PETs: not yet friendly

Kris Shrishak

Irish Council for Civil Liberties

This talk will discuss how privacy enhancing technologies (PETs) are developed, deployed, whose interests they currently serve and how they can be designed to serve public interest. PETs have the potential to address the intersection of cybersecurity and data concerns on the Internet. Yet, they also open up risks to privacy and other fundamental rights that are understudied.

PETs have been touted as being beneficial for people and for the society [NA15]. These techniques allow data processing while protecting the underlying data from being unnecessarily revealed. For example, techniques such as "homomorphic encryption" and "secure multiparty computation" make it possible to train machine learning models while aggregating data from individuals without revealing the individual information to anyone else, including the other participants. Other techniques such as "differential privacy" allow for the release of aggregate statistics while reducing the risks of individual identification.

An increased awareness of personal data collection and of data protection regulations has contributed to the appeal of these PETs. However, are the current deployments serving the needs of the public, or the narrow interests of corporations and governments? Companies such as Google are working with Mastercard to track people online and offline by combining advertisement information with purchase information [BS18]. The individual data points are protected, but the surveillance capability broadens.

The European Commission wants companies to scan devices of people, and has identified "homomorphic encryption" and "secure multiparty computation" as possible approaches to achieve this goal [Com22]. Europol has suggested that such scanning be extended beyond the initial proposal to detect child sexual abuse material because even innocent images could be useful for law enforcement purposes [MSZF23]. These examples raise the question of whether PETs entrench the current status quo of surveillance.

Furthermore, products incorporating PETs also raise competition concerns [Com23]. Certain PETs techniques require large amounts of computing power, which remain in the possession of a few "cloud" infrastructure companies. These same companies are also involved in the standardisation of PETs in various forms [1]. This creates a dependency between the digital infrastructure, its uses and corporate incentives.

Given the promise and expectation of PETs to protect people's privacy, one would imagine that significant research would have been carried out to understand the actual privacy benefits of these technologies. Many of the PETs indeed stand on years of mathematical and security analysis [DR14, Lin16]. While these are essential and important, these are agnostic to the context in which these PETs are deployed. A few recent works design PETs with abuse prevention built-in [KGT20, TBB+22]. But such thoughtful designs are far from the norm.

[1] In particular, Internet Engineering task Force (IETF) and the World Wide Web Consortium (W3C)

For PETs to truly serve public interest, they need to protect privacy of people in the context of deployment. Otherwise they will be a tool for privacy-washing, deployed to encroach on people's rights.

References

[BS18] Mark Bergen and Jennifer Surane. Google and mastercard cut a secret ad deal to track retail sales. https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales, 30 August 2018.

[Com22] European Commission. Commission staff working document impact assessment report accompanying the document proposal for a regulation of the european parliament and the council laying down rules to prevent and combat child sexual abuse. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0209, 11 May 2022.

[Com23] Competition and Markets Authority. Investigation into Google's 'Privacy Sandbox' browser changes. https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes, 8 January 2021 (Last updated on 26 October 2023).

[DR14] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014.

[KGT20] Blagovesta Kostova, Seda F. Gürses, and Carmela Troncoso. Privacy engineering meets software engineering. on the challenges of engineering privacy bydesign. *CoRR*, abs/2007.08613, 2020.

[Lin16] Yehuda Lindell. How to simulate it - A tutorial on the simulation proof technique. *IACR Cryptol. ePrint Arch.*, 2016.

[MSZF23] Andre Meister, Ludek Stavinoha, Giacomo Zandonini, and Apostolis Fotiadis. Interne Dokumente: Europol will Chatkontrolle-Daten unbegrenzt sammeln. https://netzpolitik.org/2023/interne-dokumente-europol-will-chatkontrolle-daten-unbegrenzt-sammeln, 29 September 2023.

[NA15] European Network and Information Security Agency. *Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics.* Publications Office, 2015.

[TBB+22] Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda F. Gürses, Jean-Pierre Hubaux, Dennis Jackson, James R. Larus, Wouter Lueks, Rui Oliveira, Mathias Payer, Bart Preneel, Apostolos Pyrgelis, Marcel Salathé, Theresa Stadler, and Michael Veale. Deploying decentralized, privacy-preserving proximity tracing. *Commun. ACM*, 65(9):48–57, 2022.