March 6, 2023

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Via electronic filing

Re: Access Now's Submission to NTIA's Privacy, Equity, and Civil Rights Request for Comment Docket No. 230103-0001

Access Now appreciates the opportunity to submit comments to the National Telecommunications and Information Administration's ("NTIA") request for comments ("RFC") addressing issues at the intersection of privacy, equity, and civil rights. We welcome the leadership demonstrated by the NTIA to advance the ongoing policy conversation on alleviating the privacy harms suffered by marginalized communities online. The NTIA's focus on civil rights is crucial as it prepares its report. By focusing on civil rights, the NTIA can ensure that data protection and privacy regulations do not inadvertently lead to discrimination and that all individuals have equal access to the benefits of telecommunications technology. Below we provide general comments on the structure and framing that we believe will better serve NTIA's goals and intent. We then respond to specific questions posed by the RFC.

About Access Now

Access Now is an international organization that defends and extends the digital rights of people and communities at risk worldwide. By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights.[1] As part of our mission, we operate a global helpline for at-risk people to identify and mitigate specific threats to their digital security. We engage with fellow non-profit organizations and activist communities across civil society and campaign to ensure that new and emerging technologies and their investors, developers, and implementers "do no harm" first and foremost.

An example of our coalition and advocacy work includes the Ban Biometric Surveillance campaign ("BanBS"), which calls for a prohibition on using FRT and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance. The "BanBS" letter has been signed by 193 civil society organizations from 63 countries worldwide.[2] Most recently, Access Now, Immigrant Defense Project, Just Futures Law, and more than 35 human rights organizations sent a

[1] https://www.accessnow.org/.
[2] *Ban Biometric Surveillance Campaign Website*, Access Now, https://www.accessnow.org/ban-biometric-surveillance/.

letter to Amazon Web Services calling on the company to end its agreement to host the United States Department of Homeland Security's (DHS) HART database.[3]

Access Now promotes corporate transparency and accountability in technology and has done so for over a decade. In 2012, we called for Vodafone to release a transparency report and commended its groundbreaking disclosures upon its release.[4] We also maintain the Transparency Reporting Index, a one-stop shop for information on the latest corporate transparency reports.[5] We joined a coalition of organizations, advocates, and academics to create and update the Santa Clara Principles on transparency and accountability around content moderation. Most recently, and in light of the increasingly important role social media companies play during crises, Access Now and partner organizations have released a Declaration of Principles for content and platform governance in times of crisis.[6]

General Observations

Privacy is about more than just consumers. The RFC frequently mentions the concept of "consumer privacy." However, data protection and privacy protections must extend far beyond consumers. Today, many online tools and services are not "goods" in the traditional sense, in that people do not pay to use them or receive a concrete, tangible product. Instead, entities monetize personal information. Such use of data often happens with or without an individual's knowledge and often with the individual unable to use the service otherwise. The privacy implications are heightened when the data is the sole product.

For example, people using social media services are probably not "consumers" within the traditional definition due to the platforms' attenuated relationship with individuals, their role in collecting and using personal data from across the internet, and the unique privacy and security concerns such platform activities raise. Nonetheless, based on the expansive collection and processing of personal information, these practices should undoubtedly be subject to data protection and privacy rules or regulations. Entities like data brokers can passively collect information from people with whom they may never interact. These companies may maintain and sell comprehensive data profiles with individuals who do not even know the company exists.

Taken in aggregate, millions of data points implicate privacy and other rights at the societal level. For example, data protection can help reduce the risk of entities using personal information to manipulate how we associate and engage in democracy. For these reasons, focusing solely on "consumers," under a traditional understanding of the term, would fail to capture the full range of privacy risks. Instead, the focus should be on the risks and rights of all people in the U.S.

---

[3] *Access Now Letter to Amazon Web Services concerning its hosting of the HART biometric* database (May 24, 2022), https://www.accessnow.org/cms/assets/uploads/2022/05/Letter-to-AWS-re-hosting-of-HART-biometric-database_24-May-2022_Final.pdf

[4] https://www.accessnow.org/telecom-giant-vodafone-releases-groundbreaking-transparency-report-that-rev/; https://archive.nytimes.com/bits.blogs.nytimes.com/2014/06/06/vodafone-reveals-direct-access-by-governments-to-customer-data/.

