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

Computer & Communications Industry Association (CCIA)

Before the
Office and Science and Technology Policy
Washington, D.C.

In re	
Request for Information on Advancing Privacy-Enhancing Technologies	Document Number 2022-12432

COMMENTS OF

THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Request for Information ("RFI") published in the Federal Register at 87 Fed. Reg. 35250 (June 9, 2022), the Computer & Communications Industry Association ("CCIA")[1] submits the following comments to the Office of Science and Technology Policy ("OSTP"):

I. Introduction

CCIA is pleased to provide comment on how the federal government can not only facilitate but encourage implementation of Privacy-Enhancing Technologies ("PETs") for employing and transferring data, particularly the data of consumers and Internet users.

Privacy is best secured through anonymization, a goal that might never fully be reached, or, if reached, would strip data of all utility. PETs, most notably differential privacy, are the best alternative to anonymization. Rather than attempt data de-identification, which is increasingly difficult and susceptible to reverse-engineering, PETs enable data minimization. But, as the RFI notes, PETs are not yet widely adopted.

Though the United States presently lacks a federal privacy statute of general application, many of our federal agencies presently are authorized to adopt consumer-protection measures focused on data privacy and security. In addition, within any federal privacy legislation that it takes up in the future, Congress could consider creating safe harbors, and possibly exemptions,

[1] CCIA is a nonpartisan, not-for-profit trade association. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A complete list of CCIA members is available at http://www.ccianet.org/members.

when PETs are in use. The federal government might be best suited to creating incentives that will make PETs commonplace tools for protecting consumer privacy.

II. How PETs Maximize the Benefits of Data While Minimizing Risk

The central question in privacy analysis is how much specificity of information the data user is willing to forego versus how much security the data owner one wants to preserve. Historically the risk-reward tradeoff in data privacy could be plotted as a straight line between no access/zero risk and full access/unlimited risk. Where a particular data policy fell between those points was a function of operations that were largely manual – truncating Social Security numbers and data deletion, for instance. Experience has shown that such measures are neither scalable nor reliable.

Previously the strategy for securing data was anonymization through "injecting noises into the original data," like blurring a photograph, which obscures much of the original data in order to render the data set de-identified.[2] But, like a blurred photograph, "the more protection there is, the less useful the released data are."[3] PETs have shifted the paradigm of choosing between data utility and data security. They have significantly lowered the baseline of risk associated with handing over one's data and made the incremental increases of risk much smaller. PETs have introduced machine learning (artificial intelligence) into data security, which "has the power to reveal information that would not be obvious to a human evaluating a dataset unassisted."[4]

A. Forms of PET.

Forms of PET include differential privacy and federated learning. Differential privacy, or "DP", defines privacy as a matter of mathematical probability rather than an absolutist question whether data does or does not correspond to a particular individual. DP can be described as "a privacy-protecting layer between raw data and a user of the data."[5] It thus provides responses to queries without "enough information to identify any individual included in the dataset."[6] DP is

---

[2] Fang Liu, Ph.D., A Statistical Overview on Data Privacy, 34 Notre Dame J.L. Ethics & Pub. Pol'y 477, 478 (2020).
[3] Fang Liu, *supra* n.2, at 478.
[4] Andrea Scripa Els, Artificial Intelligence as a Digital Privacy Protection, 31 Harvard J.L. & Tech. 217, 218 (2017).
[5] Anna Myers & Grant Nelson, Differential Privacy: Raising the Bar, 1 Geo. L. Tech. Rev. 135, 137 (2016).
[6] Andrea Scripa Els, *supra* n.4, at 220.

considered "state of the art" in privacy protection, because it cannot be reverse-engineered – DP does not reveal data, but rather it reveals the result of machine-learning decisions about data.[7]

Federated learning is a process that uses AI to import small sets of data from users into the cloud, then immediately aggregate and average those sets with other users' sets in a centralized learning model. No one user's data is stored uniquely, but rather it uses a "collaborative learning method" to "train" an AI model on answering questions via supplied data.[8] These "meta-updates," so-called,[9] are the data sets against which a specific algorithm is applied to answer one particular question, which further ensures that identifiable consumer data is not exposed.

