Special Topics on Privacy and Public Auditability

STPPA event #1: January 27, 2020 @ NIST Gaithersburg, Building 101, Lecture Room B

Topics: fake videos, census data, differential privacy, public randomness

Meeting agenda

10:00am–10:15am: René Peralta, NIST — **Introductory remarks**

10:15am–10:45am: Luís Brandão, NIST
Randomness Beacons as Enablers of Public Auditability

10:45am–11:30pm: Simson Garfinkel, U.S. Census Bureau
De-Identification and Differential Privacy

11:30am–11:45am: **Break**

11:45am–12:30pm: Simson Garfinkel, U.S. Census Bureau
Differential Privacy at the US Census Bureau: Status Report

12:30pm–02:00pm: **Lunch**

02:00pm–03:00pm: Charles Bennett, IBM
What Math and Physics can do to Combat Fake Videos

03:00pm–03:15pm: **Closing remarks**

Note: the initially shared agenda mentioned a different 2nd talk (10:45am–11:30am), but the speaker could not attend; this version is corrected, showing the actual 2nd talk, given by Simson Garfield from the U.S. Census Bureau.

Abstracts

Title: ***What math and physics can do to combat fake videos***

Speaker: Charles Bennett

Affiliation: IBM

Abstract: Progress in artificial intelligence has made it easy to produce "Deep Fake" videos that are so realistic that even experts have trouble identifying them, and go on to spread virally, due to people's susceptibility to content that appeals to their prejudices or fears, especially when forwarded by friends with whom they correspond regularly. It would seem that the hard sciences can do little to mitigate this problem, which has so much to do with psychology and human nature. But math and physics can be a significant part of the solution, by establishing in a hard-to-fake way a video's time and place of origin, and that it has not been subsequently altered. An ordinary smartphone, if it is internet-connected, can be used to make rather hard-to-fake videos, and with the help of public randomness beacons, very hard-to-fake ones whose authenticity can be verified without needing to trust either the maker of the video or any centralized authority. A more serious problem is content that spreads virally despite containing no evidence at all of its provenance. Trusted open-source client-side scanning software and differential privacy techniques may offer a way to flag rapidly-spreading items for subsequent fact-checking without seriously compromising social media users' privacy or freedom of speech.

Title: ***Differential privacy and the 2020 Census***

Speaker: Simson Garfinkel

Affiliation: Senior Computer Scientist for Confidentiality and Data Access, U.S. Census Bureau

Abstract: The privacy risks associated with the publication of official statistics have increased significantly over the last decade, fueled by the proliferation of detailed, third-party data sources and technological advances that make re-identification of individuals in public data releases increasingly easy. This presentation will discuss the U.S. Census Bureau's research into these emerging privacy threats, and the agency's efforts to modernize its disclosure avoidance methods using differential privacy to ensure the confidentiality of individuals' data. Differential privacy offers significant advantages over traditional disclosure avoidance methods for safeguarding individuals' privacy, but the implementation of differential privacy at scale for the 2020 Decennial Census has also posed a number of challenges. This presentation will explore these challenges and discuss the lessons learned from this initiative.

Title: ***De-Identification and Differential Privacy***

Speaker: Simson Garfield

Affiliation: Senior Computer Scientist for Confidentiality and Data Access, U.S. Census Bureau

Abstract: TBD

Title: ***Randomness beacons as enablers of public auditability***

Speaker: Luís Brandão

Affiliation: Cryptographic Technology Group, NIST

Abstract: The NIST Randomness Beacon provides public randomness as a public good. A beacon produces periodic outputs of fresh randomness, in an expected format, and makes them publicly available perpetually thereafter. For example, this could be used to assign court cases to judges, in a publicly auditable manner. More generally, beacons offer the potential to improve fairness, auditability and efficiency in numerous societal applications that require randomness. However, their implementation and use are challenging in terms of security and trust. This talk will briefly overview some aspects of the NIST reference for randomness beacons, and allude to their potential to enhance public auditability. We hope to encourage the development of applications of public randomness, and the implementation of interoperable randomness beacons in every country.