[5] https://www.accessnow.org/transparency-reporting-index/.

[6] https://www.accessnow.org/new-content-governance-in-crises-declaration/.

Define key terms. We encourage the NTIA to incorporate several definitions of key terms used throughout the RFC. It would greatly benefit from the inclusion of definitions for various terms such as "risk," "personal information," "accessibility," and "sensitive personal information." However, we recommend that all personal information be treated as sensitive to prevent an unnecessarily narrow approach to data protection. Moreover, while the term "consumer" is not defined, we recommend that the NTIA adopt a more inclusive definition below. The definitions in this framework should be as technology-neutral and future-proof as possible, considering the fast technological and market developments related to data protection, privacy, and telecommunications technology.

Responses to Specific Questions in the Request for Comment

- ***(1) (a) Is "privacy" the right term for discussing these issues? Is it under-inclusive? Are there more comprehensive terms or conceptual frameworks to consider?***

The right to personal data protection is closely interconnected to, but distinct from, the right to privacy. More than 160 countries refer to the right to privacy in their constitutions, but what "privacy" means varies from one nation to another based on its history, culture, or philosophical influences.[7] Thus, the way to protect privacy might differ from country to country, even if many legal traditions center the protection of privacy on the right to respect for family life, home, and correspondence, for example. Data protection, on the other hand, is sometimes but not always considered a right.

Access Now has worked on data protection legislation across the world since 2009, and, on the EU reform that led to the adoption of the General Data Protection Regulation. The EU and its member states enjoy a long data protection tradition. The EU is often considered a standard-setter in this area, and many countries are interested in replicating the GDPR in their jurisdictions. Data protection is often recognized through binding frameworks at the national, regional, and international levels. In many places where it still needs to be codified, lawmakers are in the process of doing so. This should happen quickly, especially in the US.

Data protection and privacy differ, but you cannot have one without the other.[8] Data protection refers to the mechanisms, practices, safeguards, and rules to prevent unauthorized access or misuse of data.[9] Data privacy defines who should have authorized access to the data and who should not. Another important distinction between data protection and data privacy is that data privacy controls are given to individuals, and data protection is an entity's responsibility. In short, a data privacy framework enables people to decide whether they want to share their information, who has access to it, for how long, and for what reason.

With advances in technology and its use of data in various industries, it is essential to have a data protection and privacy framework that can adapt to these changes and provide adequate protection

[7] *Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers - Lessons from the EU General Data Protection Regulation to contribute to the global discourse on data protection*, Access Now (Nov. 2018), https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf.
[8] *Id*.
[9] Estelle Masse, *Data protection: why it matters and how to protect it*, Access Now (Jan. 25, 2018), https://www.accessnow.org/data-protection-matters-protect/.

for personal data. However, a data protection framework offers a more neutral and technical approach to discussing personal data protection than a privacy framework. It helps to ensure that solutions are focused on the specific technical and legal issues involved in protecting personal data rather than being framed only in terms of personal privacy.

In conclusion, data protection and privacy are not mutually exclusive goals. Governments can adopt robust data protection frameworks that respect individuals' privacy rights while providing security and transparency around corporate and government data practices. Considering the full spectrum of issues involved in collecting, processing, storing, and using personal data, a human rights-centered data protection and privacy framework supplies a comprehensive framework for defending civil liberties.

