Written Statement of Marshall Erwin, Chief Security Officer
Mozilla

Before the House Subcommittee on Oversight and Investigations

"Who is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy"

April 19, 2023

Chair Rodgers and Ranking Member Pallone, Chair Griffith and Ranking Member Castor, thank you for holding this hearing today and for the opportunity to testify on this important topic.

I'm Marshall Erwin, Chief Security Officer at Mozilla. Over the course of my testimony, I hope to illustrate how technical protections, such as those in Mozilla's products, can only go so far in preserving the privacy of individuals online and how urgent policymaker intervention is needed to mitigate the most egregious practices of the data broker ecosystem.

Our Public Mission and Incentives

Mozilla is a unique public benefit organization and open source community owned by 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.

Protecting People from Pervasive Data Collection

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. Many of the harms we see on the internet today are in part a result of pervasive data collection and underlying privacy threats. The targeting and personalization systems based on this data generate real value for consumers. But, as we have learned from whistleblower disclosures[1] and independent research[2], 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. Further, many of these harms of unchecked data collection and use online today - in the data broker industry and beyond - are completely opaque to users and policymakers alike.

At Mozilla, we believe the web can do better and have been working to drive the industry in a better direction and to make Mozilla's vision for privacy and security a reality. We have done so by limiting the use of third-party cookies[3], developing more privacy preserving ways to measure user interactions online, and advancing privacy preserving advertising[4]. These open innovations are available to the wider internet: other organizations, internet applications, and consumers. We are engaging at standards development organizations (SDOs) committing to plug the holes; this can be seen with the increasing focus on privacy at the World Wide Web Consortium (W3C).

A huge amount of our focus is on building privacy protections into the browser itself to make data collection harder and to help consumers avoid the harms of the data ecosystem. We specifically work to protect consumers' browsing history. This is the data you create as you browse from website to website. It can over time create an incredibly detailed, sensitive portrait of your online life. To protect this data, we focus on two areas.

---

[1] "Facebook putting profit before public good, says whistleblower Frances Haugen" The Guardian. October 4 2021. Available at: https://www.theguardian.com/technology/2021/oct/03/former-facebook-employee-frances-haugen-identifies-herself-as-whistleblower

[2] Milano, S., Mittelstadt, B., Wachter, S. et al. Epistemic fragmentation poses a threat to the governance of online targeting. Nat Mach Intell 3, 466–472 (2021). https://doi.org/10.1038/s42256-021-00358-3

[3] "Firefox rolls out Total Cookie Protection by default to all users worldwide." Mozilla Blog. June 14, 2022. https://blog.mozilla.org/en/products/firefox/firefox-rolls-out-total-cookie-protection-by-default-to-all-users-worldwide/

[4] Eric Rescorla, "The future of ads and privacy". Mozilla Blog. May 28 2021. Available at: https://blog.mozilla.org/en/mozilla/the-future-of-ads-and-privacy/

- In security, we have driven major initiatives such as standardizing the internet's most deployed security protocol, **TLS 1.3**[5] and founding **Let's Encrypt,** a free service that gives people the digital certificates they need in order to encrypt their website. This has resulted in more than 85% of online traffic being encrypted with HTTPS, compared to less than 30% in 2014. This work makes it harder to surveil your activity online and collect data about your web browsing. It also makes online ecommerce safer.

- We also work hard to block cross-site tracking in the browser. This prevents parties from following you around the Internet and building profiles of your browsing history. In 2019 we enabled **Enhanced Tracking Protection**[6] in Firefox, protecting people from cross-site tracking. We did this by default because we believe the burden should not be on consumers to protect themselves from complex privacy risks.

We also seek to protect consumer data at point of collection, for example through our **Lean Data Practices (LDP)** methodology.[7] LDP includes being conscious to collect only data we need, clearly and concisely explaining what we collect, how we use it, how we mitigate risks and so on. This includes engaging consumers (making privacy policies more accessible and explaining data collection through "just-in-time" notifications), staying lean (rather than collecting, storing, and sharing indiscriminately), and build-in security (improving key security features, training for employees and vendor due-diligence). We implement these principles in our own products using our Data Privacy Principles, and we support new rules imposing data minimization limitations on companies' collection, use, and retention of consumer data. If you can minimize the data collected initially, or ensure meaningful consent mechanisms, you can reduce risk from the start.

Dark Patterns, Data Sharing, and Data Brokers

Despite the progress we have made building privacy protections into the key desktop and mobile platforms people use, major privacy gaps still exist both from a technical and a policymaking perspective.