Another type of PET is multi-party computational privacy ("MPC"). This method permits users to share query outcomes without sharing the individual data inputs. Its first known usage was in 2008, when an auction was designed in Denmark to find the market-clearing price for sugar beets.[10] Beet farmers wanted their individual pricing structures to remain confidential, but all agreed that the market-clearing price should be publicly available. MPC enables this analytical scenario by using encryption to essentially create an electronic bailiff for data inputs,[11] allowing third parties to access only query outcomes.

B. Existing Applications of PETs.

Apple and Google already use DP in their respective mobile operating systems. Apple built DP into iOS 10 for all data collection and uses it for improving pre-installed applications like Notes and the keyboard.[12] Google, credited with developing federated learning, uses it for word recommendations in the Android keyboard and possibly soon for ranking photos and modeling language.[13] In addition, IBM and Uber have released open-sourced libraries for

---

[7] *See* Fang Liu, *supra* n.2, at 482; *see also* Andrea Scrips Els, *supra* n.4, at 221.
[8] Micah J. Sheller, *et al*., Federal learning in medicine: facilitating multi-institutional collaborations without sharing patient data, Scientific Reports 10:12598, at p.2 (2020).
[9] Andrea Scrips Els, *supra* n.4, at 223.
[10] Multi-Party Computation: Private Inputs, Public Outputs, Forbes.com (Oct. 26, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/10/26/multi-party-computation-private-inputs-public-outputs/?sh=403c70521bb0.
[11] *See* Multiparty computation as supplementary measure and potential data anonymization tool, IAP (Oct. 27, 2021), https://iapp.org/news/a/multiparty-computation-as-supplementary-measure-and-potential-data-anonymization-tool/.
[12] Andrea Scrips Els, *supra* n.4, at 221; Fang Lui, *supra* n.2, at 486.
[13] Andrea Scrips Els, *supra* n.4, at 223; Fang Lui, *supra* n.2, at 486.

experimenting with various DP applications.[14]

The U.S. Census Bureau adopted DP in 2018 to protect publications of data and statistics developed from the 2020 Census.[15] Called the Disclosure Avoidance System ("DAS"),[16] this technology relies on algorithms borrowed from 1965 Voting Rights Act enforcement – more specifically, drawing legislative districts – to "efficiently distribute the noise injected by differential privacy."[17] The Bureau published a handbook describing DAS and outlining the increased risks of data disclosure that caused it to adopt DP technology for the first time.

III. How the U.S. Government Can Foster PET Adoption and Innovation

Although PETs are substantially automated through reliance on AI, they nonetheless entail great cost.[18] DP requires several processes to establish a privacy layer that is exactly porous enough to enable the user to answer questions while preserving the pristine raw data. Federated learning requires creation of theoretically infinite meta-updates, one for each question that can ever be asked, constructed from the point of collection. Presently, due largely to the absence of a uniform and final set of privacy regulation, there is no external incentive for developing and deploying these technologies. There are neither guideposts nor rewards for privacy technology. CCIA urges OSTP to establish, or recommend the establishment of, PET incentives.

A. PETs Can Be Expressly Incorporated Into Existing Federal Regulations.

Many federal agencies already have regulatory vehicles for encouraging the development and use of PETs. The Federal Trade Commission can review PETs in the context of its Section 5 authority to protect consumer privacy. In addition, and as the RFI notes at Paragraph 4, adding PETs as a criterion for selection under the Federal Acquisition Regulations could be a meaningful incentive for deployment. Additional regulatory applications can include making PETs a required component of data-breach notifications: the disclosing entity could be required

---

[14] Fang Lui, *supra* n.2, at 486.
[15] John M. Abowd, The U.S. Census Bureau Adopts Differential Privacy, Ass'n for Computing Machinery (July 19, 2018), https://dl.acm.org/doi/10.1145/3219819.3226070.
[16] U.S. Census Bur., Processing the Count: Disclosure Avoidance Modernization, https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance.html.
[17] John M. Abowd, *supra* n.15.
[18] Jonathan Mayer and Arvind Narayanan describe several impediments to adopting what they term "privacy substitutes" in their paper Privacy Substitutes, 66 Stan. L. Rev. Online 89 (2013-14).