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

Collecting and using biometric data poses significant risks to marginalized communities and deserves more scrutiny and attention.[10] According to the European Data Protection Board ("EDPB"), *"the processing of biometric data under all circumstances constitutes a serious interference in itself."*[11] The EDPB also emphasized the chilling effect these technologies can cause:

> *"it is also not inconceivable that the collection, analysis and further processing of the biometric (facial) data in question might have an effect on the way that people feel free to act even if the act would be fully within the remits of a free and open society"*[12]

Moreover, because these technologies can process people's biometric data without their knowledge, they pose a particular threat and are even more prone to causing a chilling effect:

> *"[I]t has to be considered as a matter of severity, that if the data is systematically processed without the knowledge of the data subjects, it is likely to generate a general conception of constant surveillance. This may lead to chilling effects in regard of some or all of the fundamental rights concerned."*[13]

Using biometric recognition technologies to infer emotions and gender is particularly troubling and deserves greater attention. Emotion Recognition Technology ("ERT") is being deployed worldwide and attempts to make inferences about people's emotions, moods, and personalities, often without

[10] Access Now and more than 175 civil society organizations, activists, and researchers from across the globe are calling for a ban on uses of facial recognition and remote biometric recognition that enable mass and discriminatory targeted surveillance, https://www.accessnow.org/civil-society-ban-biometric-surveillance/.
[11] *Submission to the consultation on the European Data Protection Board's guidelines 05/2022 on the use of facial recognition technology in law enforcemen*t, Access Now (Jun. 27, 2022), https://www.accessnow.org/cms/assets/uploads/2022/07/Access-Now-submission-to-the-consultation-on-the-European-Data-Protection-Boards-FRT-for-LEAs-guidelines-05_2022.pdf.
[12] *Id*.
[13] *Id*.

their consent or knowledge. From hiring,[14] to education,[15] to healthcare, and [16] to policing.[17] The encroachment of ERT on people's rights in the United States has seemingly been innocuous, with the intent of providing tailored recommendations for music or facilitating sales calls. However, when companies like Spotify and Zoom deploy these powerful tools to manipulate our feelings for profit and make biased inferences about us, we protest and call for regulation.[18] The comfort of having a song recommendation or "knowing" how an employee feels during a meeting may seem innocent. However, this technology raises serious human rights concerns that the U.S. cannot overlook.

The relationship between facial expressions and a person's emotional state is much more complex than it might appear because people express their emotions differently across cultures, ethnicities, and circumstances. Researchers from the University of Glasgow found that culture shapes the perception of emotions.[19] Facial expressions are filtered through culture to gain meaning, and our culture and societal attitudes fundamentally shape our emotions.[20] Facial expressions are not accurate indicators of genuine emotions because people often mask or suppress them.[21] Research also shows that some emotion recognition technology fails to identify the emotions of darker-skinned faces. In one study, emotion recognition systems assigned more negative emotions to Black men's

---

[14] Douglas Perry*, Emotion-recognition technology doesn't work, but hiring professionals, others are using it anyway: report*, The Oregonian (Dec. 16, 2019), https://www.oregonlive.com/business/2019/12/emotion-recognition-technology-doesnt-work-but-hiring-professionals-others-are-using-it-anyway-report.html; Minda Zetlin, *AI Is Now Analyzing Candidates' Facial Expressions During Video Job Interviews*, Inc. Magazine, https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html.

[15] Michael Standaert*, Smile for the camera: the dark side of China's emotion-recognition tech*, The Guardian (Mar. 3, 2019), https://www.theguardian.com/global-development/2021/mar/03/china-positive-energy-emotion-surveillance-recognition-tech.

[16] Marwan Dhuheir, et. al., *Emotion Recognition for Healthcare Surveillance Systems Using Neural Networks: A Survey*, Cornell University (Jul.13, 2021), https://arxiv.org/abs/2107.05989.

[17] Ismat Ara*, Lucknow Police to Use AI Cameras to Track Women's Distress, Activists Slam Privacy Invasion*, The Wire (Jan. 22, 2021), https://thewire.in/women/uttar-pradesh-lucknow-police-artificial-intelligence-camera-women; Alex Engler, *Why President Biden should ban affective computing in federal law enforcemen*t, The Brookings Institution (Aug. 4, 2021), https://www.brookings.edu/blog/techtank/2021/08/04/why-president-biden-should-ban-affective-computing-in-federal-law-enforcement/.

