SIIA
POLICY

Comments of the Software & Information Industry Association (SIIA) on the Request for Information on Advancing Privacy-Enhancing Technologies

Submitted to the Office of Science and Technology Policy and the Fast Track Action Committee on Advancing Privacy-Preserving Data Sharing and Analytics of the Subcommittee on Networking and Information Technology Research and Development

August 2022

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide input on the Request for Information on advancing privacy-enhancing technologies (PETs).[1]

Introductory Comments

SIIA, a non-profit organization, is the principal trade association for the software and digital information industries worldwide. Our over 450 member companies reflect the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions globally, and companies specializing in data analytics and information services. We count among our membership companies on the cutting edge of PETs development and use.

We strongly support the U.S. government's effort to develop a national strategy on privacy-preserving data sharing and analytics. We share the government's optimism about the potential for PETs to address critical challenges around data sharing, collaboration, and analysis in a multitude of areas, including cross-border data transfers, financial crime detection, health care research, and others.[2] SIIA has steadfastly supported the development and adoption of PETs. In the past year, we have championed PET-related programs in submissions to federal agencies on digital policy development and in our recommendations to U.S. and European Commission officials leading up to the May 2022 meeting of the U.S.-EU Trade and Technology Council (TTC).

There is growing momentum for advancing PETs in the United States and abroad. For example, the White House National Economic Council and Department of Transportation announced a collaboration to use PETs to expedite and streamline the movement of goods in the supply chain

[1] Office of Science and Technology Policy, Request for Information on Advancing Privacy-Enhancing Technologies, 87 Fed. Reg. 35250 (June 6, 2022).

[2] See, e.g., The Center for Data Ethics and Innovation, "PETs Adoption Guide: Repository of Use Cases," https://cdeiuk.github.io/pets-adoption-guide/repository/; Kaitlin Asrow and Spiro Samonos, Federal Reserve Bank of San Francisco, "Privacy Enhancing Technologies: Categories, Use Cases, and Considerations" (June 2021), https://www.frbsf.org/banking/publications/fintech-edge/2021/june/privacy-enhancing-technologies/; Luis T.A.N. Brandao and Rene Peralta, NIST Differential Privacy Blog Series, "Privacy-Enhancing Cryptography to Complement Differential Privacy" (Nov. 3, 2021), https://www.nist.gov/blogs/cybersecurity-insights/privacy-enhancing-cryptography-complement-differential-privacy.

ecosystem, which is expected to reduce delays and costs for American consumers. [3] This energy complements growing global interest. The TTC has announced work towards a common project on PETs.[4] The U.K. Information Commissioner's Office is exploring guidance on PETs and ways to incorporate PETs into data regulations. The United Nations has launched a "PETs Lab" to test PETs against data sets from the United States, the U.K., Canada, Italy, and the Netherlands, and work with researchers and the private sector to develop use cases and create guidance.[5] Singapore has recently launched a Digital Trust Centre along with a PET Sandbox to pilot PETs and facilitate data sharing and analytics.[6]

Further adoption of PETs can be an essential part of a democratic model of emerging technology in practice, as a counter to a model that sacrifices privacy, trust, safety, and transparency.[7] PETs can enable the secure sharing of data between entities and across jurisdictional boundaries, expanding data access and utility and enabling organizations to reduce risk while making faster, better-informed decisions.[8] As the White House stated in announcing the new U.S.-U.K. prize challenge, PETs "present an important opportunity to harness the power of data in a manner that protects privacy and intellectual property, enabling cross-border and cross-sector collaboration to solve shared challenges."[9]

[3] White House, Readout of Supply Chain Event: Launching Data Initiative for Greater Supply Chain Resilience (Mar. 15, 2022).

[4] U.S.-EU Joint Statement of the Trade and Technology Council (May 16, 2022), at ¶¶ 14, 19, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/16/fact-sheet-u-s-eu-trade-and-technology-council-establishes-economic-and-technology-policies-initiatives/.

[5] United Nations, "UN launches first of its kind 'privacy lab' to unlock benefits of international data sharing" (Jan. 25, 2022), https://unstats.un.org/bigdata/events/2022/unsc-un-pet-lab/UN%20PET%20Lab%20-%20Press%20Release%20-%2025%20Jan%202022.pdf.

