SOCIAL COHESION, GLOBAL GOVERNANCE
AND THE FUTURE OF POLITICS

The Digital Freedom Pass: Emancipation from Digital Slavery

Dennis J. Snower

(Global Solutions Initiative, GSI)

April 1, 2019

Abstract

Digital identity management is currently undertaken by central identity providers, with users providing their data free to digital networks that own their digital identities. If users leave their digital networks, they must leave all their digital possessions, including their digital identities, behind. This system is analogous to slavery. It is neither efficient nor equitable. Users have no assurance that the value of the free data they provide bears any relation to the value of the free services they receive. The digital networks have overwhelming market power relative to their users. This column argues for reform in the form of a Digital Freedom Pass, – the digital equivalent of a wallet containing verified pieces of an individual's digital identity. The person can then choose which identification to share, with whom, and when, allowing emancipation from our current digital slavery.

Challenge

Imagine a new form of slavery – call it slavery 2.0. Slaves provide free labour for their owners; in return, the owners give them free food, clothing and shelter. Furthermore – and this is the new twist – slaves are free to leave their owners whenever they wish, but when they do so, they must leave everything behind – their belongings, their friends and acquaintances, their reputation and all other external aspects of their identity. Would a labour market built on this system be considered efficient and equitable?

The obvious answer is: Silly question, of course not! But this silly question turns out to be supremely important for us nowadays, because in the digital world we are all slaves 2.0. We provide information about ourselves for free. This free labour enables digital networks – such as the 'Big Five' (Apple, Facebook, Amazon, Google, and Microsoft) – to amass vast fortunes. In return, we receive free apps and other internet services. We are free to leave any networks to which we belong, but when we do so, we must leave everything behind – the information about us, our contacts, our ratings, our digital identities on those networks. We have no property rights on the data we generate, and only by generating such data can we derive benefit from our digital networks. This relationship between the digital networks and their users is digital slavery 2.0.

An inefficient and inequitable system

This system is inefficient, since economic markets cannot generate efficiency when the commodities transacted – information about individuals in return for some free internet services – are free. It is analogous to old-style slaves providing their free labour in return for free food, clothing, and shelter. There is of course no guarantee that, for every individual, the marginal value of the free internet services is equal to the marginal value of the users' information. On the contrary, we have every reason to believe that the value of the information supplied by users to the network owners far exceeds the value of the internet services that the users get for free – much like the marginal value of slave labour far exceeded the marginal value of the food, clothing, and shelter that the slaves received. People with high skills in generating valuable data have no incentive to employ their talents for this purpose if data are supplied for free. Costless data also gives people no incentive to develop skills that could improve internet services.

These inefficiencies are tolerated by the digital network providers, since what they lose from these inefficiencies they make up handsomely through the market power gained through digital slavery 2.0. Hal Varian, the chief economist at Google, argues that data nowadays are plentiful and thus virtually worthless, whereas the designers of the networks are scarce and thus generate most of the value of the digital network services. This argument is self-serving. It is analogous to arguing that slave labour, in the heydays of slavery, was plentiful and that most of the value was generated by the designers of the slave plantations. It is impossible to assess the marginal contributions of data users and network designers when one of these groups works for free. Furthermore, as Posner and Weyl (2018) note, it is far from clear that the marginal value of the data generated by network users declines with the amount of data, given that the data are used to handle more and more complex problems (such as face and emotion recognition and predictable cognitive processes).

The system is also inequitable, since the owners of the digital networks wield overwhelming power. They own the access to the digital data on which their users rely, much as old-style slave-owners owned the access to their slaves' basic necessities. The fact that the slave-owners provided something of value to their slaves did not make the exchange of slave labour for basic necessities equitable. The slave-owners were in a position to exploit their market power to their own material advantage, much like the digital networks nowadays are doing.

Proposal

The solution: Digital emancipation

There is a straightforward solution to this monstrously unjust and wasteful system: digital emancipation. Just like the emancipation from old-style slavery gave the slaves property rights over their own services, so emancipation from digital slavery must give users property rights on the data they generate.

Since users currently don't have property rights on their data, they generally don't know how their information is used. They are subject to manipulative advertising that exploits their data. They are vulnerable to attack by hackers. They are largely powerless in the hands of global digital monopolies. They are vulnerable to digital automatisation, enabling machines to take over the routine work they perform, without giving them the opportunity to put new, user-generated work in its place. All these problems could be overcome by giving digital users property rights over their services.

A small but growing number of insightful policymakers are calling for this reform. Recently, at the Global Solutions Summit, Chancellor Merkel suggested that digital data be priced and users be able to sell their data. It is not worth being half-hearted about this reform – improving data protection, granting users more information about how their data is used, etc.

– though doubtlessly there will loud voices from the digital special interest groups calling for half-heartedness. A comprehensive solution – offering true emancipation – is feasible. We have the knowledge and technology to implement it. All that is required now is political will.