[18] *Dear Spotify: don't manipulate our emotions for profit*, Access Now (Apr. 15, 2021), https://www.accessnow.org/spotify-tech-emotion-manipulation/; see also *27 Rights Groups Demand Zoom Abandon 'Invasive,' and 'Inherently Biased' Emotion Recognition Software*, Gizmodo (May 11, 2022), https://gizmodo.com/zoom-emotion-recognition-software-fight-for-the-futur-1848911353.

[19] Chaona Chen, et.al., *Distinct Facial Expressions Represent Pain and Pleasure Across Cultures*, Proceedings of the National Academy of Sciences of the United States of America, vol. 115, no. 43, 2018, pp. E10013–E10021, https:// www.pnas.org/content/115/43/E10013.

[20] Michael Price, *Facial Expressions – Including Fear – May Not Be As Universal As We Thought*, Science (Oct. 17, 2016),https://www.science.org/content/article/facial-expressions-including-fear-may-not-be-universal-we-thought; Carlos Crivelli, et al., *The Fear Gasping Face as a Thread Display in a Melanesian Society*, Proceedings of the National Academy of Sciences of the United States of America (Oct. 17, 2016) ,https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5098662/.

[21] Miho Iwasaki and Yasuki Noguchi, *Hiding true emotions: Micro-expressions in eyes retrospectively concealed by mouth movements*, Scientific Reports (Feb. 26, 2016), https://www.nature.com/articles/srep22049.

faces when compared to white men's faces. These systems read Black men's faces as angrier than white men's, no matter their expression.[22]

Using emotion recognition systems in education could further exacerbate existing oppressive dynamics. For instance, it is common knowledge that Black students experience more suspensions and other disciplinary actions than white students, often for the same behavior.[23] Another study exploring the racialized perception of emotions and bias among prospective teachers concluded that the teachers are more likely to interpret Black boys' and girls' facial expressions as angry, even when they are not.[24] If companies deploy racially biased emotion recognition technology in these problematic situations, existing inequalities and oppression could be magnified.

Moreover, according to the UN, "the use of emotion recognition systems by public authorities, for instance, for singling out individuals for police stops or arrests or to assess the veracity of statements during interrogations, risks undermining human rights, such as the rights to privacy, to liberty and a fair trial." We support the conclusion of the UN High Commissioner for Human Rights that a "risk-proportionate approach to legislation and regulation will require the prohibition of certain A.I. technologies, applications or use cases, where they would create potential or actual impacts that are not justified under international human rights law, including those that fail the necessity and proportionality tests."[25]

In their Joint Opinion on the European Union's Artificial Intelligence Act, the EDPB and European Data Protection Supervisor (EDPS) states that the "use of A.I. to infer emotions of a natural person is highly undesirable and should be prohibited."[26] While the EDPB-EDPS statement further notes that exceptions should be made for "certain well-specified use-cases, namely for health or research purposes," the fact that these systems are based on flawed scientific premises suggests that they should not be allowed in sensitive domains such as health.[27]

Similarly, Automatic Gender Recognition (AGR) claims to infer the gender of individuals from data collected about them. AGR uses information, like a legal name or the bone structure of your face, to infer your gender identity, often reducing it to a simplistic binary.[28] Automated recognition of gender

---

[22] Lauren Rhue, *Emotion-reading tech fails the racial bias test*, The Conversation (Jan. 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404.

[23] Travis Riddle and Stacey Sinclair, *Racial disparities in school-based disciplinary actions are associated with county-level rates of racial bias*, Princeton University (Apr. 2, 2019), https://www.pnas.org/content/116/17/8255.

[24] Amy G. Halberstadt, et al., *Racialized Emotion Recognition Accuracy and Anger Bias of Children's Faces*, American Psychological Association (2020), https://www.apa.org/pubs/journals/releases/emo-emo0000756.pdf; Amy Halberstadt and Matt Shipman, *Future Teachers More Likely to View Black Children as Angry, Even When They Are Not*, NC State University (Jul. 6, 2020), https://news.ncsu.edu/2020/07/race-anger-bias-kids/.

[25] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, A/HRC/48/31, UN Human Rights Council, 48th Session (Sept. 13, 2021), https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalReports.aspx.

