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

Cybernetica

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.

CYBERNETICA

Recommendations on Advancing Privacy-Enhancing Technologies

Response to RFI

Version: 1.0

July 7th, 2022

5 pages

Contents

1 Introduction....3
1.1 Purpose....3
1.2 Background....3
2 Responses to topics of the RFI....4
2.1 Specific research opportunities to advance PETs....4
2.2 Specific technical aspects or limitations of PETs....4
2.3 Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs....4
2.4 Existing barriers, not covered above, to PETs adoption....5

1 Introduction

1.1 Purpose

This document is a response to the Request for Information on Advancing Privacy-Enhancing Technologies as published in a notice from A Notice by the Science and Technology Policy Office on 06/09/2022.

1.2 Background

Cybernetica is a research organization with 15 years of practice in developing Privacy-Enhancing Technologies and their applications. Cybernetica has engaged with research programs in United States of America (e.g., DARPA PROCEED, DARPA Brandeis, DARPA SIEVE) and European Union (various European Commission and Estonian programs)[1]. Our researchers have published a range of papers on privacy technologies[2].

Cybernetica has also been successful in procurements on applications of privacy technology applications and training by multinational organizations (e.g., European Space Agency, EUROSTAT, OECD).

1 A list of recent projects is available at https://cyber.ee/research/projects/

2 A list of all papers https://cyber.ee/research/library, papers on secure multi-party computation papers up to 2021 available at https://sharemind.cyber.ee/research/

2 Responses to topics of the RFI

2.1 Specific research opportunities to advance PETs

We propose the following opportunities.

1. Training programs on (re)designing services and business processes for data minimisation, including with PETs. These should be parts of existing academic programs, but also retraining programs
2. Training programs about the usage patterns and re-identification risks of different PETs (what works in identity protection, cloud services, what works in data publishing, what works in data collaborations).
3. Piloting programs that support small enterprises and startups in prototyping services with PETs. The service developer will have to justify that they are performing service innovation, reducing unneeded data processing and they have a technology partner that is competent in supporting the development of new innovative service models with PETs.
4. Funding academic research into PETs in general, but also in specific domains (healthcare, finance, homeland security, government applications are good initial candidates). This can build on successful programs from DARPA, IARPA, NSF and private foundations.

2.2 Specific technical aspects or limitations of PETs

We would like to recommend the following materials (justification to why the materials are relevant is provided).

1. United Nations Handbook on Privacy-Preserving Computation Techniques. Available from: https://unstats.un.org/bigdata/task-teams/privacy/UN%20Handbook%20for%20Privacy-Preserving%20Techniques.pdf
   Provides a helpful explanation of the trade-offs of several privacy-preserving techniques.

2.3 Specific sectors, applications, or types of analysis that would particularly benefit from the adoption of PETs

We would like to recommend the following materials (justification to why the materials are relevant is provided).

1. THE PROMISE OF EVIDENCE-BASED POLICYMAKING Report of the Commission on Evidence-Based Policymaking. September 2017. Available from: https://web.archive.org/web/20210207094854/https://www.cep.gov/ (copy attached).
   Provides examples of using data and privacy technologys in policymaking.
2. Social Impact Applications of Secure Multi-Party Computation. Asemio Available from: https://www.asemio.com/social-impact-applications-of-secure-multi-party-

computation/
Descriptions of using secure computing in social impact applications.

2.4 Existing barriers, not covered above, to PETs adoption

We would like to recommend the following materials (justification to why the materials are relevant is provided).

1. A study of barriers to the adoption of secure computing techniques conducted by social scientists, among multiple industries.
   a) Usable and Efficient Secure Multi-party Computation. Requirements specification based on the interviews. Available from: http://uaesmc.cyber.ee/workpackages-and-reports/wp1-requirements-gathering/d12-requirements-specification-based-on-the-interviews.html
   This document lists possible preconditions and barriers that need to be addressed for the implementation of SMC, and possible use-cases brought out by the interviewees.
   b) Usable and Efficient Secure Multi-party Computation. Expert feedback on prototype application. Available from: http://uaesmc.cyber.ee/workpackages-and-reports/wp1-requirements-gathering/d14-expert-feedback-on-prototype-application.html
   The document further drills down on the barrier perception to adoption of secure computing by interviewees.