MOZILLA'S RESPONSE TO THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA) REQUEST FOR COMMENT ON "PRIVACY, EQUITY AND CIVIL RIGHTS"

March 6, 2023

Table of Contents

I. MOZILLA'S VISION FOR THE INTERNET

At Mozilla, privacy is at the center of our universe. We are the maker of the open-source web browser Firefox, as well as a suite of privacy and security-enhancing products. Owned by a not-for-profit foundation, Mozilla is the mission-driven technology company that advocates to keep the internet open and accessible for all. A foundational principle of Mozilla's guiding Manifesto[1] demands that individual privacy and security online must not be treated as optional. This is why privacy comes first in our products, like Enhanced Tracking Protection (ETP)[2] and our end-to-end encrypted Firefox Sync

[1] Mozilla Manifesto. https://www.mozilla.org/en-US/about/manifesto/
[2] Deckelmann, Selena. "Latest Firefox rolls out Enhanced Tracking Protection 2.0." August 4, 2020.

service[3]. Mozilla also prioritizes privacy in our public interest advocacy, calling for comprehensive privacy legislation, greater ad transparency, and robust enforcement of data privacy law and regulations around the globe – such as California's Consumer Privacy Rights Act (CPRA)[4] and the European Union's General Data Protection Regulation (GDPR).[5] The US lags behind most of the world in terms of recognizing consumer privacy and protecting people from indiscriminate data collection and use, making it all the more important that federal agencies such as the National Telecommunications and Information Administration (NTIA) engage on these issues to help fill the gaps.

The Mozilla Foundation is the movement building muscle of Mozilla that we flex to advance our vision for a healthy, open internet across the globe. We believe in a multidisciplinary approach, pooling together our global community of researchers, advocates, and technologists, to better understand and create the conditions necessary for trustworthy AI in the world. Through research like the award-winning Internet Health Report[6] and our practical consumer guide called Privacy Not Included (PNI),[7] Mozilla serves as a global, open resource to empower consumers, inform policymakers, and inspire industry best practices.

Mozilla welcomes NTIA's efforts to examine the implications of privacy, equity, and civil rights in relation to commercial data protection practices, and appreciates the opportunity to provide comments. We offer a unique perspective as a builder of privacy-preserving technology, as well as vocal advocates for improving consumer technology and tech policy to advance better options for consumers. We

---

https://blog.mozilla.org/en/products/firefox/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default/

[3] Ritter, Tom. "Privacy by Design: How we build Firefox Sync." November 13, 2018. https://hacks.mozilla.org/2018/11/firefox-sync-privacy/

[4] Mozilla. "Four key takeaways to CPRA, California's latest privacy law." Mozilla Open Policy & Advocacy Blog. November 20, 2020. https://blog.mozilla.org/netpolicy/2020/11/20/here-are-four-key-takeaways-to-cpra-californias-latest-privacy-law/

[5] Kelly, M.J. "13 things to know about the GDPR." May 23, 2018. https://blog.mozilla.org/en/products/firefox/gdpr-mozilla/

[6] Internet Health Report 2022. https://2022.internethealthreport.org/facts/

[7] Privacy Not Included. https://foundation.mozilla.org/en/privacynotincluded/

hope to serve as a thought partner to understand, promote and model what privacy, transparency, and equity can look like for consumer experiences online.

II. MOZILLA'S THINKING ON PRIVACY & DATA COLLECTION PRACTICES ONLINE

A. Current State of Commercial Data Collection Practices

The internet is powered by consumer data. While that data has brought remarkable innovation and services, it has also put internet consumers, and trust online, at substantial risk. We believe that everyone should have control over their personal data, understand how it's obtained and used, and be able to access, modify, or delete it. Additionally, we believe that consumers should be protected from particularly egregious practices (such as third party tracking) by default, both in the form of technical measures but also strong legal protections.

At Mozilla, we strive to create the tools necessary to provide consumers with insights, controls, and protection over their data with regard to our products — not only to offer consumers better privacy-preserving choices, but to influence commercial privacy practices at large. Mozilla's Lean Data Practices methodology and framework, for example, advocates for better privacy practices that strike the balance between delivering value in service and minimizing consumer data collection[8]. In practice, this means being conscious to collect only the data we need and for how long we need it, and to clearly and concisely explain what we collect, how we use it, and how we mitigate risks. This also includes engaging consumers by making privacy policies more accessible and explaining data collection through "just-in-time" notifications. We implement these practices in our own products using our Data Privacy Principles, and we support new rules around data minimization limitations on companies' collection, use, and retention of consumer data (these practices address question *5d* on approaches to data minimization and data retention and deletion practices).

