Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on Advancing Privacy Enhancing Technologies

Mozilla

July 8, 2022

Office of Science and Technology Policy
Eisenhower Executive Office Building
725 17th Street NW
Washington, D.C.
United States of America

Via Email to: PETS-RFI@nitrd.gov

Subject: "RFI Response: Privacy-Enhancing Technologies"

—

Mozilla is submitting this response, focused on digital advertising, to the Office of Science and Technology Policy's (OSTP) Request for Information[1] to inform the development of a national strategy on privacy preserving data sharing and analytics, along with associated policy initiatives. Regulators and technology companies together have an opportunity to improve the privacy properties of online advertising—an industry that has not seen privacy improvement in many years. Mozilla has worked on shaping the ongoing evolution of privacy preserving advertising for the past decade, both in our products[2] as well as in our external

[1] Request for Information on Advancing Privacy-Enhancing Technologies, Science and Technology Policy Office. 6 July, 2022. Available at: https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies

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

engagement with regulators[3], industry[4], and standards bodies.[5] We welcome this opportunity to briefly share our thinking on this critical issue, with the intent of placing our extensive work so far on the record and paving the way for further conversations.

Specifically, our response covers the following items from the scopes listed in the RFI request "2. Specific technical aspects or limitations of PETs"; "3. Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs"; and "10. Other information that is relevant to the adoption of PETs".

About Mozilla

Mozilla is the maker of the open-source Firefox web browser, the Pocket "read-it-later" application and other products and services that collectively are used by hundreds of millions of individuals around the world. Mozilla is also a global community of contributors and developers who work together to keep the internet open and accessible for all. 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's Thinking on Privacy Preserving Advertising

Mozilla has often outlined[6] that the current state of the web is not sustainable, particularly in the context of how online advertising works today. It is a hostile place for user privacy, and is effectively an arms race[7] between browser anti-tracking technologies and trackers. It's opaque by design, rife with fraud, and does not serve the vast majority of those which depend on it - from publishers, to advertisers, and of course, the people who use the open web. It is also important to note that many critical aspects of internet architecture were not created with privacy in mind. However, the growing importance of privacy has led to experts at standards

---

[3] Despite improvements, delaying the deprecation of third party cookies in the CMA's Privacy Sandbox commitments will hold back privacy on the open web, Mozilla Blog. December 17, 2021. Available at: https://blog.mozilla.org/netpolicy/2021/12/17/privacy-sandbox-cma-dec2021/

[4] Analysis of Google's Privacy Budget Proposal, Eric Rescorla. October 1, 2022. Available at: https://blog.mozilla.org/mozilla/google-privacy-budget-analysis/

[5] Interoperable Private Attribution (IPA) at the Private Advertising Technology Community Group (PATCG) of the World Wide Web Consortium. 6 January, 2022. Available at: https://github.com/patcg/private-measurement/issues/9

[6] Mozilla responds to the UK CMA consultation on Google's commitments on the Chrome Privacy Sandbox, Marshall Erwin. July 9, 2021. Available at: https://blog.mozilla.org/mozilla/uk-cma-google-commitments-chrome-privacy-sandbox/

[7] Narayanan, A., 2018. The web tracking arms race: Past, present, and future. In Enigma 2018 (Enigma 2018). Available at: https://www.usenix.org/conference/enigma2018/presentation/narayanan

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).

At the same time, we also believe there's nothing inherently wrong with digital advertising. It supports a large section of services provided on the web and we believe it is here to stay. However, the ways in which advertising is conducted today - through pervasive tracking, serial privacy violations, market consolidation and lack of transparency - is not working and causes more harm than good.

At Mozilla, we have been working for years to drive the industry in a better direction, away from pervasive and opaque web tracking. We've done so by limiting[8] the use of Third-party cookies, developing more privacy preserving ways to measure user interactions online,[9] and working on advancing privacy preserving advertising.[10] We believe the web can do better and are already doing work on the technical side to eliminate third party tracking, and engaging with thePrivate Advertising Technology Community Group (PATCG) at the W3C and other industry fora.

Opportunities & Challenges for Multi-Party Computation Solutions

In addition to our extensive work analyzing various PETs proposals put forward by industry, Mozilla has done considerable work exploring, developing, and implementing one class of PETs solutions - those involving *Multi-Party Computation (MPC)*. This includes developing, deploying, and testing Prio, a privacy preserving data collection technique developed at Stanford, within the Firefox browser. More recently, in partnership with Meta, we developed and proposed Interoperable Private Attribution (IPA), an MPC solution that would allow advertisers to measure and understand the effectiveness of their ad campaigns without having to track and collect extensive user level data.