[6] Singapore Personal Data Protection Commission, "Launch of Privacy Enhancing Technologies Sandbox" (Jul. 20, 2022), https://www.pdpc.gov.sg/news-and-events/announcements/2022/07/launch-of-privacy-enhancing-technologies-sandbox; Singapore Infocomm Media Development Authority, "Singapore grows trust in the digital environment" (June 1, 2022), https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2022/Singapore-grows-trust-in-the-digital-environment.

[7] Andrew Imbrie, et al., "Privacy Is Power: How Tech Policy Can Bolster Democracy," *Foreign Affairs* (Jan. 19, 2022), https://www.foreignaffairs.com/articles/world/2022-01-19/privacy-power.

[8] Two use cases involving SIIA members will help to illustrate this point. First is a partnership between Enveil (an SIIA member) and DeliverFund, the leading counter-human trafficking intelligence organization, which leveraged Enveil's PETs-powered solutions to accelerate reach and efficiency by allowing users to securely and privately screen existing assets at scale by cross-matching and searching across DeliverFund's extensive data. Second is Meta's use of secure multi-party computation, on-device learning, and differential privacy tools to minimize the amount of data collected in the advertising space while ensuring that personalized content reaches end users.

[9] White House Office of Science and Technology Policy, "US and UK to Partner on Prize Challenges to Advance Privacy-Enhancing Technologies" (Dec. 2021), https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/; *see also* White House, Remarks of Jake Sullivan (July 13, 2021), https://www.whitehouse.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit/.

Comments on Topic 4: Specific regulations or authorities that could be used, modified, or introduced to advance PETs

Amend FinCEN Regulations to Incentivize PETs Adoption

We encourage the national strategy to include recommendations on regulatory reform to promote the adoption of PETs in data sharing, analysis, and collaboration to detect and address suspicious financial activity and improve compliance with U.S., foreign, and international laws. We focus on the financial activity space for several reasons. First, as demonstrated in a growing literature and pilot projects undertaken globally, PETs have proven effective in the detection, reporting, compliance, and remediation of suspicious financial transactions associated with money-laundering, corruption, human trafficking, and other illicit activities.[10] Second, government authorities have already begun to examine how PETs can help to improve detection of suspicious activity. Third, the U.S. government has made this application of PETs a priority, as demonstrated in the Summit for Democracy and the U.S.-U.K. prize challenges on PETs.

Nevertheless, despite these data points and considerable advances in PETs in recent years, widespread adoption of PETs has not occurred in the financial sector. A key reason for this is the asymmetry between technological capability and regulatory frameworks. Legal and regulatory regimes proscribe uses and transfers of personal and financial information to maintain confidentiality and privacy. There are numerous challenges in this space. These are reflected, for example, in a recent report by the Financial Action Task Force (FATF), an independent, inter-governmental body.[11] In connection with the U.S.-U.K. prize challenge, the White House cited the FATF report for its finding that "uncertainty about the regulatory implications of using these technologies is a significant barrier to adoption."[12]

The FATF report describes many such barriers. Particularly relevant are barriers created by limitations in the applicable legal and regulatory frameworks. Legal frameworks governing anti-money laundering (AML), combatting the financing of terrorism (CFT), and other areas (such as anti-corruption and sanctions compliance) require internal controls but do not incentivize or require firms to adopt advanced technologies to improve the identification of suspicious activity through data sharing and analysis that protects the privacy and confidentiality of the underlying data. Moreover, confusion about the complex data protection and privacy (DPP) rules, especially in the cross-border context – even within

[10] See, e.g., RUSI and FFIS, "Case studies of the use of privacy preserving analysis to tackle financial crime" (Jan. 2021), https://www.future-fis.com/the-pet-project.html; The Royal Society, "Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis" (Mar. 2019), https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf; European Union Agency for Cybersecurity, "Privacy enhancing technologies," https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies; U.K. Financial Conduct Authority, "2019 Global AML and Financial Crime TechSprint" (July 2019), https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint.

[11] *See* Financial Action Task Force, "Stocktake: Datapooling and Collaborative Analytics," at ¶¶ 53-67, 70-72, https://www.fatf-gafi.org/media/fatf/documents/Stocktake-Datapooling-Collaborative-Analytics.pdf.

