Computing Community Consortium's Response to RFI "Request for Information on Advancing Privacy-Enhancing Technologies"

July 8, 2022

Written by: Brian LaMacchia

This response is from the Computing Research Association (CRA)'s Computing Community Consortium (CCC). CRA is an association of nearly 250 North American computing research departments - academic, industrial, and professional societies. The mission of the CCC is to enable the pursuit of innovative, high-impact computing research that aligns with pressing national and global challenges. The CCC brings together a diverse set of individuals representing the broad community to lead initiatives and activities, such as this response.

Developing a national strategy around privacy enhancing technologies (PETs), and how such technologies may be harnessed to develop privacy-preserving data sharing and analytics, is a critical need for our nation. Every day both public and private sector organizations create, use, and store exceptional amounts of data and use it in exponentially new ways, but these uses are restricted to specific intra-organization silos or governed by one-off data-sharing agreements to which users have given explicit consent. PETs hold the promise to permit sharing, aggregation, and analysis of relevant data across organizations while maintaining the privacy of its subjects.

In this RFI response, we focus on two of the questions presented in RFI: Question #1 (research opportunities to advance PETs), and Question #5 (specific laws that could be used, modified, or introduced to advance PETs).

With respect to Question #1, we see two broad areas where an increased research focus would help the development and deployment of PETs and specifically advance the goal of furthering privacy-preserving data sharing and analytics. At present, there are not any widely accepted and adopted standards for sharing PET-protected information, even within a category of PET technology (e.g., secure multi-party computation, fully homomorphic encryption, etc.). If the Federal Government wants to use PETs to ensure the confidentiality of telemetry it desires to collect, there needs to be well-defined standards for how specific PETs are applied to various classes of telemetry and how PET implementations interoperate. Even though data is theoretically accessible (in the cloud) and shareable, it is difficult to preserve privacy of that data because PET technologies, data formats, encryption and signature techniques, etc. are not able to work together. A series of interoperability standards for PETs as applied to common data categories of interest would help tremendously both for data use and the creation of new technologies.

A related problem which standards may help address is users' comfort and acceptance of sharing of their data through privacy-preserving mechanisms with the Government. While the proliferation of private and public clouds makes it possible to share collected data with Government entities, individual users still have to decide to opt-in to such sharing. For example, in the case of desired collection of citizen data, citizens need to (a) see the value to society of the data collection, (b) have confidence that data associated with them personally that is shared through a properly working PET cannot be re-identified by the Government, and (c) have further confidence in the security and privacy of the PET's security protocols.

The second broad area that needs increased research and development is that of privacy-preserving credentials. Just as users have expectations about the privacy of data related to them, they also have privacy expectations around the secure credentials that they use to authenticate to various cloud-based services. Privacy-preserving credentials have been an area of active research for well over two decades, yet they still have not seen widespread adoption and use. Now, however, we may have an opportunity to push research and adoption of privacy-preserving credentials enhanced with minimal disclosure technologies; that is, capabilities that allow users to selectively reveal aspects of their identity that they choose and control. Some research in these areas has already begun, particularly building on digital vaccine credentials (e.g., SMART Health Cards) that saw widespread adoption and availability by States, pharmacies, and medical providers during COVID-19 pandemic, but we have only scratched the surface of what is possible in this realm.

We turn now to Question #5, which asks for input regarding specific laws that could be used, modified, or introduced to advance PETs. Here we would note that many PETs are implemented using encryption technologies that are currently subject to regulation under the Export Administration Regulations (EAR) enforced by the Department of Commerce's Bureau of Industry and Security (BIS). This is true both for PETs built on classical public-key and symmetric key technologies as well as those built on quantum-resistant public-key schemes. For example, fully homomorphic encryption (FHE) schemes are often based on shortest vector or closest vector problems associated with lattices, and schemes based on these problems are now explicitly regulated under the EAR (see Title 15 Part 774, 5A002.a, and Technical Note 2.c.1 in the N.B. for 5A002.a.4).

Using PETs to enable privacy-preserving data sharing and analytics is going to necessitate using the encryption schemes that underlie many PETs and applying those schemes to data gathered both within the United States and around the world. A national strategy for privacy-preserving data sharing and analytics should examine the application of the existing EAR related to cryptography to encryption used within PETs, as the existence of export regulations that encompass PETs will hinder their commercial development and deployment. We would suggest that as part of the development of a national strategy that BIS consider whether the EAR should be amended to make the use of encryption within a PET scheme an uncontrolled use.