The basic premise of these MPC solutions is that, using various advanced cryptographic techniques, data is shared across multiple servers in a way that avoids allowing any single entity — websites, browser makers, or advertisers — to learn about user behavior. Those servers can then work together to produce aggregate results that cannot be linked to individual users. For example, Mozilla has run a trial using 'Prio' to better understand what websites were being blocked in Firefox by privacy features.[11] This would have previously required directly collecting data about users' browsing activity. To know what was being

---

[8] Firefox 86 Introduces Total Cookie Protection, Tim Huang, Johann Hofmann and Arthur Edelstein. February 23 2021. Available at: https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/

[9] Next steps in privacy-preserving Telemetry with Prio, Steven Englehardt. June 6, 2019. Available at: https://blog.mozilla.org/security/2019/06/06/next-steps-in-privacy-preserving-telemetry-with-prio/

[10] Building a more privacy preserving ads-based ecosystem, Mozilla blog. Available at: https://blog.mozilla.org/mozilla/building-a-more-privacy-preserving-ads-based-ecosystem/

[11] Kogan, D., & Corrigan-Gibbs, H. (2021). Private blocklist lookups with checklist. In the 30th USENIX Security Symposium (USENIX Security 21) (pp. 875-892). Available at: https://rwc.iacr.org/2020/slides/Gibbs.pdf and https://www.usenix.org/system/files/sec21-kogan.pdf

blocked, we would have needed to know what websites users were trying to visit. As a privacy respecting company, that is data we do not want to collect. Instead, the Prio trial allowed us to collect aggregate information about websites without ever learning about individuals' browsing activity.

While MPC solutions have specific use-cases in browser measurement and advertising that have motivated Mozilla's work on this topic, the example above demonstrates the potential power of these tools. The internet today is having a profound, sometimes harmful impact on people's lives. But to really understand that impact and do data driven policy making today requires collecting highly sensitive data about people's online activities, even if we aren't interested in any individual's behavior. MPC provides a means to collect this data and understand aggregate activity without compromising people's privacy.

There are, however, a number of hurdles for this technology to ensure that it can both protect privacy and allow a diversity of parties to benefit from better aggregate insights. First, transparency and strong governance are critical to the success of MPC solutions and more work must be done to develop governance models for those that run pieces of these systems. One shortcoming of these approaches is that the different parties in the system might collude to break the privacy properties of the design and to gain access to individual level data. The relationship between those parties must be set up in such a way that they have strong incentives, structural limitations, and bylaws that prevent such collusion.

Second, it is important that a diversity of parties be able to offer MPC services and the federal government should explore ways to create and support that diverse ecosystem of MPC services. These services are complex to design and operate, requiring deep technical expertise and resources that can be found within a small number of major tech companies. Indeed, Apple, Google, and Meta have been on the forefront of developing this technology and have done very promising work on this topic. But a privacy-preserving world in which only the most dominant players have the means to offer MPC solutions would be a mixed blessing. Moreover, dominance of this space by major tech companies, which are not known for their transparency and are already known to abuse their market positions to disfavor competitors, would likely exacerbate the governance challenges mentioned above.

Finally, it is important that these services be available to diverse public and privacy sector parties. Again, a privacy-preserving world in which only the most dominant players are able to take advantage of these services, while researchers, academics, and watchdogs groups that could benefit from these services are left out in the cold, could reinforce the have/have not data divide that has allowed a small number of parties to gain significant insight into public life on the Internet while leaving outside groups starving for such insights.

Need for Complementary Regulatory Solutions

Apart from technical solutions, we believe in the need for better regulation and creating more partnerships with the ecosystem within the diverse range of actors. Without a better

regulatory framework, a sufficient incentive won't exist to move towards more privacy preserving techniques. And even with some of those techniques in place, various types of harm will persist that require regulatory intervention. We do not think that technical work alone will not solve the problem of the dependence on data, and the risks and harms that this causes, which include:

- Disinformation (elections, politics, etc.)
- Discrimination (race, age, gender, etc.)
- Societal Manipulation (vaccines, etc.)
- Privacy Violations (leaks, breaches, etc.)

Our vision is a web which empowers individuals to make informed choices without their privacy and security being compromised. While there is no denying behavioral advertising is the underlying business model of the web today, it does not mean that it cannot be reformed to minimize its societal harms. In order for this ideal to be realized, we think that:

- its impact on society should be understood better (research);
- Users—including publishers, advertisers, and oversight bodies—should be able to understand how or why they are being targeted (transparency);
- targeting should happen with minimal data collection (privacy preserving advertising);
- regulators should penalize violations of privacy and competition laws (enforcement);
- regulatory solutions should be explored which limit targeting and pave the way for better technical solutions (regulation)

In an ideal state, a combination of new research, technical solutions, increased public awareness and effective regulatory enforcement would reform behavioral advertising for the future of the web.

Importance of Standards Bodies

Open SDOs should play an essential role in the development and deployment of privacy preserving technologies for online advertising. Many of the underlying standards that form the bedrock of today's internet have been transparently debated and collaboratively developed at SDOs by relevant stakeholders through formal processes. For example, Transport Layer Security (TLS) is a foundational security protocol that was developed at the Internet Engineering Task Force (IETF). Cascading Style Sheets (CSS) is a cornerstone technology to develop webpages and was developed at the W3C.