---

[5] Eric Rescorla, "TLS 1.3 Published: in Firefox Today." Mozilla Security Blog. August 13, 2018. https://blog.mozilla.org/security/2018/08/13/tls-1-3-published-in-firefox-today/

[6] 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/

[7] Nneka Soyinka. "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/

Technical privacy measures by companies are critical but not sufficient. We know from our experience in Firefox that we cannot solve every privacy problem with a technical fix. Dark patterns, for example, are pervasive across the software people engage with daily. Consumers are being tricked into handing over their data with deceptive patterns, then that data is used to manipulate them. Our protections against data collection via third party cookies might prevent cross-site tracking but they can do little to help users sharing data directly with websites (also called first party data sharing).

Once a consumer has been tricked into handing over their data, that is where data brokers come in. While companies like Mozilla and consumers have some limited visibility into online tracking, we lose that visibility entirely once that data lands on a company's servers and is shared on what we sometimes call the *backend.* Companies may then share data internally to power their other products; intercompany data transfers are used by the biggest vertically integrated tech players, to their benefit and our expense. Or companies may share or sell data to data brokers, for eventual use by other parties. This type of backend data transfer is something the browser cannot see. Because of this limited visibility, it is nearly impossible to fully understand the extent of this data selling and sharing today.

As browsers and mobile operating systems have moved to clamp down on leading forms of online tracking, particularly cookie-based tracking, parties are increasingly using other forms of tracking and backend data sharing. For example, we are concerned by the growing use of identity-based tracking. Often when you visit a website, you are encouraged to sign up for an account and hand over your email address. What many consumers do not realize is that their email address may then be handed over to other parties – including data brokers – and may be used as an index to build a profile of browsing activity. Companies engaged in this activity will often say that they *hash* these identifiers in order to protect privacy. Hashing is a process where basically companies take one string of letters, run it through an algorithm, and translate it into another string of letters. This hashing nonetheless will create an identifier that remains unchanged for years and – most concerning – can easily be reversed to determine the original email address. Hashing is essentially privacy theater with no meaningful privacy benefits.

Mozilla offers a tool called Firefox Relay[8] to address this risk, allowing consumers to generate unique email addresses when they sign up. Not enough consumers benefit from such a service – email identifiers are now a major tracking vector.

[8] Firefox Relay. https://relay.firefox.com/

Identity based tracking is just one of the many privacy loopholes that exist today. Persistent identifiers generally – ad identifiers, email addresses, and what we call browser fingerprints – are tools that data brokers can use to build a data profile about you and then sell that profile. We are reaching the limits of what we can do in the browser to protect people from this data collection and sharing.

Addressing the Systemic Privacy Problem Through Legislation

While Mozilla and likeminded companies play an important role in keeping people secure and protecting privacy on the internet, we 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 companies to voluntarily prioritize privacy with the adoption of protocols and practices like the ones we have designed is an incomplete solution. We cannot solve every privacy problem with a technical fix. Legislators and technology companies together have an opportunity to improve the privacy ecosystem.

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, in 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 is why Mozilla strongly supports privacy and data protection laws around the world, including in the United States. Despite being a powerhouse of technology and innovation, the U.S. 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.

Transparency is a key piece of the puzzle. Mozilla has long supported rules to provide greater transparency into how people experience online discrimination and harm when their data is collected, used and shared without meaningful awareness or consent. Transparency is a key part of how Mozilla approaches user trust, and greater transparency from all players would shine a light on hidden harms, enabling policymakers to better understand and intervene.

Most importantly, 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. We supported the American Data Privacy and Protection Act (ADPPA) in the last Congress, and are eager to see it advance in this Congress. It is time that we tackle the real-world harms that emerge as a result of pervasive data collection online and abusive privacy practices.

ADPPA, for example, defines sensitive data to include *information identifying an individual's online activities over time and across third party websites or online services.* This is incredibly important. As we mentioned above, Mozilla spends a large amount of time trying to protect this data in Firefox. Regulatory regimes need to similarly move beyond narrow categories of what is traditionally considered Personally Identifiable Information. Browsing data can be some of the most sensitive and potentially harmful data collected and sold about a consumer. It must be protected both by the platforms people use and by privacy laws.

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.

This year is the 25th anniversary of Mozilla's founding. We've been working to protect our consumers for those 25 years. We established the first private bug bounty program more than 20 years ago. We were the first company to encrypt people's web traffic. And we are particularly proud of the progress we have made in recent years to prevent cookie tracking. Unfortunately, privacy regulation has not kept pace with this progress. It is time for federal policy to protect consumers too.

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 continuing our work with policymakers to achieve meaningful reform that restores trust online and holds companies accountable. Thank you.