[12] White House, "U.S. and U.K. Governments Collaborate on Prize Challenges to Accelerate Development and Adoption of Privacy-Enhancing Technologies (June 13, 2022), https://www.whitehouse.gov/ostp/news-updates/2022/06/13/u-s-and-uk-governments-collaborate-on-prize-challenges-to-accelerate-development-and-adoption-of-privacy-enhancing-technologies.

the same organization – disincentivize the use of advanced technological tools: the potential for non-compliance with DPP laws outweighs the potential for increased compliance with financial activity regulations.[13]

Government financial authorities in the United States and the U.K. appear to recognize the potential that PETs as a class can contribute to improving detection, reporting, compliance, and remediation. The new U.S.-U.K. prize challenge and other efforts emanating from the Summit for Democracy, along with discrete efforts in both the United States and the U.K., demonstrate increased attention on the potential of PETs to address pressing challenges. This is in addition to promising efforts underway in other jurisdictions globally. (Later in this submission we touch on efforts by Singaporean and U.K. governments that serve as models for recommendations in the national strategy.)

We encourage OSTP and the interagency FTAC to include in the national strategy concrete recommendations to operationalize these efforts by creating regulatory drivers for financial firms to adopt PETs that are deployment ready. To achieve this, we recommend amendments to FinCEN regulations at 31 CFR Chapter X. The regulations in Chapter X implement portions of the Bank Secrecy Act (BSA) and govern how covered financial institutions must record and report suspicious activities.[14] Under current law, covered financial institutions are required to maintain records, file reports, and report suspicious activity that could indicate criminal conduct (such as money laundering, tax evasion, or terrorist financing). They are required as well to maintain policies, procedures, and internal controls to enable the detection, reporting, and remediation of suspicious activity.[15] The rules in Chapter X include requirements and restrictions related to data sharing and the use of data maintained by financial institutions, along with financial penalties for non-compliance and for maintenance of inadequate internal controls.

Building on the work that FinCEN has begun through its Innovation Hours program and a January 2022 notice of proposed rulemaking,[16] we recommend that OSTP and the FTAC consider the following recommendations in the national strategy.

- *Incorporate PETs into the FinCEN pilot program under 31 USC 5318(g)(8).*

Earlier this year, FinCEN issued a notice of proposed rulemaking (NPRM) to establish a pilot program pursuant to 31 USC 5318(g)(8), added by section 6212(a) of the Anti-Money Laundering Act of 2020.[17] The pilot program would permit "financial institutions with a SAR reporting obligation to share SARs and related information with foreign branches, subsidiaries, and affiliates for the purpose of

[13] See, e.g., supra note 11 at ¶¶ 57, 71, 72.

[14] See 12 USC 1829b, 12 USC 1951-19600, 31 USC 5311-5314, 5316-5336, and 31 CFR Chapter X.

[15] See, e.g., 31 CFR 1020.210 (anti-money laundering program requirements for covered banks); 31 CFR 1020.220 (customer identification program requirements for covered banks).

[16] Department of the Treasury, Financial Crimes Enforcement Network, "Pilot Program on Sharing of Suspicious Activity Reports and Related Information With Foreign Branches, Subsidiaries, and Affiliates," 87 Fed. Reg. 3719 (Jan. 25, 2022).

[17] Enacted as Division F, sections 6001-6511 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116-283, 134 Stat 3388 (2021).

combatting illicit finance risks."[18] As proposed by FinCEN, the pilot program would require financial institutions to implement internal controls beyond those already required by law in order to ensure the confidentiality of information and comply with U.S. and foreign law. The pilot program would be an ideal vehicle to deploy PETs to undertake secure data sharing across jurisdictions within financial institutions.

- *Encourage FinCEN to pursue rulemaking to amend provisions of Chapter X to permit greater data sharing across firms, between firms, and between firms and the government if done with PETs.*

In addition, we recommend FinCEN explore rulemaking to incorporate PETs into the guidelines for data sharing under 31 CFR 1010.520 (information sharing between financial institutions and government agencies) and 31 CFR 1010.540 (voluntary information sharing among financial institutions).

These data sharing measures require financial institutions to maintain confidentiality and security of data. Advancements in the PET space can enable financial institutions to do so with greater confidence, potentially increasing the quality of data shared as well as the confidentiality of customer information relevant to that data. We would encourage the national strategy to recommend that FinCEN amend these rules to require use of PETs, where feasible, to incentivize their adoption. This would lead to increased data sharing without materially increasing the risk to confidentiality of underlying financial data.