[26] Natasha Lomas, *EU's data protection adviser latest to call for ban on tracking ads*, TechCrunch (Nov. 19, 2021), https://techcrunch.com/2021/11/19/edpb-call-to-ban-tracking-ads/.

[27] *Id.*

[28] OS Keyes, *The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition*, Proceedings of the ACM on Human-Computer Interaction (Nov. 2018), https://ironholds.org/resources/papers/agr_paper.pdf.

and sexual orientation can cause several harms to LGBTQI+ people. You could be interrogated at the airport if the system determines you do not match the gender marker in your passport. On the same basis, a transgender person could be prohibited from access to gender-specific spaces like bathrooms and locker rooms. Authorities in repressive countries could analyze security camera footage or social media profiles to track down individuals they believe to be LGBTQI+ and arrest them.[29]

When biometric technology is used to infer gender, it limits a person's ability to self-identify.[30] It puts companies in a dangerous position of power over people using or subject to the service.[31] Spotify, for example, is incentivized to manipulate a person's emotions to encourage them to continue listening to content on its platform—which could veer towards exploitation, like playing on a person's depression to keep them depressed.[32]

For technologies that threaten the essence of our rights or are incompatible with the foundations of a democratic society, a prohibition is the only option. In January 2021, Access Now joined over 60 civil society organizations in calling for red lines on uses of AI that are incompatible with a democratic society, including the use of remote biometric identification technologies in publicly accessible spaces. Similarly, we encourage the NTIA to take a stronger stance in support of protecting biometric data.

We also urge the NTIA to prioritize attention to the adverse impacts of targeted surveillance technologies, including spyware, on the rights to privacy and data protection. While the capabilities of modern spyware, such as the invasive Pegasus product sold by NSO Group[33] go beyond facial recognition and other biometric technologies, their combination further exacerbates potential human rights violations that are unacceptable in a democratic society. Therefore, Access Now calls for a moratorium limiting the sale, transfer, export, servicing, and use of targeted surveillance technologies until people's rights are safeguarded under international human rights law. A ban is necessary when such safeguards or remedies cannot sufficiently mitigate these violations - like in the case of NSO Group's Pegasus spyware.

- ***(6)(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?***

[29] https://campaigns.allout.org/ban-AGSR.
[30] Veronica Arroyo and Daniel Leufer, *Facial recognition on trial: emotion and gender "detection" under scrutiny in a court case in Brazi*l, Access Now (Jun. 29, 2020), *https://www.accessnow.org/facial-recognition-on-trial-emotion-and-gender-detection-under-scrutiny-in-a-court-case-in-brazil/*; *Petition to Ban Automated Recognition of Gender and Sexual Orientation*, Access Now, *https://act.accessnow.org/page/79916/action/1*.
[31] *Dear Spotify: don't manipulate our emotions*, Access Now (Apr. 15, 2021) https://www.accessnow.org/spotify-tech-emotion-manipulation/.
[32] *Id*.
[33] For more information on current US litigation against spyware developer NSO Group, see Access Now, *U.S. Supreme Court rejects latest NSO Group attempt to avoid accountability*, 10 Jan 2023, available at https://www.accessnow.org/u-s-solicitor-general-and-department-of-commerce-must-hold-nso-accountable.

Transparency reporting is becoming the norm for the tech sector as it is a powerful method for entities to reveal potential risks to privacy and freedom of expression to the public. More than 40 companies have released these regular reports, which are becoming more comprehensive and global in scope, and governments, including the EU, are moving to require such disclosures.[34]

The benefits of transparency reporting include increased stakeholder trust and confidence and improved accountability and oversight. They inform the public, force companies to clarify their policies and practices, and can influence government policies and practices. Additionally, investors refer to these reports to verify that companies are fulfilling their obligation to uphold human rights. Transparency reporting can also help to identify areas where an organization may need to improve its data protection practices. By providing such reports, entities empower individuals to gain insight into their policies and measures to prevent government abuses. The reports also shed light on various practices that affect fundamental rights, such as online surveillance, internet shutdowns, and content removal.