to state whether any PETs were in use for the data believed to have been compromised, and if so, how those technologies might mitigate the risk that the unlawfully obtained data could harm any consumers.[19]

The FTC's rulemaking authority seems a particularly appropriate tool for incentivizing PETs at this time. American industry needs guidance on how PETs can be incorporated into their various business models. The FTC has expertise in collecting and harmonizing technological solutions for preserving privacy. An FTC proceeding devoted to assessing the feasibility and efficacy of DP, federated learning, and other forms of PET would give businesses the confidence to choose and implement privacy technologies that will benefit consumers.

A good deal of scholarship has arisen on how PETs can be used to comply with the Family Educational Rights and Privacy Act of 1974 (FERPA)[20] and the privacy laws that govern healthcare information.[21] Education and health care both rely on personal data, within the context of larger sets of data, to make decisions that deeply affect an individual's life. And FERPA in particular protects not only PII (personally identifiable data) but also statistics built from PII.[22] DP is well suited to enabling access to large data sets through the protective layer of targeted machine learning. Thus, the Department of Education and the Department of Health and Human Services might consider releasing guidance on implementing PETs as a means for privacy compliance within their respective data regimes.

B. Federal Agencies Can Advise Congress on Including PET Safe Harbors and Exemptions in Privacy Legislation.

In recent weeks, Congress has displayed a renewed interest in federal privacy legislation. This past June, H.R. 8152, the American Data Privacy and Protection Act, was given a hearing and a markup in the House Consumer Protection Subcommittee, and Senator Cantwell has

---

[19] Examples of data-breach notification rules include the Consumer Proprietary Network Information (CPNI) rule for customer notifications, 47 C.F.R. § 64.2011, the forthcoming Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rules, and the Health Insurance Portability and Accountability Act Breach (HIPAA) Notification Rule, 45 C.F.R. §§ 164.400-.414.

[20] *E.g.*, Kobbi Nissim, *et al.*, Bridging the Gap Between Computer Science and Legal Approaches to Privacy, 31 Harvard J.L. & Tech. 687 (2018).

[21] *E.g.*, Micah J. Sheller, *et al.*, *supra* n.8; *see also* Mirko Forti, The Deployment of Artificial Intelligence Tools in the Health Sector: Privacy Concerns and Regulatory Answers within the GDPR, 13 Eur. J. Legal Stud. 29 (2021). The need for technologically assured patient privacy is a chief inhibitor of moving toward healthcare information portability. W. Nicholson Price II, Ph.D., Risk and Resilience in Health Data Infrastructure, 16 Colo. Tech. L.J. 65, 71-73 (2017).

[22] Kobbi Nissim, *et al.*, *supra* n.15, at 722.

introduced a slightly different privacy bill in S.3195, the Consumer Online Privacy Rights Act. It is expected that privacy will receive even greater attention in the next Congress. This activity provides a significant opportunity for encouraging PET innovation and adoption.

Expert agencies like OSTP can advise Congress on the technologies available for collecting and using consumer data in a responsible manner. More than that, they can work with Congress to establish statutory incentives, like safe harbors and exemptions, centered on PETs. A federal privacy statute can, in a technologically neutral way, encourage the use of reliable automation to protect individual data. In this way, federal privacy legislation would become a means of, as one professor put it, "recoding privacy law" to become a solution and not merely a punitive tool.[23]

IV. Conclusion

CCIA applauds OSTP's constructive approach to securing consumer data through technological innovation. Encouraging the adoption of PETs through existing federal regulation would be a meaningful way to preserve privacy and data security as we await the enactment of a federal legislative solution spurring adoption through statutory incentives.

Respectfully submitted,

Stephanie A. Joyce
Chief of Staff and Senior Vice President
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001

July 8, 2022

[23] *See generally* Urs Glasser, Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy, 130 Harvard L. Rev. F. 61 (2016).