[8] Soyinka, Nneka. "Practicing lean data is a journey that can start anywhere." January 26, 2022. https://blog.mozilla.org/netpolicy/2022/01/26/lean-data-practice-journey/

As a complementary strategy, Mozilla places pressure on companies to adopt these principles through campaigns and research projects like Privacy Not Included (PNI),[9] which investigates the privacy and data collection "fine print" of common smart tools and products, to educate and empower consumers on the risk[10] tradeoffs associated with a particular product or service. The above features and tools speak to question *1b* around the value that privacy controls can provide.

Question *1b* also asks about the limitations of such controls or requirements. Depending on where someone lives, they may not have rights to access, delete, or even correct data – for example, false criminal records that data brokers share about users.[11] Even when consumers have certain rights, it can be difficult for people to meaningfully understand their rights let alone how to enforce them. Often privacy policies aren't in an easily digestible format, effectively leaving people without any information or control over their privacy and data.[12] To fully honor consent, there must be transparency so that the individual consenting has a full understanding of what will happen with their data. Consent should be freely given (i.e. not mandatory), specific, informed, and unambiguous (i.e. provided through an affirmative action by the individual).

Finally, many companies unfortunately do the minimum required, leaving the majority of users across the globe without adequate protections. Even if others in industry share Mozilla's approach to privacy, those of us driving a more private internet can't alone address the risks and harms. The limitations above demonstrate that current requirements and controls require complementary solutions from regulators, both in the form of guidance but also outright prohibition of egregious practices that cause

---

[9] Tran, Nancy. "The design process behind *Privacy Not Included mental health apps." October 26, 2022. https://foundation.mozilla.org/en/blog/the-design-process-behind-privacy-not-included-mental-health-apps

[10] Mozilla. "In Post Roe v. Wade Era, Mozilla Labels 18 of 25 Popular Period and Pregnancy Tracking Tech With *Privacy Not Included Warning." August 17, 2022. https://foundation.mozilla.org/en/blog/in-post-roe-v-wade-era-mozilla-labels-18-of-25-popular-period-and-pregnancy-tracking-tech-with-privacy-not-included-warning/

[11] Wired. "Transparency Laws Let Criminal Records Become Commodities." December 23, 2021. https://www.wired.com/story/criminal-justice-transparency-law-data-brokers/

[12] Washington Post. "I tried to read all my app privacy policies. It was 1 million words." May 31, 2022. https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/

significant harm to consumer interests. With the current lack of comprehensive federal privacy legislation in the US, many consumers (particularly communities most at risk) are simply unprotected and have no way of meaningfully assessing how their data is collected, let alone used and potentially harmed in the commercial setting.[13]

III. MOZILLA'S THINKING ON EQUITY, TARGETING & AUTOMATED DECISION-MAKING SYSTEMS (ADMS)

There are two related mechanisms online today that pose substantial risk to equity and civil rights that we will highlight below: 1) sophisticated ad targeting systems and 2) automated-decision making systems. Both of these mechanisms are powered by people's data, often collected without meaningful consent, and can result in different, sometimes harmful effects across demographic groups.

A. Discriminatory Effects of Ad Targeting

Sophisticated ad targeting systems drive the internet today. The ad tech ecosystem allows advertisers to choose the targeting parameters they are most interested in, including the target's interests, behaviors, and demographics. The advertising ecosystem then marries those chosen parameters against pools of data collected about consumers to ensure that messages or content is shown only to the intended audience. This provides efficiency gains for advertisers. But the system also allows for easy segmentation of racial or demographic groups, with potential discriminatory effectives that are not well understood today. In addition, these targeting systems often incorporate automated optimization mechanisms that ensure ads are seen by the most susceptible populations and share some similarities with the automated-decision making systems (ADMS) discussed below. These optimization systems likely further exacerbate equity and discrimination concerns.

