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

ACT | The App Association

July 8, 2022

Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, District of Columbia 20504

RE: Comments of ACT | The App Association to the Office of Science and Technology Policy on its Request for Information on Advancing Privacy Enhancing Technologies

ACT | The App Association (App Association) appreciates the opportunity to submit views to the Office of Science and Technology Policy (OSTP) on its Request for Information on Advancing Privacy Enhancing Technologies (PETs). The App Association agrees with OSTP that PETs are an important tool for unlocking the full potential of the data economy and can help ensure that innovation in emerging technologies runs concurrently with a respect for basic human rights, promotes equity in data processing activities, and increases trust in the digital economy writ large.

The App Association represents thousands of small business software application development companies and technology firms that create the technologies that drive internet of things (IoT) use cases across consumer and enterprise contexts. Today, the ecosystem the App Association represents—which we call the app economy—is valued at approximately $1.7 trillion and is responsible for 5.9 million American jobs.[1] Alongside the world's rapid embrace of mobile technology, our members create the innovative solutions that power IoT across modalities and segments of the economy. App Association members exist at the cutting edge of the research, development, and implementation of PETs in their products and services.

Consumers who rely on our members' products and services expect that our members will keep their valuable data safe and secure. The small business developer community the App Association represents practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Their customers have serious data security and privacy expectations, and as such, ensuring that the company's business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity. For this reason, we support the Administration's goal of ensuring the United States leads the world in responsible data practices and technologies, including PETs, which are critical to our economic prosperity and national security, and to maintaining

[1] The App Association, State of the App Economy 2020, January 2021, https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf.

the core values behind America's scientific leadership, including openness, transparency, honesty, equity, fair competition, objectivity, and democratic values.

I. General Comments on Privacy Enhancing Technologies

The RFI notes that PETs encompass a "broad set of technologies that protect privacy," listing examples such as "secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic data generation tools."[2] The RFI goes on to emphasize "privacy-preserving data sharing and analytics technologies," a subset of PETs that help facilitate data sharing between entities and ensure those entities can perform advanced analytics without revealing the identities of the data subjects.

While we agree with the importance of advancing such PETs in the analytics space, we note that the constellation of PETs that app developers rely upon extends far beyond those few use cases. While there is no universally accepted taxonomy of PETs (or definition for the term, for that matter), existing efforts typically include categories of technologies that assist in the process of obtaining consent, data minimization, anti-tracking, encryption, anonymity, and control, among other categories, in addition to the technologies mentioned in the RFI.[3] One strategy OSTP may consider when taking stock of the full spectrum of PETs for its analysis is to either bifurcate its research into business to business (B2B) and business to consumer (B2C) buckets, or to simply track the entire life-cycle of a given piece of data in various industry verticals, from collection, to processing by the first-party collector and subsequent processing by service providers or other third parties. This would help ensure that OSTP takes all possible PETs into account, including those utilized by B2B and B2C developers.

In general, we encourage OSTP to take as broad a view of PETs as feasible as it takes on the responsibility of coordinating the national strategy to ensure that these tools benefit individuals and society. This would track similar work carried out by allied governments and existing efforts at the congressional level. For example, the Privacy Commissioner of Canada took an inclusive view of PETs in its report, "A Review of Tools and Techniques," saying, "PETs are intended to allow users to protect their (informational) privacy by allowing them to decide, amongst other things, what information they are willing to share with third parties such as online service providers,

---

[2] OSTP RFI on Advancing Privacy Enhancing Technologies, "Background", June 9, 2022. https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies

[3] See, e.g., Office of the Privacy Commissioner of Canada, "Privacy Enhancing Technologies -- A Review of Tools and Techniques," November 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/ pet_201711/#fn9

ENISA, "PETs controls matrix - A systematic approach for assessing online and mobile privacy tools", December 2016, https://www.enisa.europa.eu/publications/pets-controls-matrix

under what circumstances that information will be shared, and what the third parties can use that information for."[4] In the United States, the Promoting Digital Privacy Technologies Act, S.224, also takes a broad lens, defining PETs as "any software solution, technical processes, or other technological means of enhancing the privacy and confidentiality of an individual's personal data in data or sets of data."[5]

II. Specific Research Opportunities to Advance Privacy Enhancing Technologies

The App Association and the Innovators Network Foundation (INF) serve as principal resources in the privacy space for thought leadership, advocacy, and education for the global small business technology developer community.[6] We regularly work to keep our members up to speed on the latest policy and legal developments and to translate those into practical and usable guidance to ease the burden of compliance.[7] Furthermore, through our INF Privacy Fellowship, we support thought leadership that covers a wide range of privacy issues, including privacy enhancing technologies.[8]

We encourage OSTP to look to existing work from the privacy fellows and other leading academics on this topic as it conducts further research on PETs. For example, The Rise of Privacy Tech is an organization led by INF Privacy Fellow Lourdes Turrecha that serves as a leading conduit for startups in the privacy technology space to connect with funders, peers, and mentors in the industry and to catalyze privacy tech innovation. Recently, The Rise of Privacy Tech published its landscape analysis, "Defining the Privacy Tech Landscape," which included a full cataloguing of the different technologies that encompass privacy tech, including PETs (noting that PETs are a subset under the

---

[4] Office of the Privacy Commissioner of Canada, "Privacy Enhancing Technologies – A Review of Tools and Techniques", November 2017,"https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/

[5] U.S. House of Representatives, "Promoting Digital Privacy Technologies Act", Sec. 2, February 4, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/224/text.

