of protected classes who may not be able to afford the luxury of paying for fundamental privacy rights.

Many comprehensive state privacy proposals include such language, though they often leave significant loopholes for businesses to discriminate against consumers when the business offers a loyalty program. Section 104 of ADPPA also includes non-discrimination language[44], though Consumer Reports has noted that it could be improved to clearly prohibit differential pricing and differential treatment, rather than just denial of service.[45]

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?

[42] See, e.g., Virginia Consumer Data Protection Act, Virginia Code § 59.1-578 (A)(1), https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

[43] Section 101, Amendment in the Nature of a Substitute to the American Data Privacy and Protection Act, https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf

[44] Ibid, Section 104.

[45] Consumer Reports, Letter on the American Data Privacy and Protection Act, page 4, (July 17, 2022) https://advocacy.consumerreports.org/wp-content/uploads/2022/07/CR-letter-to-EC-re-ADPPA-AINS.pdf

In general, we support broad privacy protections that apply to all. For example, we've advised the FTC against issuing children- or teen-specific rules through their rulemaking proceeding.[46] First, there is already an existing framework for childrens' data collection and surveillance advertising — the Children's Online Privacy Protection Act. That law was passed in 1998 and postdates Section 5 of the FTC Act by fifty years. Enacting sector-specific rules through Section 5 on an area where Congress has subsequently legislated invites legal challenge as to whether the FTC retains the authority to issue such rules.

Perhaps more importantly, age-specific privacy protections create their own privacy issues, as determining whether or not a particular consumer is a child or not is intrinsically privacy-invasive. For example, the recently enacted Age Appropriate Design Code in California has been criticized for raising the prospect that companies will feel compelled to collect additional data or even authenticate all users in order to determine whether the law's protections apply.

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

The differing needs of different populations as they age provides a good example of why we advocate for strong and broad privacy rules. It is a difficult, and perhaps even impossible, challenge for policymakers to craft age cutoffs that appropriately scope protections and perfectly match the needs of a given age cohort. Among both minors and the elderly, sophistication and ability to navigate the digital ecosystem differ widely. Policymakers should sidestep this issue by applying strong protections to all.

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?

See above (*supra* Questions 1(c), 2(e), 5(a)) for comments on purpose limitation and data minimization. To supplement data minimization, privacy laws should ensure that any data that is collected is only retained for the minimum amount of time necessary to fulfill the requested service and automatically deleted after that time

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

[46] Consumer Reports, Comments on the Federal Trade Commission's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security, (November 21, 2022) https://advocacy.consumerreports.org/wp-content/uploads/2022/11/CR-comments-on-FTC-privacy-ANPRM-combined-2.pdf

The single most impactful action federal agencies can take to reign in harmful data collection and processing practices is to support the FTC's Commercial Surveillance and Data Security rulemaking. We've argued for the Commission to promulgate a number of separate rules through this process:

- Data Minimization Rule: Companies should be required to limit data collection, use, retention, and sharing to what is reasonably necessary to provide a service or conduct an activity that a consumer has requested, with limited additional permitted operational uses. This Rule should also include the principle of Non-Retaliation — that companies should not be allowed to discriminate or offer differential treatment to consumers who do not agree to unrelated data processing activities.
    - Alternatively, companies should be required to offer consumers the ability to opt out of most secondary uses and data sharing, including through universal opt-out mechanisms such as platform-level signals. These opt-out rights should also be subject to Non-Retaliation obligations — companies cannot discriminate against users who opt out of secondary data processing and sharing.
- Data Security Rule: Companies should be required to implement and maintain reasonable security procedures and practices to safeguard personal information.
- Nondiscrimination Rule: Companies should be prohibited from discriminating against protected classes such as race, religion, gender identity, and sexuality in the provision of economic opportunities and public accommodations. This rule should be supplemented by rules specifically for automated data processing, such as a requirement for substantiation, explainability, and in some cases third-party auditing.
- Access, Correction, Portability, and Deletion Rule: Companies should offer consumers the right to access, correct, move, and delete their data with limited exceptions.
- Transparency Rule: Companies should provide standardized and simple instructions to users on how to take advantage of new legal rights, and large companies should be required to provide detailed information about data processing practices to provide for external accountability.

Additional details can be found in our comments to the FTC.[47]

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

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

[47] Consumer Reports, Comments on the Federal Trade Commission's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security, (November 21, 2022) https://advocacy.consumerreports.org/wp-content/uploads/2022/11/CR-comments-on-FTC-privacy-ANPRM-combined-2.pdf

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

c. What roles should third-party audits and transparency reporting play in public policy responses to harmful data collection and processing, particularly in alleviating harms that are predominantly or disproportionately experienced by marginalized communities? What priorities and constraints should such mechanisms be guided by? What are the limitations of those mechanisms? What are some concrete examples that can demonstrate their efficacy or limits?

