**Written Statement of Marshall Erwin, Chief Security Officer**
**Mozilla**

**Before the Committee on House Administration**
**United States House of Representatives**

**"Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors"**

**February 16, 2022**

Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, thank you for holding this hearing today on such an important issue, and for the opportunity to testify.

I'm Marshall Erwin, Chief Security Officer at Mozilla.

## Our Public Mission and Incentives

Mozilla is a unique public benefit organization and open source community formed as a non-profit foundation. We build the open-source Firefox web browser, Mozilla VPN, and the Pocket "read-it-later" application. These products are used by hundreds of millions of individuals around the world. As a mission-driven technology company and a non-profit foundation, we are dedicated to putting people in control of their online experience, and creating an internet that is open and accessible to all.

To fulfill this mission, we are constantly investing in the security of our products, the privacy of our users and in advancing the movement to build a healthier internet. Mozilla has influenced major companies to adopt better privacy practices such as browser anti-tracking measures and empowered people directly with tools to better understand and block third party data collection. For Mozilla, privacy is not optional. It is an integral aspect of our founding principles, which state that individuals' security and privacy on the internet are fundamental and must not be treated as optional.

**Mozilla's Meaningful Protections by Default and Design**

We have worked hard to make Mozilla's vision for privacy and security a reality in the products we build and the technologies we develop. We do this by leading and participating in the creation of web standards that make the internet more secure and more protective of privacy, and by pioneering the product-level implementation of privacy and security-enhancing browser technologies through Firefox. These open innovations are available to the wider internet: other organizations, internet applications, and consumers.

For example, we have made online commerce and navigation safe through protocols and initiatives like TLS 1.3 and Let's Encrypt. TLS 1.3 is the protocol that powers every secure transaction on the internet. Let's Encrypt is a major internet security success story; because of its creation, 85% of online traffic is now encrypted with HTTPS (signaled by a green padlock on many web browsers), compared to less than 30% in 2014.

We have always put privacy first in our own products and features.

- In 2019 we enabled **Enhanced Tracking Protection**[1] by default in Firefox, protecting our people from cross-site tracking. While anti-tracking features had been available for many years in Firefox, we turned this feature on by default because we believe[2] that the onus should not be on consumers to protect themselves from sophisticated privacy risks they do not understand.
- Last year, we introduced one of our strongest privacy protections to date, **Total Cookie Protection,**[3] to provide additional protections from cross-site tracking.
- Mozilla has also been instrumental in the technological development and product roll-out of technologies to encrypt web traffic. This includes most recently our work on **DNS over HTTPs**[4] - or DoH - the protocol that encrypts domain name look-ups and closes one of the last great security vulnerabilities in the internet architecture.

---

[1] Dave Camp, "Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise," Mozilla dist://ed (June 4, 2019), *at* https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/

[2] Steven Englehardt, "Why we need better tracking protection," Mozilla Security Blog (Sept. 5, 2018), *at* https://blog.mozilla.org/security/2018/09/05/why-we-need-better-tracking-protection/

[3] Selena Deckelmann, "Latest Firefox release includes Multiple Picture-in-Picture and Total Cookie Protection," Mozilla dist://ed (Feb. 23, 2021), *at* https://blog.mozilla.org/en/products/firefox/latest-firefox-release-includes-multiple-picture-in-picture-and-total-cookie-protection/

[4] Patrick McManus, "Improving DNS Privacy in Firefox," Firefox Nightly News (June 1, 2018), *at* https://blog.nightly.mozilla.org/2018/06/01/improving-dns-privacy-in-firefox/

- Our **VPN** (Virtual Private Network)[5] helps people create a secure, private connection to the internet.
- And our end-to-end encrypted **Firefox Sync[6]** service by default protects all your synced data so Mozilla can't read it.

We also support practical solutions to help companies have a healthier relationship with data, through our Lean Data Practices (LDP) framework and trainings.[7] LDP helps other organizations to reduce the amount of user data that is initially collected and focuses on only collecting essential data to lower risk and promote trust with users. We have published this framework under an open license, and have worked with organizations around the world to educate other businesses on the benefits of such an approach. We have learned through LDP workshops with public sector participants that the absence of a uniform data protection law causes challenges to minimize, delete, and limit the sharing of data today. Especially at the local level, there may also be a lack of resources to better secure data or explain to constituents how it is used and shared.

**Addressing the Systemic Privacy Problem Through Legislation**

While we play an important role in keeping people secure and protecting privacy on the internet, we nonetheless recognize that the lack of privacy online today is a systemic problem. We need structural change to protect data and empower people. We therefore believe that law and regulation have an essential role to play in creating a healthier internet. Relying on the voluntary adoption of protocols and practices like the ones we have designed is an incomplete solution.

In our view, technical privacy protections by companies and privacy regulation are complementary and necessary. Neither alone is sufficient. The internet was not originally designed with privacy and security in mind, which is why technical solutions are necessary to create a less permissive environment that is more protective of people. But we cannot solve every privacy problem with a technical fix.

For example, we know that dark patterns are pervasive across the online applications that people engage with daily. Unfortunately, there is little any browser can do when a person visits a website directly and is deceived by the website into handing over and sharing their data without meaningful consent. This is where law, plus a robust enforcement regime, must step in. That is why provisions such as the one in the *Online Privacy Act* that prohibit dark patterns are so critical.