[13] Pew Research Center. "Key takeaways on Americans' views about privacy, surveillance and data-sharing." November 15, 2019. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

For example, Facebook's ad targeting system in the past allowed advertisers to target along racial lines, resulting in discriminatory targeting of jobs and housing ads in clear violation of federal red-lining law.[14] Facebook has since made this type of targeting more difficult, but it remains possible on the platforms to target based on certain proxies for race and ethnicity. Even without explicitly discriminatory targeting parameters, research has shown that Facebook's optimization system can result in messages or ads being shown to certain racial groups and not others.[15]

Facebook is perhaps the most studied ad targeting system for discriminatory effectives, particularly for jobs and housing, but the properties of that system are not unique. In fact, other major tech platforms, as well as smaller ad tech players, offer similar ad targeting systems. We should expect those other ad tech platforms to have similar problems and should expect similar discriminatory practices in other markets beyond housing and jobs.

B. Automated-decision Making Systems

Automated-decision making systems (ADMS) present a similar set of equity risks, albeit across a broader set of use cases that can include everything from facial recognition, to policing, to decisions about mortgage rates or health insurance.

To answer questions *1g, 2a, and 3b,* related to ADMS and equity, we will share our learnings on the harms associated with ADMS[16] and the challenges related to addressing such harms, leaning on Mozilla's extensive research and investigations. For example, previous research from Mozilla has shone a light on Tinder's unfair

[14] NPR. "Housing Department Slaps Facebook With Discrimination Charge." March 28, 2019. https://www.npr.org/2019/03/28/707614254/hud-slaps-facebook-with-housing-discrimination-charge
[15] The Hill. "Facebook delivers housing, employment ads based on race, gender stereotypes: study." April 4, 2019. https://thehill.com/policy/technology/437399-facebook-delivers-housing-employment-ads-based-on-race-and-gender/
[16] For examples, see the AI Incident Database for a non-exhaustive catalog of such cases: https://incidentdatabase.ai/

personalized pricing algorithms[17] as well as YouTube's ineffective user controls,[18] which demonstrate the opaque and fallible nature of an ADMS. Risks associated with automated systems can be rooted in a variety of different issues[19], all of which need to be addressed: from the data used to train and test machine learning-based systems as well as their design to the unsubstantiated capability of some systems,[20] or their very purpose and the context in which they are deployed.

Importantly, automated decision-making systems (ADMS) are often trained or "taught" using historical data sets, making them susceptible to replicating and potentially perpetuating biases found within our society — and in some cases at great scale. Even without discriminatory intent, these systems are still capable of producing disparate impact because of this training data. Research by Mozilla fellows Abeba Birhane, Deborah Raji, and others has repeatedly pointed to harmful and toxic data as well as privacy risks in datasets widely used for machine learning. For instance, they have uncovered misogynistic and racist imagery in large computer vision datasets[21] and issues of obtaining genuine consent in the construction of such datasets.

Equity harms caused by ADMS are of particularly grave consequence when deployed in critical areas and where they affect people's livelihoods, safety, or liberties — be it a rejected loan, wrongful termination of a job, or discriminatory pricing of goods and services. Additionally, certain categories of data pose greater risks when used as input for ADMS. Like other biometric information, reproductive health data[22] has

---

[17] Mozilla. "New Research: Tinder's Opaque, Unfair Pricing Algorithm Can Charge Users Up to Five-Times More For Same Service." February 8, 2022. https://foundation.mozilla.org/en/blog/new-research-tinders-opaque-unfair-pricing-algorithm-can-charge-users-up-to-five-times-more-for-same-service/

[18] Ricks, Becca and McCrosky, Jesse. "Does This Button Work? Investigating YouTube's ineffective user controls." September 2022. https://assets.mofoprod.net/network/documents/Mozilla-Report-YouTube-User-Controls.pdf

[19] See: Mozilla's "Movement Building Landscape" https://movementbuilding.mozillafoundation.org/category/ai-impacts-in-the-consumer-space-social-justice/

[20] See Narayanan, Arvind. "How to recognize AI snake oil." https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf

[21] See, for example, Birhane et al., "Multimodal datasets: misogyny, pornography, and malignant stereotypes", 2022, https://arxiv.org/pdf/2110.01963.pdf; Prabhu & Birhane, "Large Datasets: A Pyrrhic Win for Computer Vision?", 2020, https://arxiv.org/pdf/2006.16923.pdf

[22] See footnote 10.