These seminal standards were not developed overnight or by a single company; rather, multiple stakeholders, including different browsers and browser engines, worked

collaboratively and transparently over years in open SDOs. This approach, sometimes colloquially referred to as "rough consensus and running code" prioritizes real world deployment and validation and helps ensure critical technologies for the internet also serve the collective interest. This also allows third party vendors (service providers) and browsers to operate across diverse offerings of the same or similar services, and create consistently clear experience expectations for consumers, which is especially vital for online advertising.

Mozilla has always believed that a vibrant and open internet depends on fair conditions, open standards, and opportunities for a diversity of market participants to participate. We have substantial experience contributing to open SDOs over the last two decades, having played a key role in the development and implementation of critical standards such as TLS 1.3 and HTTP/3 as well as industry wide initiatives like Let's Encrypt. It is through open standards that we believe the internet can remain decentralized, open, and interoperable.

Global standards development is a voluntary consensus-driven process. For this reason, stakeholder commitment to final specifications and deployment on specific timelines is vital for an open web. The commitment and deployment, particularly by large stakeholders, is necessary to materialize theory developed in SDOs into practical applications used widely across products in a particular industry. Markets can be distorted, and consumers impacted, either due to the absence of commitment to the final standard itself *and/or* not respecting the agreed upon timelines to deploy or deprecate relevant technologies. We think that this interplay of process and consensus is vital for privacy preserving technologies around advertising to develop in a sustainable manner rather than being unilaterally imposed upon the ecosystem.

The direct implementation of web features by dominant players often leads to them becoming de facto web standards, often well before the relevant SDO has formally adopted the underlying standard itself. This could put many current industry proposals in this space at risk of becoming de facto industry benchmarks merely via their unilateral implementation by a few players, leaving publishers, and other browsers without choice or say in the matter. Taking the relevant standards to the appropriate formal SDOs, on the other hand, will help ensure that their properties are validated rigorously while also allowing for relevant public visibility and engagement to stakeholders via open processes. It will also allow for other players to play the appropriate role in the development of standards themselves.

Mozilla's Previous Work

The section below contains links to our previous work and regulatory submissions on the topic, which elucidate the thoughts we've mentioned above in greater detail.

Overview

- Building a more privacy preserving ads-based ecosystem[12]

[12] Building a more privacy preserving ads-based ecosystem, Mozilla Blog. May 28 2021. Available at: https://blog.mozilla.org/mozilla/building-a-more-privacy-preserving-ads-based-ecosystem/

- The future of ads and privacy[13]

Technical Analysis

- Privacy analysis of FLoC[14]
- Privacy analysis of SWAN.community and United ID 2.0[15]
- Analysis of Google's Privacy Budget Proposal[16]
- Privacy Preserving Attribution for Advertising[17]

Regulatory Submissions

- Mozilla responds to the UK CMA consultation on Google's commitments on the Chrome Privacy Sandbox[18]
- Despite improvements, delaying the deprecation of third party cookies in the CMA's Privacy Sandbox commitments will hold back privacy on the open web[19]
- Competition should not be weaponized to hobble privacy protections on the open web[20]

Conclusion

We believe that there is a real opportunity now to improve the privacy properties of online advertising by drawing upon the internet's founding principles of transparency, public participation, and innovation to make progress. We hope these brief thoughts are helpful in the OSTP's efforts in understanding the space and looking forward to continued engagement on this issue with relevant agencies in the coming months.

Contact for Additional Information

Jenn Taylor Hodges, Head of US Public Policy, Mozilla Corporation -

Udbhav Tiwari, Senior Manager, Global Public Policy, Mozilla Corporation -

---

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

[14] Privacy analysis of FLoC, Eric Rescorla. June 10, 2021. Available at: https://blog.mozilla.org/privacy-security/privacy-analysis-of-floc/

[15] Privacy analysis of SWAN.community and United ID 2.0, Mozilla Blog. August 4, 2021. Available at: https://blog.mozilla.org/mozilla/swan-uid2-privacy/

[16] Analysis of Google's Privacy Budget Proposal, Eric Rescorla. October 1, 2021. Available at: https://blog.mozilla.org/mozilla/google-privacy-budget-analysis/

[17] Privacy Preserving Attribution for Advertising, Martin Thomson. February 8, 2022. Available at: https://blog.mozilla.org/mozilla/privacy-preserving-attribution-for-advertising/

[18] Mozilla responds to the UK CMA consultation on Google's commitments on the Chrome Privacy Sandbox, Marshall Erwin. July 9, 2021. Available at: https://blog.mozilla.org/mozilla/uk-cma-google-commitments-chrome-privacy-sandbox/

[19] Despite improvements, delaying the deprecation of third party cookies in the CMA's Privacy Sandbox commitments will hold back privacy on the open web, Mozilla Blog. December 17 2021. Available at: https://blog.mozilla.org/netpolicy/2021/12/17/privacy-sandbox-cma-dec2021/

[20] Competition should not be weaponized to hobble privacy protections on the open web, Udbhav Tiwari. April 12, 2022. Available at: https://blog.mozilla.org/netpolicy/2022/04/12/competition-should-not-be-weaponized-to-hobble-privacy-protections-on-the-open-web/