[6] ACT | The App Association, Innovators Network Foundation Announces Inaugural Privacy

Fellows (September 2019), available at: https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/; Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection and Commerce, 117 Cong. (2022) (Statement of Graham Dufault, sr. dir. for public policy, ACT | The App Assoc.), *available at* https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Dufault_CPC_2022.06.14_0.pdf.

[7] See e.g., ACT | The App Association, General Data Protection Regulation Guide (May 2018), available at: https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf; What is the California Consumer Privacy Act (January 2020), available at: https://actonline.org/wp-content/uploads/What-is-CCPA.pdf.

[8] ACT | The App Association, Innovators Network Foundation Announces Inaugural Privacy Fellows (September 2019), available at: https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/

larger privacy tech umbrella).[9] Their investigation covered everything from key definitions and categorizing the different facets of the privacy tech stack, to a business analysis on the present and future of the privacy tech market.

Another privacy fellow, Dr. Lorrie Cranor, directs Carnegie Mellon's CyLab Security & Privacy Institute, which also conducts research at the cutting edge of certain PETs. For example, Dr. Cranor's scholarship on "privacy nutrition labels" has informed the rollout of similar labels on both of the major app platforms in recent months.[10] Dr. Cranor's research team has also been at the forefront of developing internet of things security labels,[11] machine extractable opt-out choices,[12] and privacy enhancing plug-ins for app developers.[13]

III. Specific Sectors, Applications, or Types of Analysis That Would Particularly Benefit from the Adoption of PETs

App developers are already working to adopt and implement PETs in their products, services, and features in order to meet market demands. Here are a few examples of PETs that our members rely on every day:

- On-device processing. Apps utilize on-device processing for certain sensitive features to ensure that no external processing occurs and that the company cannot see or access the data. To share one key use case, our members currently use facial verification technologies embedded at the platform level, such as Apple's Face ID, to allow users to login to apps using a scan of their face from the camera app. An app developer can choose integrate Apple's Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual's face (the gallery image) used to validate the comparison image

[9] The Rise of Privacy Tech, "Defining the Privacy Tech Landscape, November 2021, https://www.riseofprivacytech.com/wp-content/uploads/2021/11/TROPT-Defining-the-Privacy-Tech-Landscape-2021-v1.0-1.pdf

[10] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. ACM Press. https://doi.org/10.1145/ 1572532.1572538

[11] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal and L. F. Cranor, "Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?," *2021 IEEE Symposium on Security and Privacy (SP)*, 2021, pp. 519-536, doi: 10.1109/SP40001.2021.00112.

[12] Kumar et al., "Finding a Choice in a Haystack: Automatic Extraction of Opt-Out Statements from Privacy Policy Text". In WWW '20: The 2020 Web Conference, April 20–24, 2020, Taipei. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/1122445.1122456/.

[13] C Tianshi Li, Yuvraj Agarwal, and Jason I. Hong, Coconut: An IDE Plugin for Developing Privacy-Friendly Apps, Proc. ACM Interact Mob, Wearable Ubiquitous Technol, 2, 4, Article 178, December 2018 https://doi.org/10.1145/3287056

is stored within Apple's Secure Enclave on the device and is not available to the developer, Apple, or any other third party.[14]

- Encryption. The App Association supports fully leveraging technical measures including end-to-end encryption to protect data broadly, enabling key segments of the economy to function—from banking to national security to healthcare—by safeguarding access to, and the integrity, of data from unwanted interlopers. Encryption's role should not be understated – without encryption, entire economies and industries are put at a significantly heightened risk of their data being compromised. The importance of encryption to the app economy has only heightened during the COVID-19 pandemic and the increasing desire to perform traditionally offline functions in the digital space due to social distancing mandates. That's why we've been strong supporters of the National Institute of Standards and Technology's (NIST) efforts to support the development of encryption technologies, as well as their leadership in advancing risk-based scaled approaches to cybersecurity management in the NIST Cybersecurity Framework (which includes an emphasis on encryption as a technical protection mechanism), while opposing legislation seeking to undermine end-to-end encryption, such as the Lawful Access to Encrypted Data Act or the EARN IT Act.
- App Tracking Transparency. Even as federal lawmakers debate legislation that would put new guardrails around data sharing practices in the digital economy, app developers comply with a growing number of platform-level restrictions on certain types of data sharing with third parties. For example, Apple's App Tracking Transparency (ATT) tool creates a simple solution to the opt-in/opt-out binary by presenting users with a just-in-time push notification asking if they want to permit apps to track them across third-party tracking that follows them outside of the app onto the open web or even other third-party apps. This type of engineering solution has so far evaded an easy resolution in the policy world but has markedly improved user privacy outcomes along the way.[15] We have also raised the concern that antitrust measures that prohibit restrictions by platforms on access to personal data would likely prohibit ATT and undermine privacy by outlawing key PET developments by the market.[16] The development of PETs is too important to fall victim to proposals that impose blanket prohibitions on

