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

Brave Software

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

RFI Response: Privacy-Enhancing Technologies

***Organization**: Brave Software*
***Organization Type**: Industry*
***Authors**: Shivan Kaul Sahib (Privacy Engineer and PM), Pete Snyder (Senior Privacy Researcher and Director of Privacy)*
***Date**: July 8, 2022*

Brave Software welcomes the opportunity to make brief comments in response to the Office of Science and Technology Policy's request for information on Advancing Privacy-Enhancing Technologies to help inform development of a national strategy on privacy-preserving data sharing and analytics.

Comments

Risks with PETs that rely on centralization (topics 2 and 7)

Some privacy-enhancing schemes rely on centralization of user data and resources to operate. For example, Google's Signed Exchanges [1] and Private Prefetch Proxy [2] proposals improve privacy for users by making Google's cache servers sit in-between the user and the website; the website owner does not come to know the user's IP address but the cache server learns all websites a user would potentially connect to. Privacy-preserving protocols like these centralize the collection of sensitive user data by one entity which then hides it from other entities. These kinds of privacy-enhancing technologies are problematic because they only improve privacy if you absolutely trust the centralizing party. If not, they are strictly worse for privacy. In addition, such schemes create a single point of privacy failure.

Even when the sensitive user data being collected is encrypted and the centralizing parties cannot view the raw data, which is the case with several new privacy-preserving data analytics schemes [3] that rely on multi-party computation, there are still concerns around cost of operation. Schemes that rely on multi-party computation tend to be extremely expensive and complex to operate, effectively ruling out deployment by smaller organizations. In effect, this means that centralization increases and economic competition decreases when it comes to deploying PETs. **To alleviate these concerns, there should be a focus on researching and developing PETs that can enhance privacy while not being prohibitively expensive or complex to deploy.**

Client telemetry (topics 3 and 6)

Browsers and other user clients rely on sending telemetry signals to a backend server in order to identify problems, detect breakages and inform product decisions. However, there is a risk of sending potentially-sensitive information about a user in these signals. There is active work being done in the Internet Engineering Task Force (IETF) [4] to standardize protocols that enable privacy-preserving data analytics, particularly in the Privacy Preserving Measurement (PPM) [5] and Oblivious HTTP Application Intermediation (OHAI) [6] working groups. Also note that some browsers like Brave have already deployed privacy-preserving analytics systems [7].

One of the protocols being discussed in the Privacy Preserving Measurement (PPM) IETF working group is Distributed Secret Sharing for Private Threshold Aggregation Reporting (STAR) (standardization draft [8], research paper [9]), which aims to provide k-anonymity privacy guarantees for client-submitted data using a combination of secret sharing and Oblivious Pseudorandom Functions (OPRFs). The focus of STAR is privacy that is cost-effective and easy to deploy.

Privacy-preserving client telemetry is an important area for research and development that often relies on multiple parties, and it's important that this work happens in open standardization bodies. Open source development of privacy-respectful protocols that prevent centralization should be encouraged.

Global Privacy Control (topics 4 and 5)

Global Privacy Control (GPC) [10] is a signal that allows users to notify websites and businesses of their privacy preferences when it comes to selling or sharing data. It is implemented in the Brave browser as well as the DuckDuckGo Privacy Browser, Mozilla Firefox, EFF Privacy Badger and others. GPC is recognized as a legitimate Do Not Sell request on behalf of a user according to the California Consumer Privacy Act (CCPA) [11]. **Privacy regulations should make it easy for users to indicate preferences similar to how CCPA explicitly supports the GPC signal. In general, legislation should allow privacy-focused client software to make privacy-relevant assertions on behalf of their users. User signals like Global Privacy Control should be supported on a federal level.**

References

1. “Signed Exchanges (SXGs).” *web.dev*, https://web.dev/signed-exchanges/. Accessed 7 July 2022.
2. “Private prefetch proxy in Chrome.” *Chrome Developers*, 11 May 2022, https://developer.chrome.com/blog/private-prefetch-proxy/. Accessed 7 July 2022.
3. Thomson, Martin. “Privacy Preserving Attribution for Advertising.” *The Mozilla Blog*, 8 February 2022, https://blog.mozilla.org/mozilla/privacy-preserving-attribution-for-advertising/. Accessed 7 July 2022.
4. *IETF | Internet Engineering Task Force*, https://www.ietf.org/. Accessed 7 July 2022.
5. “Privacy Preserving Measurement (ppm).” *IETF Datatracker*, https://datatracker.ietf.org/wg/ppm/about/. Accessed 7 July 2022.
6. “Oblivious HTTP Application Intermediation (ohai).” *IETF Datatracker*, https://datatracker.ietf.org/wg/ohai/about/. Accessed 7 July 2022.
7. “Privacy-Preserving Product Analytics (P3A).” *Brave Browser*, 22 August 2019, https://brave.com/privacy-preserving-product-analytics-p3a/. Accessed 7 July 2022.
8. “draft-dss-star-00 - STAR: Distributed Secret Sharing for Private Threshold Aggregation Reporting.” *IETF Datatracker*, 7 March 2022, https://datatracker.ietf.org/doc/draft-dss-star/. Accessed 7 July 2022.
9. “[2109.10074] STAR: Secret Sharing for Private Threshold Aggregation Reporting.” *arXiv*, 21 September 2021, https://arxiv.org/abs/2109.10074. Accessed 7 July 2022.
10. *Global Privacy Control — Take Control Of Your Privacy*, https://globalprivacycontrol.org/. Accessed 7 July 2022.

11. “California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General.” *California Department of Justice*, https://oag.ca.gov/privacy/ccpa/#heading7b. Accessed 7 July 2022.