- *Encourage FinCEN to pursue rulemaking to amend requirements for AML and customer identification (CID) requirements.*

FinCEN regulations govern both AML and CID program requirements for banks and other financial institutions. These program requirements differ depending on the type of financial institution. For banks, the relevant rules are contained at 31 CFR 1020.210 (AML) and 31 CFR 1020.220 (CID).

As noted above, pilot projects and proofs of concept in the financial services space have demonstrated an increased ability to identify potentially suspicious transactions without revealing confidential information by incorporating different types of PETs.[19] Requiring use of PETs as part of the "system of internal controls" required by the AML and CID rules would create a regulatory driver for banks to adopt PETs and improve their ability to detect financial crime. We would further recommend that use of PETs be required (or incentivized) as part of the due diligence program requirements at 31 CFR 1020.610 and 31 CFR 1020.620.

- *Encourage FinCEN to update its Bank Secrecy Act enforcement guidelines to consider PET adoption as a factor to consider in enforcement decisions.*

Violations of the Bank Secrecy Act may result in civil and/or criminal penalties. Civil penalties are imposed by the Department of the Treasury through authority delegated to FinCEN. Criminal

[18] Supra note 16 at 3721, 3725.

[19] See, e.g., RUSI and FFIS, supra note 10.

penalties are imposed by the Department of Justice (DOJ).[20] Creating incentives in the structure of the penalty rules and guidelines could encourage firms to adopt PETs in their AML and CID programs.

We recommend that FinCEN and DOJ consider policy guidance to encourage financial institutions to adopt PETs in their AML CID programs. Amending the underlying statutes is not practicable given the design of those provisions; they authorize the imposition of penalties, provide legal standards, and establish penalty caps. Likewise, the applicable regulations implementing those statutes do not detail factors that authorized officials may consider in exercising discretion. Yet both FinCEN and the DOJ have issued policy guidance to inform the public about discretionary factors. Amending this guidance to include usage of PETs in internal controls and compliance programs could prove effective in encouraging adoption in the financial sector.[21]

Amend Privacy Act regulations to increase data sharing and analysis in the federal government

The recommendations addressed above would help in driving adoption of PETs in the financial sector. PET adoption in other sectors would benefit from attention to other regulatory impediments. While there are many, we provide feedback on one measure to improve data sharing and analytics within the U.S. federal government. The Privacy Act of 1974, as amended, 5 USC 552a, governs how the federal government can use information that it collects on U.S. persons. The advent of PETs can enable federal agencies to make greater use of personal information without increasing the material risk of improper disclosure. We encourage OSTP and the FTAC to consider recommending that federal agencies update the routine uses in their system of records notices to include additional uses made possible without compromising personal information by incorporating approved PETs. We also encourage adoption of a recommendation to enable more robust use of matching programs under 5 USC 552(a)(8) to allow federal agencies to engage in matching programs using PETs that can generate insight for policy development without compromising personal information.

Comments on Topic 5: Specific laws that could be used, modified, or introduced to advance PETs

There are countless ways in which new laws could advance the adoption of PETs. For example, the Promoting Privacy Technologies Act (H.R. 847),[22] which recently passed in the House of Representatives, would assist in promoting fundamental research into PETs. Likewise, the recently enacted CHIPS And Science Act of 2022 contains measures to support efforts of the National Institute of Standards and Technology (NIST) to advance PETs.[23] The government has a critical role to play in

[20] See 31 USC 5321-5322, 31 CFR 1010.820, and 31 CFR 1010.840.

[21] For FinCEN enforcement guidelines, see "Financial Crimes Enforcement Network (FinCEN) Statement on Enforcement of the Bank Secrecy Act," https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf. FinCEN may consider cooperation and remediation in determination about whether to assess penalty at maximum amount. See, e.g., *In the Matter of: Capital One, National Association, McLean, Virginia*, No. 2021-01, Assessment of Civil Money Penalty at 19 (Jan. 15, 2021), https://www.fincen.gov/sites/default/files/enforcement_action/2021-01-15/Assessment_CONA%20508_0.pdf.

[22] Promoting Digital Privacy Technologies Act, H.R.847 (117th Cong.).

[23] CHIPS and Science Act of 2022, H.R. 4346 (117th Cong.), §§ 10223 (privacy and cybersecurity), 10226 (biometrics), 10232 (artificial intelligence). Signed into law on August 9, 2022.

fostering fundamental research – especially in areas, such as PETs, where robust markets have yet to develop. Efforts such as this would stimulate further momentum around PETs. In addition, it is important to fund initiatives that go beyond research as many of these technologies are ready for use at scale today.