See above for our thoughts (*supra* Question 4(e)) on third-party audits in the algorithmic decisionmaking space. We've also called for the FTC to issue a transparency rule through its Commercial Surveillance rulemaking.[48]

Without clear mandates, it is unlikely that companies will be sufficiently forthcoming about their data processing practices. Since 2004, California has required that companies publish privacy policies; however that law did not provide details about what information needs to be presented in such a policy.[49] On the other hand, regulators' enforcement of prohibitions on deceptive business practices penalizes companies for making inaccurate statements about data processing in such a policy. As a result, privacy policies have evolved to be nebulous and evasive documents, providing legal cover for current and future business practices while offering insufficient concrete information about what companies are actually doing with data. The FTC should implement a Transparency Rule to provide for clear transparency and disclosure requirements — at least for the largest and most sophisticated companies — to ensure that their data processing activities accords with the Data Minimization and other Rules that are promulgated. Smaller companies' obligations would be limited to providing clear instructions on how to take advantage of new privacy rights.

Without a dramatic expansion of relevant agency staff (see i*nfra* Question 6(f)), the regulators will have difficulty policing the accuracy and sufficiency of privacy policies — even if such a requirement is limited to the largest companies.[50] However, by mandating such transparency, journalists, advocates, researchers, and other regulators can play a role in evaluating this documentation and holding companies to account.

See *supra* Question 1(b) for further thoughts on the role of transparency.

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

[48] Ibid.

[49] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22575.

[50] E.g., Letter from Consumer Reports to Honorable Rosa L. DeLauro et al., (May 25, 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR-letter-on-FTC-appropriations-052521.pdf

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

Manipulative design choices subvert consumer choice and autonomy, reducing their ability to resist commercial surveillance practices. In response to GDPR and the ePrivacy Directive, many companies have resorted to cookie consent interfaces that strongly steer users to granting blanket consent to tracking and that make turning off certain tracking considerably more difficult. While the approaches otherwise outlined in these comments are designed to minimize the role of consent and user choice, there is no way to wholly remove individual autonomy from any privacy framework — not should there be. If secondary uses are prohibited, a company may make a pitch for using data for a different primary purpose. If a user globally opts out, a company may be able to ask for an exception. Guardrails must be implemented to ensure that such prompts do not overwhelm or confuse users as an end run around the protections of storing data minimization. For example, Consumer Reports has previously argued that consent prompts should: be separate from any privacy policy, license policy, or other longform contract, offer symmetry of choice, limit repeated requests, avoid interfaces and dialogues that subvert consumer autonomy, and give conspicuous notice of opt-out/opt-in state.[51]

There is increased precedent on the state level for prohibitions on the use of dark patterns — a prohibition in the CCPA regulations on the use of dark patterns in opt outs;[52] a prohibition in CCPA as amended by Proposition 24, on the use of dark patterns in obtaining consent to opt back into the disclosure of their information,[53] in the Colorado Privacy Act,[54] and in California's new Genetic Information Privacy Act.[55] The measures use similar language, prohibiting interfaces or processes designed with the substantial effect of subverting or impairing user choice. While this is an important first step, to be effective future policy would likely need to be more prescriptive, specifying how privacy disclosures and user interfaces should look. There may be some cost to innovation, but standardization and narrower options would better serve consumers in the long run.

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?

As is evidenced by the prevalence of unwanted data collection and processing practices described above, existing legal frameworks and self-regulatory efforts have been insufficient to

[51] Consumer Reports, Comments of Consumer Reports in Response to the Colorado Attorney General's Office Request for Comments Pursuant to Proposed Rulemaking under the Colorado Privacy Act, (August 5, 2022) https://advocacy.consumerreports.org/wp-content/uploads/2022/08/Colorado-rulemaking-input-summer-2022.pdf

[52] Cal. Code Regs tit. 11 § 999.315(h)

[53] Cal. Civ. Code §1798.140(h)

[54] CO S. 21-190 (2021) § 6-1-1303(5)(c), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.

[55] CA SB 41 (2021) § 2(b)(6), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220SB41.

address the core privacy issues. In our view, the definitive response should be in law, as there is a direct conflict between businesses' incentives to collect data and the consumer interest in preserving their personal privacy.

In one telling contribution, some of the largest data collectors have attempted to influence comprehensive state privacy laws to enable continuation of the status quo, including by directly drafting weak legislation subsequently pushed to amenable legislators.[56] The explicit aim of these efforts is to preempt stronger proposals and create a low baseline that other states could then adopt as model legislation.

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

Congress needs to fund such federal agencies accordingly so that they can keep pace with technology and compete with dominant tech firms that can pay generous salaries that lure experts away from the public sector. Some of the key agencies responsible for enforcing our existing consumer protection laws lag in manpower behind the growth and sophistication in technology. For example, the FTC currently employs fewer people than it did in 1979.[57]

We've previously called on Congress to increase funding for the FTC, which is especially important because it will enable the Commission to protect people of color and low-income communities from identity theft, fraud, scams, and exploitation.[58]

****
We thank the National Telecommunications and Information Administration for its consideration of these points, and for its work to secure strong privacy protections for consumers. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Matt Schwartz (matt.schwartz@consumer.org) or Justin Brookman (justin.brookman@consumer.org) for more information.

[56] Todd Feathers and Alfred Ng, "Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at a Time," the Markup, (May 26, 2022), https://themarkup.org/privacy/2022/05/26/tech-industry-groups-are-watering-down-attempts-at-privacy-regulation-one-state-at-a-time

[57] Federal Trade Commission, FY 2023 Congressional Budget Justification, (March 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P859900FY23CBJ.pdf

[58] Consumer Reports, Group Letter in Support of FTC Privacy Funding, (September 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/09/Group-letter-in-support-of-FTC-privacy-funding.pdf