With very few exceptions, marginalized communities have historically been unable to consistently measure the scope and scale of threats to their online privacy and freedom of expression. Government agencies usually do not report statistics on their surveillance activities, and companies are under no legal obligation to disclose or hand over data. Transparency reports have been valuable for improving basic knowledge about government surveillance, facilitating a better-informed debate on surveillance topics, and offering reassurance to individuals about what protections are in place for their private communications and data. Nevertheless, as surveillance practices evolve, so too must these efforts.

Third-party audits also provide several benefits for entities seeking to ensure compliance and maintain stakeholder trust. First, they provide an independent and objective evaluation of the entity's processes, controls, and data-handling practices. They can also help to identify any gaps or weaknesses that entities must address to improve security, privacy, and data protection. Second, third-party audits can help entities demonstrate compliance with legal, regulatory, and industry standards. Third-party audits can be critical in industries with strict data handling and protection requirements, such as healthcare or financial services.

While third-party audits and transparency reporting can provide valuable insights into an entity's data protection practices, their focus and scope differ. Third-party audits are typically more comprehensive and rigorous, focusing on ensuring compliance and identifying any areas for improvement. Transparency reporting is typically more focused on disclosing information to stakeholders and the public, intending to improve transparency and accountability. Below, we highlight a few suggested priorities and constraints surrounding transparency reports and third-party audit reporting mechanisms and examples of their efficacy and limits:

Priorities and Constraints:

Third-party audits and transparency reporting should prioritize the needs and perspectives of marginalized communities. This can be done by involving community stakeholders in designing and

[34] *Transparency Reporting Index*, Access Now, https://www.accessnow.org/transparency-reporting-index/.

implementing these mechanisms and ensuring that reports and audits are accessible and easily understood. Third-party audits and transparency reporting should also minimize the risk of re-identification of sensitive data and address the systemic issues that allow these data abuses and harms to occur. This might include analyzing Big Tech's business models and economic incentives, as well as the regulatory frameworks that enable or fail to prevent these practices.

Efficacy and Limits:

Third-party audits and transparency reports are often limited in scope, focusing on specific companies or issues which may not capture the full extent of harm. First, transparency reporting is typically voluntary, which means that entities may not disclose all relevant, complete, and accurate information or may choose only to disclose positive information. The voluntary nature also limits the usefulness of transparency reporting in identifying areas for improvement or holding entities accountable for their actions. They can also be resource-intensive and require personnel, technology, and infrastructure investment. For example, Facebook underwent a civil rights audit by a third-party auditor, which identified several areas where the company's data practices were causing harm to marginalized communities, from hate speech to advertising to algorithmic bias.[35]

The Facebook civil rights audit concludes that the company handles civil rights issues "too reactive and piecemeal."[36] The audit raises doubts about whether Facebook is committed to addressing its problems and highlights the tension between free expression and hate speech on social networks. Similarly, Google's transparency report provides data on government requests for data, content removal requests, and other issues.[37] While it identifies the harms and how governments access and use data, it does not address the underlying systemic issues that allow these practices to occur. Notably, we have seen stagnation in transparency reporting as the growth rate of companies publishing transparency reports has been decreasing persistently since 2013.[38]

Secondly, third-party audits are typically conducted at a specific time and may not capture ongoing changes in an entity's data handling practices. In other words, an entity may be compliant during the audit but fall out of compliance later. Third-party audits may also not capture emerging risks or best practices since they may be limited by compliance with legal or regulatory requirements. This can limit entities from staying ahead of evolving threats and lead to a narrow focus on compliance rather than a broader focus on data protection and risk management.

In conclusion, third-party audits and transparency reports can effectively address harmful data practices and be used as an effective tool to safeguard civil and human rights. However, entities must carefully design and implement these mechanisms to prioritize marginalized communities while balancing transparency and privacy and addressing the systemic issues underlying harmful data practices. Reporting on matters impacting human rights is necessary for businesses to realize their responsibilities. Investors, peer companies, and individuals depend on companies to respect rights

---

[35] Barbara Ortutay, *Facebook civil rights audit: 'Serious setbacks' mar progress*, AP News (Jul. 8, 2020), https://apnews.com/article/us-news-ap-top-news-politics-technology-business-94189e0798d2ca7701d5c248c2843dbe.