With our focus on advancing the adoption of already deployable PETs, we encourage the national strategy to identify ways that PETs can be incorporated into existing or new privacy, cybersecurity, and safety laws (or into regulations that implement those laws).

Advance PETs in General Purpose Privacy Legislation

The GDPR and other new privacy regimes have helped to foster increased attention in PET capabilities abroad. Official action by the U.S. government can have a similar effect and lead to the development and use of PETs designed to address critical needs around private and secure data usage – enhancing innovation in the United States and helping to drive behavior globally. PETs can also help to drive up compliance with a range of laws and regulations in ways not possible when those laws and regulations were drafted.

PETs can have a role in realizing the objectives of general-purpose consumer privacy legislation. Legislation and bills at the federal and state level in the United States often require covered entities to take steps to implement privacy by design frameworks and to pursue data minimization. In addition, there are often carve outs for data that has been anonymized or de-identified, despite well documented challenges in achieving true anonymization or de-identification.

As an example, the recently introduced American Data Protection and Privacy Act (ADPPA)[24] would require covered entities to implement policies, practices, and procedures to achieve "privacy by design," require additional measures to further data minimization, and permit uses of data that is sufficiently de-identified. PETs provide a means to achieve these objectives with significantly less risk to personal privacy. While there may not be an opportunity to incorporate PET adoption into the legislative text of the ADPPA, we encourage the national strategy to recommend that PETs be incorporated into future federal privacy bills (assuming the ADPPA does not become law) and implementing regulations on the ADPPA or any other federal privacy bill signed into law.[25]

In addition, PETs can help to achieve data deidentification or anonymization that is required by state privacy laws to render data usable in different, productive ways. California's privacy law, for example, allows businesses to avoid stringent obligations if data is de-identified.[26] To establish de-identification, a business must meet several criteria, including "reasonable measures to ensure that the information cannot be associated with a consumer or household." This factor proves challenging to meet from a technical perspective and there are well documented concerns around the ability to re-identify

[24] Amendment in the Nature of a Substitute to H.R. 8152 (117th Cong.) (Jul. 20, 2022).

[25] The ADPPA would direct the Federal Trade Commission, in consultation with other agencies such as NIST, to develop appropriate implementing regulations.

[26] Cal. Civ. Code sec. 1798.140(o)(m) (effective Jan. 1, 2023).

previously deidentified data. Similar concerns arise in compliance with state laws that contain provisions on pseudonymous data, such as Virginia and Colorado.[27]

Establish a Centralized Data Center to Support Development of PET Applications and Enable More Robust Data Analysis Using PETs

The RFI references proposed legislation to create a National Secure Data Service (NSDS) as one potential method to advance PETs. The CHIPS and Science Act of 2022, passed by both houses of Congress and signed into law on August 9, 2022, authorizes the NSF Director to establish the NSDS as a demonstration project with funding authorized through fiscal year 2027.[28] The NSDS will enable the collection, analysis, and dissemination of data from federal and state agencies (on a voluntary basis) to support government-side evidence-building activities. Executing this mission will require use of PETs to maintain confidentiality of data from government sources and may prove fruitful as a testbed for new PET applications. We support the overall objectives of this proposal.

In addition, we recommend that the national strategy explore ways to include PET-focused activity in the National Artificial Intelligence Research Resource (NAIRR).[29] As the FTAC knows, the NAIRR Task Force has issued an interim report and is working on a final report to provide Congress and the executive branch with a roadmap to establish the NAIRR "as a shared computing and data infrastructure that will provide AI researchers and students across scientific fields and disciplines with access to compute resources and high-quality data, along with appropriate educational tools and user support."[30] Incorporating a PETs-focused data center into the NAIRR framework will provide an additional means to pilot PET projects and cultivate new PET applications.

Comments on Topic 6: Specific mechanisms, not covered above, that could be used, modified, or introduced to advance PETs

Continue to Prioritize International Cooperation

As noted above, SIIA is steadfast in our support for the U.S. government's efforts to coordinate on the research, development, deployment, and adoption of PETs with partners and allies. We support the efforts underway in the TTC, as part of the U.S.-Israel Strategic High-Level Dialogue on Technology, with the U.S.-U.K. prize challenge, in dialogue with other nations as part of the UN PETs Lab, and others. We encourage the National Strategy to devote attention to the international context as a discrete line of effort to encourage the adoption of PETs. This may include, for example, expanding the prize

[27] Privacy laws in Virginia and Colorado, for example, exempt "pseudonymous data" from rights of access, deletion, correction, and data portability.