become a particularly sensitive form of data that can be potentially criminalized following the Supreme Court's ruling in Dobbs v. Jackson. However, other types of data can be made sensitive depending on the context in which it is used. For example, real-time location data in combination with a personal identifier can provide information on an individual's whereabouts at any given moment, not only invading their privacy but fundamentally jeopardizing their safety. Additionally, facial recognition systems[23] have been documented to be ridden with racial bias, which can create significant equity concerns, for example in managing access to public or private spaces or in a law enforcement context.[24]

Companies, both those developing and those deploying ADMS, are already in a position to prevent or mitigate such harms. While neither easy nor straightforward, people across industry, academia, civil society, and the public sector have developed a range of tools and frameworks[25] that can contribute to ensure that an ADMS helps rather than harms people. Yet, the incentives for broad adoption of these are lacking. Rules that change this incentive structure and make companies price in the externalities caused by the ADMS they develop or put to use are therefore necessary.

---

[23] MozFest event. "Responding to Coded Bias: Black Women Interrogating AI." Mach 17, 2021. https://www.mozillapulse.org/entry/2142. See also Schreder, Straith. "Does facial recognition software have a racial bias problem?" IRL Podcast. February 5, 2018. https://blog.mozilla.org/en/uncategorized/irl-face-the-future/

[24] See: Hill, Kashmir. "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match." New York Times. December 29, 2020. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

[25] See: Raji. "It's Time to Develop the Tools We Need to Hold Algorithms Accountable." 2022. https://foundation.mozilla.org/en/blog/its-time-to-develop-the-tools-we-need-to-hold-algorithms-accountable/ ; For an auditing framework for the public sector, see: Reisman et. al. "Algorithmic Impact Assessments: A Practical Framework For Public Agency Accountability" April 2018. https://ainowinstitute.org/aiareport2018.pdf

IV. MOZILLA POLICY RECOMMENDATIONS

C. The Need for Transparency

Policy as a Tool to Enable Transparency

Question *5e* asks 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. A large amount of harm happens on major tech platforms outside the view of regulators and the public. These platforms offer highly sophisticated targeting tools and automated decision-making systems that allow content producers to narrowly segment their audience, tailor content accordingly, and reach people most susceptible to their messages. Each consumer has their own individualized, potentially misleading, deceptive, or discriminatory experience. This highly-personalized experience means that harm enabled by platforms through their targeting and decisioning systems is not easily identified by regulators, watchdog groups, or researchers. Because the experience is so personalized, harm can only be shown anecdotally, when a particular piece of content appears to be harmful and when the regulator is somehow made aware of that content. There is dangerously little insight into what people experience and why. This creates an asymmetry of information between those who produce harmful content and those seeking to understand it. Even when credible research can be conducted, given the necessarily limited information available, studies are often criticized as incomplete, resulting in a stalemate.[26]

Recent history has shown that major tech platforms do not have sufficient incentive to provide the necessary level of transparency and access to researchers, and that they must be required to do so.[27] Mozilla has long encouraged the strengthening of

[26] Mozilla. “Congratulations, YouTube... Now Show Your Work.” July 6, 2020. https://foundation.mozilla.org/en/blog/congratulations-youtube-now-show-your-work/
[27] Marshall Erwin. Why Facebook’s claims about the Ad Observer are wrong. Mozilla blog, August 2021. https://blog.mozilla.org/en/mozilla/news/why-facebooks-claims-about-the-ad-observer-are-wrong/

mechanisms that empower policymakers and trusted experts to have greater visibility and understanding in order to address the harmful practices that abound online today. New rules can't succeed unless experts have sufficient visibility to systematically identify violations of those rules. To address this, we need to mandate greater access to platform data (subject to strong user privacy protections), greater research tooling, and greater protections for researchers, at the federal level. In response to question *1b*, we believe transparency is a crucial prerequisite to both empowering consumers and diagnosing the potential harm and risk associated with certain data collection practices.

Recommendations for Transparency of ADMS

To make inroads on reigning in the equity harms associated with automated decision making systems, policymakers and regulators should consider the following measures.

