INSEAD The Business School for the World®

KNOWLEDGE

Safeguarding Privacy in a Pandemic

Speeding up the adoption of blockchain and other digitised ledger technologies (DLT) can help society reconcile security and privacy.

In many countries, privacy is in danger of becoming a casualty of the COVID-19 pandemic. For example, GPS-enabled smartphone apps with liberal **data-gathering permissions** are now mandatory in Hong Kong, China and South Korea. Privacy concerns may appear trivial next to the pressing threat to human life that COVID-19 represents but the ground ceded to the authorities in the name of public health **may not be regained once the crisis passes**. Already, strongman leaders such as Hungary's Viktor Orban are capitalising on the coronavirus **to consolidate far-reaching powers for themselves.**

Do we, as a society, have to make a stark choice between privacy and safety? Luckily, the answer is no: Privacy and safety can both be maintained by managing personal data using blockchain and other DLTs. **DLTs and privacy**

Blockchain – and similar technologies that included under the name of DLTs – was created to allow anonymous individuals to maintain an immutable record of transactions in a peer-to-peer, decentralised way. Crucially, the same technology can also be applied to all sorts of records, including records containing personal data.

So far, the main use of DLT in the context of personal data has been to verify the authenticity of a piece of information. As an example (somewhat simplified for the purposes of illustration), considering a digital driver's licence. The government office issuing driving licences is a participant in the network maintaining the blockchain, with a known and publicly recognised address. Whenever this office issues a new licence, it also simultaneously uploads the hash (i.e. cryptographic summary) of this driver's licence to the blockchain. This specific hash is a string of text and numbers which represents a cryptographic version of the licence. It has two important properties: Any variation in the licence (an extra comma, a different pixel) will produce a drastically different hash, and at the same time it is impossible to recover the content of the licence just by viewing its hash. Because this hash is uploaded into the blockchain, it becomes impossible to edit it afterward.

This hash is publicly observable, but it is impossible to recover any information about the licence just by looking at it. Hence, no private information is publicly disclosed. At the same time, a person can send the digital copy of their driver's licence via email to, for example, a bank as proof of identification to open an account. The receiving party can easily verify the authenticity of the file by computing its hash and comparing it with the one uploaded on the blockchain.

Privacy and security, simultaneously

These technologies can be used to better manage the aforementioned trade-off between privacy and security. For example, for many observers, it is crucial to **identify those who had the virus** and have developed antibodies. Because, in theory, these people are now immune, so they could be allowed to return to work or to cross borders sooner than others. They could also be drafted to take care of the most at-risk. Keeping records of who is immune in a private, secure but verifiable way is essentially the same problem as issuing a driver's licence on the blockchain – the only difference being that the trusted authority is the local health agency. In general, we already have the technological infrastructure to manage *official* health records privately and securely using blockchain. This technology should be deployed rapidly on a large scale.

More challenging – but equally important – is managing *user-generated* personal data (such as location history or any biological signal that can be recorded by wearable devices) in a private, secure but verifiable way. The challenge here is the lack of a trusted third-party certifying the data. But blockchain can also be used *to commit* to reveal information in the future. This is done by uploading on the blockchain the hash of a piece of information *before revealing it.* When this piece of information is revealed at a later date, everybody can verify the authenticity of this piece of information at the time its hash was included in the blockchain.

To illustrate why this matters, consider the following mechanism. A mobile phone app collects location data using the phone GPS, or logs every time two phones are in close proximity (this is possible using Bluetooth, see **this** and **this** project). The original, unencrypted version of the data resides on the phone, while its hash is uploaded hourly into the blockchain. If a person tests positive for the virus, then this person is legally required to remotely turn over his or her location data (limited to the period of time when they were likely to spread the disease), which is then checked against the hash registered on the blockchain for authenticity. This data (anonymised and possibly mixed together with location data from others who tested positive) are then uploaded to a public server. Every other app automatically checks whether a possibly dangerous encounter occurred. If it did, a notification appears on the app asking the person to take appropriate measures (for example, self-quarantine for two weeks). Of course, compliance cannot be verified on the spot. However, blockchain allows for subsequent verification should the owner of the data test positive for the virus.

Other features can be easily added to such a system. One is private and secure biometric authentication. A start-up called **Keyless** (that counts among its founders two INSEAD alumni) has developed a method to identify encrypted biometric data such as, for example, a fingerprint scan stored on your phone. The point is that if two encrypted pieces of data are sufficiently similar, then they must belong to the same person. Meanwhile, nobody can see the unencrypted fingerprint scan. All data are collected, and all the hash uploaded on the blockchain are uniquely associated to an individual, without ever knowing who this person is. Because this is a blockchain, it is possible to add a layer of incentives. For example, if a person agrees to disclose their location data during the period of quarantine, this person can be automatically compensated with a given amount of digital currency. This way, not only are those who do not comply caught and punished, but those who do comply can be rewarded for doing so.

These proposals would not satisfy those who insist that no personal data should be collected by the authorities. Their insistence on total *secrecy* should, however, be distinguished from concerns about *privacy*. Privacy is violated when personal data are collected automatically, on a large scale, without any *individual-specific* reason to do so. As a concrete example, **GDPR** requires that data video-surveillance systems be automatically deleted *unless* the video captured a specific security incident. Hence, collecting personal data only of people who may have contracted the virus and could spread it to others is justified by public health concerns and does not constitute a violation of privacy.

Finally, adopting such a system on a large scale would provide the backbone of a truly global standardised infrastructure to manage personal health data. If two countries use the same blockchain-based system, then authorities in country A can easily check whether a traveller from country B who claims immunity from the virus was indeed certified by the health authorities of country B. The same system can be used to rapidly verify any health record, for example, to establish whether a person has diabetes, haemophilia or any other condition that is relevant in case of a health emergency.

A pivotal moment

The world's deep concerns around privacy did not begin with COVID-19. Indeed, they have been a flashpoint of global discourse throughout the Fourth Industrial Revolution. History shows that global crises raise opportunities to resolve such long-standing societal impasses. We should seize this opportunity to reconcile privacy and security, once and for all.

Andrea Canidio *is the Stone Fellow of the* ***James M. and Cathleen D. Stone Centre for the Study of***

__Wealth Inequality__ at INSEAD and an Assistant Professor of Economics at the IMT School for Advanced Studies Lucca, Italy.

Found this article useful? __Subscribe__ to our weekly newsletter.

Follow INSEAD Knowledge on __Twitter__ and __Facebook__.

Find article at
https://knowledge.insead.edu/blog/insead-blog/safeguarding-privacy-in-a-pandemic-13956