[14] Apple, "About Face ID advanced technology", September 14, 2021, https://support.apple.com/en-us/HT208108

[15] Estelle Laziuk, "iOS 14.5 Opt-in Rate - Daily Updates Since Launch", Flurry (May 25, 2021), available at https://www. flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

[16] Graham Dufault, "Antitrust and Privacy Part 1: The Market for Privacy on Mobile Platforms," ACT | THE APP ASSOCIATION BLOG (Apr. 26, 2022), *available at* https://actonline.org/2022/04/26/antitrust-and-privacy-part-1-the-market-for-privacy-on-mobile-platforms/; Graham Dufault, "Privacy and Antitrust Part 2: What's Really At Stake if Congress Prohibits App Store Management?" ACT | THE APP ASSOCIATION BLOG (Apr. 27, 2022), *available at* https://actonline.org/2022/04/27/privacy-and-antitrust-part-2-whats-really-at-stake-if-congress-prohibits-app-store-management/.

access restrictions, especially at the platform level, and we hope that OSTP takes this consideration into account when evaluating antitrust measures.

- Privacy Labeling. Over the past few years, the app marketplace has seen the gradual introduction of the "privacy nutrition label" concept. The contemporary version of these labels (drawing from more than a decade of scholarship with researchers proposing similar concepts in various forms)[17] aims to perform a very simple function: make app developers' privacy practices more understandable to the average consumer. Initial research demonstrates that many app developers welcome privacy nutrition labels as a convenient, efficient, and user-friendly way for them to demonstrate their privacy practices and see it as a major improvement from the previous practice of directing users to lengthy privacy policies for similar information.[18] Though we believe the app platforms could do a better job of assisting developers in the creation and maintenance of the label, we believe the concept will help to maintain trust in the app ecosystem in the long run.

IV. Specific Laws that Could be Used, Modified, or Introduced to Advance PETs

The App Association has long-supported the passage of comprehensive federal privacy legislation that sets a strong baseline of consumer protection and creates legal certainty for American businesses. The App Association believes such legislation will naturally serve as a vehicle for incenting PETs as regulated entities look to comply with new requirements and ultimately compete on pro-privacy business practices. Recently, a bipartisan and bicameral group of lawmakers introduced a bill, the American Data Privacy and Protection Act (H.R. 8152) that we believe is the strongest effort at federal privacy legislation in years. Last month, the Energy & Commerce Committee's Consumer Protection & Commerce Subcommittee invited the App Association to testify on the bill, which was subsequently marked up and approved by the Subcommittee.[19]

While seemingly neutral on precise categories or applications of PETs, the legislation would incent their advancement in several ways. First, the bill states that service providers and third parties "have the same responsibilities and obligations as a covered

[17] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. ACM Press. https://doi.org/10.1145/ 1572532.1572538

[18] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA. ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3491102.3502012

[19] Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection and Commerce, 117 Cong. (2022) (Statement of Graham Dufault, sr. dir. for public policy, ACT | The App Assoc.), *available at* https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Dufault_CPC_2022.06.14_0.pdf.

entity with respect to [covered] data under all provisions of this Act."[20] One PET relevant to this requirement is the practice of data tagging, where a data controller tags a consumer's personally identifiable information with that user's data processing preferences as indicated in responses to the company's privacy policy or via specific data access requests. The tagged data elements can then be passed along with the appropriate instructions to service providers or other third parties in the data processing chain. Second, the bill's provision that covered entities "shall not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate" will also incent the development of PETs that facilitate data minimization.[21] Examples of relevant PETs include differential privacy, secure multi-party computation, zero-knowledge proofs, edge computing, and local or on-device processing. Finally, Section 103, "Privacy by Design," while not requiring covered entities to utilize specific PETs, will incent them to invest in PETs in order to satisfy their broad responsibility to "mitigate privacy risks, including substantial privacy risks, related to the products and services of the covered entity or the service provider, including their design, development, and implementation."[22] Moreover, under this section, the Federal Trade Commission would gain the authority to further opine on "what constitutes reasonable policies, practices, and procedures," which could include guidance on the use of specific PETs.

V. **Conclusion**

The App Association appreciates OSTP's consideration of the above views. We urge OSTP to contact the undersigned with any questions or ways that we can assist moving forward.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Matthew Schwartz
Public Policy Associate

[20] American Data Privacy and Protection Act (H.R. 8152), Sec. 302, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[21] Ibid. Sec. 101.

[22] Ibid. Sec. 103 (a)(3).

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005