[36] https://about.fb.com/wp-content/uploads/2020/07/Civil-Rights-Audit-Final-Report.pdf.

[37] *Transparency Reporting Index*, Access Now, https://www.accessnow.org/transparency-reporting-index/.

[38] *Id*.

and remedy abuses, even absent regulation forcing them to do so. Silent, closed-door complicity in violations will only harm the sector in the long run - not to mention the damage to marginalized communities' trust and human rights.

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

Deceptive interface designs (or "dark patterns'') have infiltrated every online marketing and sales business model, including shopping websites, social media, mobile and video games, and mobile applications.[39] Companies are utilizing deceptive interface designs to influence human decision-making online.[40] Deceptive design choices cause real-life harm. They can significantly create or enable privacy harms, particularly disproportionately experienced by marginalized communities. For example, deceptive designs can create privacy harm if they mislead individuals about the kind of data being collected, how it is being used, and who has access to it. Deceptive designs can also disproportionately harm marginalized communities who are more likely to be targeted or discriminated against based on their data or may need more resources or knowledge to understand the full implications of using these technologies. [41]

Design choices concerning the function, accessibility, description, and other components of consumer technologies can alleviate privacy harms, particularly those disproportionately experienced by marginalized communities.[42] Entities should design their products and services with and for their most vulnerable communities. This principle means, at a minimum, providing easy-to-understand and transparent interface designs that preserve autonomy and agency. Incorporating privacy by design principles into consumer technologies can help to prevent privacy harms from occurring in the first place, rather than trying to add privacy protections as an afterthought. Design choices play a critical role in online autonomy and control over data by empowering people to make informed choices about how their data is collected, used, and shared.

- ***6 (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?***

---

[39] *The time is now for the U.S. FTC to combat dark patterns*, Access Now (Jun. 1, 2021), https://www.accessnow.org/ftc-combat-dark-patterns/ ; see also *Access Now Comments to the Federal Trade Commission on Dark Patterns* (May 28, 2021), https://www.accessnow.org/cms/assets/uploads/2021/06/Access-Now-Dark-Patterns-Comments-Final-May-28-2021.pdf.

[40] *Id.*

[41] *Id.*

[42] Sage Cheng and Willmary Escoto, *No more deceptive designs: dos and don'ts for responsible user experience practices*, Access Now (Nov. 2022), https://www.accessnow.org/cms/assets/uploads/2022/11/No-more-deceptive-designs_dos-and-donts-for-responsible-user-experience-practice-11-2022.pdf.

Industry-developed codes of conduct can be essential in public policy responses to harmful data collection and processing. They can help establish voluntary standards for responsible behavior and guide companies to minimize their negative impact on marginalized communities. Industry-developed codes can also help empower and bolster private partnerships and multi-stakeholder initiatives, bringing together civil society organizations, policymakers, researchers, and corporations to address critical concerns and develop practical solutions.

However, some limitations exist when relying solely on industry-developed codes of conduct. First and most apparent, industry-developed codes are usually voluntary and do not have the power of law. As a result, companies may not prioritize compliance over their business interests. Secondly, players with vested interests can influence industry-developed codes, which may limit their effectiveness in addressing the root causes of harm. Industry codes of conduct must also be sufficiently comprehensive or detailed to address all the complex data collection and processing issues. They should make meaningful efforts to adequately account for marginalized communities' perspectives and experiences. Accordingly, while industry-developed codes of conduct can be valuable, they should be seen as something other than a substitute for regulatory frameworks or enforcement mechanisms.

Conclusion

We appreciate the NTIA's engagement with the community and trust that this feedback will assist the agency in refining and improving its current proposal. We look forward to continuing to work with your office to promote strong data privacy standards. If you have questions, please contact me at willmary@accessnow.org.

Thank you,

Willmary Escoto, Esq.
U.S. Policy Analyst
Access Now