First, regulatory mechanisms to curb harmful bias and discrimination and other harms created by an ADMS may be introduced via a comprehensive data protection regime, but also through standalone initiatives that compel more transparency around ADMS, disclosure of their use, and the introduction of redress and accountability mechanisms. Thus, providing answers to a variety of questions in relation to ADMS are critical pieces to understanding and mitigating some of the equity risks associated with their use, for example: Are ADMS used for certain decisions? How do they contribute to said decisions? What information do these systems rely on? And how exactly are they deployed? Without adequate notice, consumers usually do not have a way of knowing whether an ADMS is behind a particular decision, let alone understand the equity risks associated with the system. One example of such a notice mechanism is Article 52 in the EU's proposed Artificial Intelligence Act, which would mandate that individuals directly interacting with ADMS should be informed of this fact. However, while such a notice mechanism would create awareness of the fact that ADMS are used among people directly interacting with the system, it would still fail to notify people who are directly *affected* by its use.

Second, consumers need robust enforcement of anti-discrimination laws that eases the path for individuals seeking remedy from harms created by ADMS.[28] Civil rights advocates and legal experts[29] have flagged the inadequacy of our current legal and regulatory framework to remedy the discriminatory outcomes that may result from the deployment of automated tools in certain circumstances.[30] Even when system inputs avoid protected characteristic data, discrimination may still occur — for example due to data that may (inadvertently) serve as a proxy for protected categories. To complicate things further, developers of complex ADMS may be unable to trace how the inputs of an ADMS lead to certain outputs. This makes it difficult to identify at which exact "step" or due to which factors harmful bias is introduced in decision-making, or to create a documentation "trail" for those seeking remedy.

Transparency measures are important steps towards mitigating harm, especially when coupled with guardrails on how an ADMS can be used. Regulators must consider the high-risk contexts in which an ADMS can be potentially deployed–either where sensitive data is concerned, or when there is a sensitive use case or decision to be made. In some circumstances, this includes determining whether it is appropriate to use an ADMS at all. At the very least, human intervention should validate decisions of high consequence for consumers, such as approval for a higher mortgage interest rate, rejection for an auto loan, or flagging someone as suspect in the criminal justice system. Consumers also need effective countermeasures, such as a formal complaint mechanism to the Federal Trade Commission (FTC) for investigation, that allows individuals or organizations representing their interest to seek remedies for harms associated with an ADMS — be it privacy-related, or with respect to other harms such as discrimination or economic loss. Finally, regulators should reserve the authority to

[28] OSTP "Blueprint for an AI Bill of Rights" October 2022. https://www.whitehouse.gov/ostp/ai-bill-of-rights/algorithmic-discrimination-protections-2/
[29] Testimony of Dr. Pauline Kim before the US EEOC, January 31, 2023. https://www.eeoc.gov/meetings/meeting-january-31-2023-navigating-employment-discrimination-ai-and-automated-systems-new/kim
[30] Upturn testimony on "Stop Discrimination by Algorithms Act of 2021." https://www.upturn.org/work/testimony-on-dcs-stop-discrimination-by-algorithms-act-of-2021/

rein in the use of an ADMS that inherently poses unacceptable risks of discrimination or infringements of people's privacy.

However, it is not enough to only address harms that have already taken place. Regulators must take a proactive role in incentivizing, enforcing, and conducting ADMS audits that can surface and prevent potential harms to consumers, both before they are deployed widely in the market and after deployment. This means ensuring that automated systems are audited for both biases, accuracy, privacy risks and other harms. Further, to conduct regulatory audits, authorities further need to be able to obtain sufficient access to relevant data, documentation, and systems where necessary and justified in order to accurately and effectively understand how the ADMS system operates. The foundational work of outside experts and researchers like those at Mozilla on algorithmic auditing can be a valuable resource and learning tool for policymakers looking to understand how to make bias auditing meaningful, which includes the Open Source Audit Tooling project led by Mozilla fellow Deborah Raji as well as the Mozilla Technology Fund.[31]

D. Federal Privacy Legislation is Critical for Advancing Equity and Civil Rights Online

Despite being a powerhouse of technology and innovation, the US lags behind global counterparts when it comes to privacy protections. Everyday, people face the real possibility that their very personal information could fall into the hands of third parties seeking to weaponize it against them.

At Mozilla, we strive to not only empower people with tools to protect their own privacy, but also to influence other companies to adopt better privacy practices. That said, we can't solve every problem with a technical fix, public pressure, or rely on companies to voluntarily prioritize privacy.

