Privacy Tech

Exploring the technology of privacy

Blockchain and big data privacy in healthcare

Gary LaFever
Privacy Tech | May 2, 2016

As the volume of digital data proliferates in virtually every field, the potential value from analyzing it skyrockets—but so do associated privacy risks.

Methods of privacy protection that were developed years or even decades ago no longer translate well in the age of big data. This is because these older methods either aren't strong enough at scale (a phenomenon described by "the Mosaic Effect,") or require a degradation of the quality of the data itself, making it less valuable.

Healthcare – one of the most privacy-sensitive data domains – has a unique set of regulatory requirements related to privacy protections, primarily laid out in the U.S. under the Health Insurance Portability and Accountability Act of 1996.

Fortunately, new and complementary tools and methods of privacy protection make it possible to simultaneously protect data privacy and accuracy in order to leverage the value of big data in healthcare and also comply with federal and international laws, including HIPAA.

One promising approach is blockchain, which, together with Bitcoin, has garnered much enthusiasm in the financial sector by enabling trusted, auditable transactions using a decentralized network of peers accompanied by a public ledger.

In healthcare, blockchain could provide a secure yet transparent record of who has shared health data with whom, while protecting the details of the data itself. While this is undoubtedly a valuable piece of the privacy puzzle, blockchain is premised on mathematically derived pseudonyms for distributed ledger verification and the HIPAA Privacy Rule prohibits use of mathematically-derived pseudonyms because of potential re-

identification of de-identified protected health information (PHI). This limitation on the use of mathematically-derived pseudonyms as re-identification codes for de-identified information effectively makes blockchain non-HIPAA compliant.

Similar issues have been raised about the use of blockchain to support more accurate ratings for e-commerce and travel sites and for individuals such as teachers, doctors, landlords, colleagues, and police officers due to potential threats to anonymity and privacy online. The potentially irreversible nature of such distributed blockchain "trust" systems also raise concerns about undermining an individual's right to be forgotten.

One solution to address blockchain's challenge in healthcare (non-compliance with HIPAA), is to combine blockchain with Dynamic Data Obscurity to support non-mathematically derived dynamically anonymous identifiers to address HIPAA compliance issues, overcome the Mosaic Effect, and enable granular privacy controls.

Last year, I wrote that Dynamic Data Obscurity can support 'proportional' use of data in a manner that is responsive to the variety and complexity of different, potential uses of data. Specifically, dynamic de-identification can reveal different levels and type of information to the same and/or different parties at different times, for different purposes, at different places – with respect to each, only as necessary for each proposed use of data. By combining blockchain and Dynamic Data Obscurity, it would be possible to support de-identification requirements under the HIPAA Privacy Rule.

Potential benefits from blockchain applications in healthcare, such as those set forth below, depend on concerns over, and regulatory requirements for, maintaining privacy and security of sensitive data (e.g., Protected Health Information in the U.S. and personal data in the EU) first being resolved:

- Introducing efficiency and transparency into the heavily siloed healthcare industry by enabling governmental agencies, insurance companies, hospitals, doctors, clinics, and patients to use a common blockchain;
- Allowing health providers to share networks without compromising data privacy, security, or integrity;
- Managing the lifecycle of patient records via blockchain; and
- Streamlining the lifecycle of medical bills via blockchain.

The synergy between blockchain and Dynamic Data Obscurity can hopefully serve as an example of technologists rising to the challenge laid down by former U.S. FTC Commissioner Julie Brill in her 2013 speech on the role they can play in protecting privacy. "This is your 'call to arms,' – or perhaps, given who you are, your 'call to keyboard,'" she proclaimed, "to help create technological solutions to some of the most vexing privacy problems presented by big data."

photo credit: Bitcoin Chain IMG_9197 via photopin (license)

Comments

Logged-in as: John Wunderlich

Share your thoughts