[5] Mozilla VPN, *at* https://www.mozilla.org/en-US/products/vpn/more/what-is-a-vpn/
[6] Firefox Sync, *at* https://www.mozilla.org/en-US/firefox/sync/
[7] Mozilla Lean Data Practices, *at* https://www.mozilla.org/en-US/about/policy/lean-data/

Another example is what we call browser fingerprinting, which is a technique used to track consumers by constructing an identifier from the characteristics of their browser. Fingerprinting is opaque to users and would fail to satisfy many user privacy rights regimes. Mozilla attempts to block fingerprinting in Firefox, but we recognize that we will not be able to defeat all fingerprinting activities, no matter how we change our browser. In areas like these, technical solutions will not be enough.

This is why Mozilla strongly supports privacy and data protection laws around the world, including in the US. The US should enact baseline federal privacy protections, to ensure public and private actors treat consumers fairly. We need clear rules of the road for entities using personal data, strong rights for people who interact with those entities, and effective authority for the Federal Trade Commission (FTC) to make and enforce these rules as technologies evolve. Ultimately, privacy, security, and consumer data protection are best-served when policy is based upon a comprehensive framework of protections.

**Greater Transparency into Hidden Harms**

Many of the harms we see on the internet today are in part a result of pervasive data collection and underlying privacy risk. Targeting and personalization systems generate real value for consumers. But, as we have learned from recent whistleblower disclosures, these systems also can be abused, resulting in real world harm to individuals and communities. They are powered by people's data. Indeed, the more you know about someone, the easier it will be to deceive, or peddle disinformation, or discriminate against them.

The world has now had a few years of experience with global and state laws covering baseline data and security requirements. Unfortunately, there remains a looming gap, which is that we lack sufficient insights into how people experience online discrimination and harm when their data is collected, used and shared without meaningful awareness or consent. This includes what ads are presented to you and why, and what content is recommended to you and why. To address this, we need complementary regulatory solutions to federal privacy legislation that would provide greater levels of transparency into the ecosystem impact of our online data.

At Mozilla, we support solutions that will provide greater transparency into online discrimination and harms that today are hidden from the public and from regulators. Accordingly, we have called for establishing a safe harbor allowing researchers,

journalists, and others to access relevant datasets, free from threats of legal action. Such a safe harbor should protect research in the public interest as long as researchers handle data responsibly and adhere to professional and ethical standards. We know there is enormous value this can provide to the public. Mozilla has one of the earliest Bug Bounty programs in software. We make clear that we will not threaten or bring any legal action against anyone who makes a good faith effort to comply with our vulnerability notification policy because this encourages security researchers to investigate and disclose security issues. Their research helps make the internet a safer place.

Similarly, we advocate for a more robust disclosure regime governing the ads people see online. We have been leading the push for full ad disclosure in the European Union's Digital Services Act and we are encouraged by recent proposals in Congress that would require disclosure of ads for public benefit and understanding. These approaches would bring transparency into the opaque world of online advertising and can be done in ways that do not pose privacy risk to users.

**Structural Solutions Should be Used to Limit First Party Data Use**

Federal privacy law, while essential, should also be bolstered by regulation and enforcement to foster stronger consumer protection and competition. The most dominant technology companies today are the largest third-party trackers on the internet. At the same time, the same companies also have extensive first party relationships with consumers and have benefited the most from the absence of oversight to protect consumers.

We support efforts by regulators to tackle this problem through interventions governing how data can be shared and used within the holding structures of large platforms. For example, we strongly support Google's recent commitments to UK regulators to foreclose the use of data from Android, Chrome browsing history and sync data, Google Analytics, and Customer Matching for targeting after implementation of Chrome Privacy Sandbox proposals. This is a positive direction for the evolution of a more private and secure internet that will benefit consumers around the world. Indeed, all dominant platforms should embrace commitments like this and start practicing them immediately, beyond just advertising or browser technologies, to ensure a fairer and more interoperable internet for everyone.

At the same time, it is important that competition concerns not be a pretext to prevent better privacy for everyone. Many parties, large and small, have built their business

models to depend on extensive user tracking. Many third-party advertising companies that depend on ubiquitous user tracking seek to prevent privacy innovation. Closing privacy gaps necessarily means denying data to these parties. That is a good thing. Consumer welfare is at the heart of both competition and privacy enforcement. Focusing on consumers and their needs will ensure regulation doesn't inadvertently freeze the evolution of internet technologies that can offer consumers advances in privacy and security.

**Conclusion**

At Mozilla, we seek to advance a favorable environment for privacy-enhancing technologies, and to ensure that privacy considerations are front and center of policymakers' minds when considering how to protect consumers and grow our economy.

We believe through our product and policy work we can help address the data privacy gaps that exist today, impacting consumers, companies, and the public sector alike. Despite being a powerhouse of technology innovation for years, the United States is behind globally when it comes to recognizing consumer privacy and protecting people from indiscriminate data collection and use. We appreciate the Committee’s focus on this vital issue and look forward to further discussions with Congress. Thank you.