---

[31] Raji. "It's Time to Develop the Tools We Need to Hold Algorithms Accountable." 2022. https://foundation.mozilla.org/en/blog/its-time-to-develop-the-tools-we-need-to-hold-algorithms-accountable/ ; See also: Mozilla Technology Fund: Auditing Tools for AI Systems,https://foundation.mozilla.org/en/what-we-fund/awards/mozilla-technology-fund-mtf/

Strong federal privacy legislation is critical in creating an environment where users can truly benefit from the technologies they rely on without paying the premium of exploitation of their personal data.[32] Last year, the House Energy and Commerce Committee passed the bipartisan American Data Privacy and Protection Act (ADPPA), which Mozilla endorsed.[33] ADPPA prohibits discriminatory uses of data,[34] reining in the surveillance economy and furthering efforts to address issues at the intersection of privacy and equity. It's essential that Congress enact a strong baseline privacy rule, such as ADPPA.

We also welcome the FTC's effort to move forward on an Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security. The call for comments sought input on discrimination based on protected classes, algorithmic discrimination, and more.[35] We're encouraged by the prospect of legislation or regulation in this space.

1. Global Privacy Control (GPC)

In Question *4c*, NTIA asks if there are existing privacy laws being effectively enforced, and if not, how should these deficiencies be remedied. Mozilla has experimented with a setting - the Global Privacy Control (GPC)[36] - to help consumers opt-out of the sale or sharing of their information on the Internet. Once turned on, GPC sends a signal to the website's consumer visit telling them that the consumer does not

[32] Hodges, Jenn T. "It's Time to Pass U.S. Federal Privacy Legislation." Mozilla Open Policy & Advocacy blog. August 24, 2022. https://blog.mozilla.org/netpolicy/2022/08/24/its-time-to-pass-u-s-federal-privacy-legislation/

[33] House Energy & Commerce Committee. "ICYMI: E&C Republicans and Technology and Cybersecurity Experts Renew Calls for Comprehensive Data Privacy Protections." February 6, 2023. https://energycommerce.house.gov/posts/icymi-e-and-c-republicans-and-technology-and-cybersecurity-experts-renew-calls-for-comprehensive-data-privacy-protections

[34] Epic. "Comparison of American Data Privacy and Protection Act vs. California Privacy Laws." July 28, 2022. https://epic.org/wp-content/uploads/2022/07/ADPPAvCCPA-07282022.pdf

[35] Trade Regulation Rule on Commercial Surveillance and Data Security. August 22, 2022. https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

[36] Mozilla. "Implementing Global Privacy Control." October 29, 2021. https://blog.mozilla.org/netpolicy/2021/10/28/implementing-global-privacy-control/

want their data to be sold. This universal opt-out mechanism, set by the consumer, sent by the browser to all websites, and then enforced by the regulators, is critical.

Unfortunately, the enforceability of the GPC remains ambiguous, with many businesses uncertain about the legal enforceability when they receive a signal such as the GPC. This is particularly true for companies receiving a GPC signal from consumers outside of specific jurisdictions that have codified GPC obligations in state privacy laws. The practical impact of lack of enforceability is that businesses may simply ignore the GPC signal - especially if they have elected to use any other mechanisms to receive opt-out requests.

History shows that without a clear legal mandate, most businesses will not comply with consumer opt-out signals sent through browsers. Mozilla encourages rules that expressly require business to comply with GPC – or to honor some standardized opt-out signal for tracking. Further, enforcement authorities should expect businesses to interpret the GPC as governing both the direct sale of consumer's information as well as the sharing of consumers' information for programmatic advertising targeting purposes. Regulators must give tools like the GPC enforcement teeth and to ensure consumers' choices are honored. Otherwise, anything "voluntary" in this space is ineffective (note this relates to question *6e* regarding limitations of voluntary codes of conduct).

VII. Conclusion

Mozilla applauds NTIA's initiative to collect comments on questions related to privacy, equity, and civil rights in the context of commercial data collection practices and use of automated decision-making systems. As set out above, the practices surrounding consumer data on the internet today, and the resulting societal harms, have put individuals' trust at risk. The future of privacy online requires industry to step up to protect and empower people, and demands that lawmakers and regulators implement frameworks that preserve consumer privacy and protect people from harm.

Contact for Additional Information

Jenn Taylor Hodges, Director of US Public Policy and Government Relations, Mozilla Corporation - jhodges@mozilla.com

Reem Suleiman, US Advocacy Lead, Mozilla Foundation - reems@mozillafoundation.org