[28] CHIPS and Science Act of 2022, at § 10375. Signed into law on August 9, 2022.

[29] See National Artificial Intelligence Initiative Office, "The National Artificial Intelligence Research Resources Task Force (NAIRRTF)," https://www.ai.gov/nairrtf/.

[30] See id.

challenge agencies in other countries as part of the Indo-Pacific Economic Framework for Prosperity (IPEF).[31]

Likewise, we recommend the national strategy advocate for the Administration to advance PETs as a means to bridge the gap between differential privacy regimes in the context of cross-border data flows. This should occur in connection with existing discussions around two critical arrangements announced earlier this year: the new Trans-Atlantic Data Privacy Framework, which would replace the Privacy Shield;[32] and the Global Cross-Border Privacy Rules Forum, which would establish an arrangement among Canada, Japan, the Philippines, Singapore, South Korea, Taiwan, and the United States.[33]

Consider a NIST-Run Certification Process

We also recommend that the national strategy propose that NIST establish a certification process to vet PETs as safe, secure, reliable, and accurate. We believe a certification process would be more effective than the development of standards. We are less sanguine about the need for standards to govern PETs than in other areas, such as standards to guide development of safe, secure, reliable, and accurate AI systems.[34] Standards can be a double-edged sword. On the one hand, technical standards provide baseline technical requirements to facilitate interoperability and assure the marketplace of product quality. On the other, technical standards in advanced software can have the effect of limiting innovation as technology continues to develop at a rapid pace. While the development and adoption of certain PETs may benefit from standardization, over reliance on standards for each type of PET could hinder further innovation.

We do, however, endorse something of a certification process that could be run by NIST. As the market for PETs continues to develop, market participants, who may lack the technical expertise to assess PETs on their own, would benefit from a neutral third party that could provide a stamp of approval on different technologies. NIST is well positioned to serve in this role and has years of expertise in PETs to

[31] White House, "FACT SHEET: In Asia, President Biden and a Dozen Indo-Pacific Partners Launch the Indo-Pacific Economic Framework for Prosperity" (May 23, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-in-asia-president-biden-and-a-dozen-indo-pacific-partners-launch-the-indo-pacific-economic-framework-for-prosperity/. The Administration has also made PET collaboration a focus of bilateral technology diplomacy, for example with Japan and Israel, another important avenue towards broader adoption. See, e.g., White House, "FACT SHEET: The U.S.-Japan Competitveness and Reslilience (CoRe) Partnership" (May 22, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-the-u-s-japan-competitiveness-and-resilience-core-partnership/; White House, "Joint U.S.-Israel Statement on Launching Strategic High-Level Dialogue on Technology" (July 13, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/13/joint-u-s-israel-statement-on-launching-strategic-high-level-dialogue-on-technology/.

[32] White House, "FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework" (Mar. 25, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

[33] U.S. Department of Commerce, "Global Cross-Border Privacy Rules Declaration" (Apr. 21, 2022), https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

[34] See, e.g., ISO/IEC JTC1/SC 42 – Artificial Intelligence, at https://www.iso.org/committee/6794475.html.

apply to this task. NIST can also help to establish common taxonomies for PETs. This project could build on the expanded authorities for NIST in section 10223 of the CHIPS and Science Act.

Incorporate PETs into Discourse and Policy Efforts around Responsible AI

The growing discourse on responsible AI and promising efforts to develop frameworks for assessing and assuring the safety, security, reliability, and accuracy of AI systems can be enhanced with attention to the ways that PETs can facilitate the end goals and – in addition – support "data for good" efforts. The literature on responsible AI is substantial and we would encourage work to embed discussion and projects around PETs into responsible AI activities underway in the U.S. interagency, the Global Partnership on Artificial Intelligence, and the OECD.

Consider Models for Advancing PETs in Other Technologically Advanced Nations

Singapore has been on the front end of advancing a framework for responsible AI and other advanced technologies to address societal problems such as green energy, healthcare, transportation, and housing is what merits the nation's consistently high rankings in various benchmarks and indexes for city advancement levels.[35] Partly responsible for Singapore's success is its intent focus on digital architecture, to include advancing PETs.[36] This strengthening of cohesion between sectors and entities in usage of PETs is of paramount importance in advancing their widespread adoption.

