THEME 02

Managing your digital identity

IDENTITY DECENTRALIZATION DIGITAL TECHNOLOGY

In order to establish trust between you and other individuals or institutions or to provide points of reference for receiving services one needs to prove one's identity. As many domains digitize and more transactions are conducted digitally, the need for secure, trusted and widely adopted digital identity management becomes a necessity. However, in modern-day life, our identity has come to be managed by multiple different parties. This leaves us vulnerable to the intents and weaknesses of these different parties. What are the most developed identity systems globally and what are the innovations that might challenge the dominant ones?

Our observations

- A digital identity is an online or networked identity belonging to an individual (or organization or device). Our digital identity does not refer to a single identifier (e.g. name and date of birth), but it can vary across applications as a means to securely interact and transact (e.g. a chosen user name).
- There are three major challenges concerning digital identity. The first is identity fraud. In 2016, $16 billion was stolen from 15.4 million U.S. consumers. Second are data breaches. In 2017, 143 million identity data records were breached at Equifax. Third, a digital identity used by one system cannot be used immediately by another. This lack of reusability of identities is costly. For, instance, in 2016 financial institutions spent $60-500 million per year on average to on-board new customers.
- Our identity is increasingly linked to our biometric data. As the use of biometric data becomes more widespread, the vulnerabilities also become clear. A Dutch consumers' union tested 110 smartphone models and found that the facial recognition feature used for locking devices can be tricked with photos on 42 phones (the iPhone withstood the test). However, as the number of devices and online services and products increases, passwords for every individual device are a non-starter and some form of biometric scanning might be inevitable.
- The largest biometric identity system ever implemented is India's controversial identity program, Aadhaar. Despite data leaks and privacy issues and almost a decade after its launch, the Supreme Court of India recently ruled Aadhaar constitutional. By now, it has enrolled over 1.22 billion Indians.
- As centralized identity management models show vulnerabilities, there is a growing interest in decentralized identity platforms. Aside from financial applications, one of the most widely discussed use cases of blockchain and distributed ledger technology is identity management. Blockchain enables storage, authentication and authorization without having to rely on a centralized trusted third party. Examples are Sovrin, CIVIC, Uport, PAT, XID, Blockverify, Selfkey, and Blockstack/blockauth. Recently, Tim Berners-Lee introduced Solid, a decentralized identity platform which provides a mechanism for users to own and better control their data.
- Younger generations are more aware of the dangers of poor security in the online space and make better use of the provided privacy settings. The majority of young U.S. Facebook users say they have adjusted their privacy settings in the past year. Generation Z prefers social platforms that give them tighter control over who to interact with, such as Instagram and Snapchat or smaller online communities . As they are digital natives, they are also the generation that knows best how to separate their offline identity from their online identity.
- More than 1 billion people globally remain without official identity documentation. UNHCR is using biometric identity systems as part of development aid for refugees.

>> see next page

Connecting the dots

Since the 19th century, the state has gained a monopoly on issuing legal identity, through a system of national registers and databases. Only recently did the internet challenge these institutions of identity as private businesses such as Facebook and Google started to manage identities in the online sphere. As a result, in the digital age, our identity is scattered between many off- and online systems and models of identity.

First are the current systems states use to manage identities of citizens. Two fundamentally different state models can be recognized that are similar in how far-reaching they are for citizens, as both are key to access all kinds of services. The identity management systems of India or China rather represent a model that gives the state more power over its citizens. The information revolution means that the state can associate more data than ever with citizens. The 12-digit Aadhaar number is linked to a central database entry that contains biometric data including ten fingerprints, iris scan, face scan, and biographic data of region/place of birth. The Aadhaar is asked in many everyday activities, reducing anonymity. The centralized architecture of the system makes it susceptible to hacks, fraud and corruption. For instance, the Uttar Pradesh State Government has listed many living individuals as dead over the years in order to obtain their property rights. In the Chinese Social Credit System, behavior is tied to a person's identity. Consequently, people demonstrating "untrustworthy" behavior can be denied access to basic activities. The Estonian digital identity system represents the second state model. In contrast to the Indian and Chinese approach, the Estonian system is more about creating trust in the government through transparency of the system. For instance, the system allows all citizens to know exactly which administration has checked their personal data.

Second are the systems developed by non-state parties to manage identities of people online, where we can differentiate between centralized and decentralized approaches. Although the internet created digital identities, one of its design "flaws" was that it did not include a standardized form of accurate and irrevocable identity-management. From the early days of the internet onwards, public key cryptography became a fundamental component of digital identity systems. A public key (a chain of numbers) is used to encrypt data and only the private key belonging to an individual can decrypt these data. To ensure that public keys were linked to identities, a trusted third-party certificate authority (CA), published a public key mapped to a user using a private key. When PCs started to be widely adopted, it was recognized that relying on a centralized party, the CA, was vulnerable to flaws. Consequently, there were efforts to curb this risk, such as with the introduction of a "web of trust" (1992), in which the CA was replaced by a peer-to-peer approach in which each user has their own public and private keys. However, this decentralized trust model lacked scalability and only later would blockchain technologies provide a scalable alternative. Thus, the lack of a feasible digital identity system on the internet remained largely unsolved. Online social networks created the next big shift in digital identity when they introduced the federated identity concept. For many websites and online services, a Facebook or Google profile is sufficient proof of identity for login purposes. Therewith, these tech parties cater to our wish for convenience – as we don't want to create a new username and password for each website – but, at the same time, they are also able to gather lots of data about us. Globally, Facebook dominates this social log-in market and can thus be seen as the biggest online custodian of identities to which all other data of online behavior and preferences can be linked. The trust structure in this centralized identity model is clearly top-down. However, the backlash against Facebook, among others, for selling detailed profiles of its users, further energized the revival of decentralized trust models. Propelled by the developments in blockchain technology, this has led to calls for a self-sovereign identity. A self-sovereign identity can potentially integrate all the bits of our identity that are now scattered among services both offline and online by enabling us to have ownership of our own identity, and control over how, when, and to whom our personal data is revealed.

In the end, the question remains whether one system will be adopted to securely manage identities across domains or whether an ecosystem of alternatives will prove themselves valuable at scale. According to TechVision's 2018 the future of identity report, there is a need for a number of manageable, consistent identity services to serve as a "launching point" for the innovations we are to see over the next years.

Implications

- **In a world where we are becoming over-identified, the possibility of anonymity also decreases. Satoshi Nakamoto, the most famous anonymous person on the internet, has shown us the advantage of anonymity in providing privacy and protection while using the freedom of creation and innovation on the Internet.**
- **As awareness of the abuse of personal data grows, alternative identity platforms are offering individuals the possibility to disclose only their relevant properties. A Dutch example is IRMA.**
- **Our identity is increasingly linked to our physiological data and our behavior. Across different models, the tendency to link identities to behavioral and biometric data is increasing and with it, the ability to create a highly detailed portrait of us.**
- **The only entities that communicated on the internet used to be humans. IoT challenges this and so securely identifying devices is becoming ever-more important, as they can increasingly be considered to have agency.**

>> see next page