Evaluating Privacy Enhancing Technologies for Organizations

Carnegie Mellon University
MSIT-Privacy Engineering Capstone Project
November 2018

Ao Chen, Jeremy Thomas, Advisor: Nicolas Christin

Given the changing perspective on privacy in today's society, organizations must adapt to a growing set of requirements and constraints on practices that impact privacy. Individual choices about privacy, exposure of broken privacy practices, and expanding regulations force organizations towards expanding the influence of accepted principles of privacy throughout business operations. All of these factors encourage the use of technologies to provide stronger privacy guarantees and to directly address the privacy challenges these requirements create in an effective and efficient manner.

To better understand the use of privacy enhancing technologies (PETs) by organizations, we interviewed a set of privacy experts working across various industries and in multiple disciplines. We conducted 20 interviews of privacy experts from September 2018 to November 2018. We interviewed most participants over the phone or through video conferencing applications, and typically the interviews lasted 30 to 60 minutes.

To compare each technology's effectiveness and efficiency at addressing the privacy challenges of organizations, we first categorized privacy technologies based on their contributions towards the three primary objectives of privacy engineering as defined by The National Institute of Standards and Technology (NIST): predictability, manageability, and disassociability. Within each of these objectives, we determined the effectiveness of each technology in addressing privacy harms. For example, de-identification techniques increase the disassociability of a data subject within a dataset, and their effectiveness derives from the strength of de-identification (e.g. the value of *'k*' in *k*-anonymity). This reduces privacy risks for the individual such as those from undesirable disclosures of the dataset. The efficiency of any technology contains both the costs of implementation and the reduction, if any, in utility of the related practices to the organization. Continuing with the example of de-identification techniques, these techniques preserve the privacy of an individual within a dataset, but they potentially reduce the utility that an organization can extract from the dataset. In this way, we explored several privacy enhancing technologies that we identified through our interview process. Some key technologies include:

- Differential Privacy implementations at Microsoft, Google, Apple, and Uber
- Private Set Intersection as implemented by Google and Mastercard
- User access and control platforms such as the Data Transfer Project

Many of these technologies remain emerging technologies with most innovation occurring through academic and industry research such as differential privacy and private set intersection. Technology leaders (Google, Apple, Microsoft), represent the early adopters of many of these technologies. However, in many cases, these technologies expose the lack of maturity in the market for privacy enhancing technologies. More mature, PETs exist (access controls, audit logs, data tagging and mapping, etc.) and align with current regulations. Therefore, organizations must first apply mature PETs to safeguards on compliant data practices, and then layer emerging privacy technologies within products and services to protect higher order privacy requirements such as ethical and responsible data uses.