A handful of ongoing initiatives in Singapore could serve as models for advancing PETs in the United States. First, Singapore has launched the Core Operations Development Environment and eXchange (CODEX) to convene government agencies and private sector actors in a shared digital environment to advance interoperability by allowing developers to design and build services and products that communicate and interact with others within the platform.[37] Central to the CODEX is the government data architecture that established standardization of data formatting and sharing. Second, Singapore has created a Digital Trust Centre to drive advancements in PETs and other digital trust technologies. It provides a forum to enable companies to experiment with trust technologies involved in improving data-sharing and foster public-private-research partnerships.[38] Third, and related, Singapore recently launched the Privacy Enhancing Technologies Sandbox to pilot PET projects that "address common business

[35] Mishell Arwan, "Singapore - Information and Telecommunications Technology," International Trade Administration (Aug. 13, 2021), https://www.trade.gov/country-commercial-guides/singapore-information-and-telecommunications-technology; Smart Nation Singapore, "Achievements," Smart Nation Singapore (2002), https://www.smartnation.gov.sg/about-smart-nation/our-journey/achievements.

[36] Smart Nation Singapore, "Advancing our Smart Nation Journey," *National Artificial Intelligence Strategy*, (Nov. 2019), https://www.smartnation.gov.sg/files/publications/national-ai-strategy.pdf.

[37] Smart Nation Singapore, "Sharing Resources to Develop Digital Services For Citizens," Smart Nation Singapore – CODEX (2022), https://www.smartnation.gov.sg/initiatives/strategic-national-projects/codex.

[38] Eileen Yu, "Singapore aims to drive digital trust with $36.3M research facility," ZDNet (June 1, 2022), https://www.zdnet.com/article/singapore-aims-to-drive-digital-trust-with-36-3m-research-facility/.

solutions."[39] Fourth, Singapore has undertaken a partnership with the International Centre of Expertise of Montreal for the Advancement of Artificial Intelligence that includes concrete PET demonstration projects involving climate and healthcare.[40]

Likewise, initiatives in the U.K. provide relevant models for initiatives here in the United States. In 2019, the Financial Conduct Authority hosted its Global Anti-Money Laundering and Financial Crime TechSprint with a focus on the deployment of PETs in the financial space.[41] Ten participating teams presented their ideas to combat financial crimes with PETs to a range of representatives from academia to financial institutions. With the same intention of encouraging PET adoption, the Department of Business, Energy, and Industrial Strategy hosted a PETs for Public Good forum in which private and public sector entities consisting of representatives from health organizations, start-ups, academia, and the legal realm brainstormed methods to "enable safe and lawful data sharing in sectors beyond healthcare."[42] To aid in actualizing the new PET-oriented solutions, the Information Commissioner's Office has unveiled the Regulatory Sandbox, a service that provides support and resources to experts who are designing, building, and deploying PET-related services.[43]

Closing

Thank you for the opportunity to provide input on this important study. We would be pleased to discuss any of these issues in further detail. Please direct any inquiries to Paul Lekas, SIIA Senior Vice President for Global Public Policy (plekas@siia.net).

[39] Singapore Personal Data Protection Commission, "Launch of Privacy Enhancing Technologies Sandbox" (Jul. 20, 2022), https://www.pdpc.gov.sg/news-and-events/announcements/2022/07/launch-of-privacy-enhancing-technologies-sandbox.

[40] Singapore Infocomm Media Development Authority, "MOU Signing Between IMDA and CEIMIA is a Step Forward in Cross-border Collaboration on Privacy Enhancing Technology (PET)," IMDA (June 1 2022), https://www.imda.gov.sg/-/media/Imda/Files/News-and-Events/Media-Room/Media-Releases/2022/06/MOU-bet-IMDA-and-CEIMIA---ATxSG-1-Jun-2022.pdf.

[41] U.K. Financial Conduct Authority, "2019 Global AML and Financial Crime TechSprint" (2019), https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint.

[42] U.K. Information Commissioner's Office, "ICO consults health organisations to shape thinking on privacy-enhancing technologies" (Feb. 2, 2022) https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/02/ico-consults-health-organisations-to-shape-thinking-on-privacy-enhancing-technologies/.

[43] U.K. Information Commissioner's Office, "The Guide to the Sandbox," https://ico.org.uk/for-organisations/regulatory-sandbox/the-guide-to-the-sandbox/.