The solution could be called the Digital Freedom Pass (DFP). It involves giving each person the digital equivalent of a wallet that contains verified pieces of his or her digital identity. Specifically, it gives each person a private key for an unlimited number of recipients, who can access the encrypted data only if they possess the corresponding public key. The person can then choose which identification to share, with whom and when. This makes the person 'sovereign' over his digital identity, commonly called 'self-sovereign identity' (for excellent summaries, see Der et al. 2017 and Tobin and Reed 2017).

In the tech world, a 'digital identity' is information about an entity (for example, an individual) that represents that entity. The digital identity arises from the use of personal information and the actions of individuals on the web. In the real world, you are the provider of your own identity, since you generate the characteristics that enable others to recognise you. On the Internet you have an 'identity provider', who provides you with an identifier (often a password) in a specific domain that proves that you are you. Currently, identity providers focus on those of your characteristics that are relevant to the organisation and its objectives, without independent regard to you and your objectives. These identifying characteristics belong to the organisation, not to you. Consequently, you wind up with a large number of online personas at a large number of different organisations. By contrast, a 'self-sovereign identity' puts your identity into your own hands.

Digital identities need to be 'secure', which means that they pass requirements of privacy and trustworthiness. 'Privacy' means that only authorised recipients can access your digital identity; 'trustworthiness' means that the information contained in your digital identity is correct. The Cambridge Analytica scandal and other misdeeds suggest serious problems concerning privacy. The absence of authoritative background checks for much of the information that users provide to the digital identity providers creates problems of trustworthiness.

Prerequisites for achieving digital emancipation

Self-sovereign identities put the individual in control of his or her digital identity, giving her full access to her own data – something that is virtually unheard of under the current digital regime. An individual's digital identity needs to be persistent, portable, interoperable, and secure (see Allen 2016 for a more detailed description of these requirements). These are all recognised to be important prerequisites for the achievement of freedom in the digital space.

Since individuals are in charge of their digital identities, they will need to take responsibility for satisfying these prerequisites themselves. In order for people to do so, they will need public support in managing their digital identities. For example, they will need to have access to convenient digital sources of evidence for the correctness of their information they provide and receive (through digital signatures of third parties to prove authenticity), procedures ensuring transparent consensus concerning the content and conduct of transactions, and systems ensuring consistent usage rights for the individual's data. The implementation of such systems can draw on decentralised ledger applications such as blockchain (which verifies the accuracy of one's data decentrally, as it does for Bitcoin) and smart contracts (e.g. Jacobovitz 2016, Meitinger 2017). These applications permit us to look up decentralized identifiers without involving a centralised directory. They allow people to authenticate their data about themselves by using decentralised, verifiable credentials.

Since digital identities are meant to function across legal jurisdictions, it will be vital to specify an international legal framework relevant to each transaction. For this purpose, the EU General Data Protection Regulation (GDPR) uses the principle of Lex loci solutionis, in which transactions are associated with the citizenship of the individuals involved.

What I refer to as the Digital Freedom Pass covers the entire constellation of self-sovereign identities, along with supportive technologies and legal systems, and standardised interfaces. The DFP makes users central to the administration of their identities. It enables users to use their identity across multiple locations, but only with their consent. Since decentralised identities are difficult to access, they are also difficult to hack.

The prerequisites for the establishment of the DFP require public support, much as governments were required to build the internet and give people access to it. Meeting these prerequisites should be easier, cheaper, and much faster than the large public efforts of the past, such as building water, rail and road networks during the Industrial Revolutions. All that is required is the appropriate political will.

Such a scheme has already been conceived and is running in some limited domains. OpenID, an open standard and decentralised authentication protocol, allows users to control their personal data by enabling them to be authenticated by other users without the need for external identity providers. ID2020 is a public-private partnership aiming provide every person on earth with access to a personal, private, secure, persistent, and portable digital identity (ID2020 2017) in support of the UN Sustainable Development Goal, Target 16. The DFP could drive such initiatives. The Swiss municipality of Zug has introduced a distributed leger system to implement self-sovereign identities for its residents. Microsoft aims to support decentralised identification technology through Microsoft Authenticator.

The DFP provides a basis for the sale of user data to digital companies. The proceeds from such digital sales could be taxed and the revenue used to extend and upgrade internet access, as well as to reduce the cost of internet access for disadvantaged groups.

But the DFP will not happen by itself. There are too many digital companies with vested interests in maintaining control over their users' data. Slavery also did not disappear by itself. For the DFP to be successful, it needs broad adoption. For broad adoption in the EU, it must be made a legal requirement for the EU. The DFP could play a central role in the creation of a European digital single market and is consistent with the DGPR. Progress on this front could put the EU at the vanguard of a movement to emancipate people worldwide from their current digital slavery.

The rise of powerful digital monopolies – linked to the rise of inequalities in major market economies, large-scale manipulation of digital users for political purposes, and the widespread inability of digital users to grasp the business purposes that their data serves – threatens to undermine market economies and democratic processes. The DFP would spearhead a reversal of these alarming trends, since it would give us property rights over our most important possession – information about ourselves – and thereby would give us our most valued freedom in the economic realm: the freedom to choose.

References

1. Allen, C (2016), The Path to Self-Sovereign Identities, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
2. Der, U, S Jähnlichen and J Sürmeli (2017), "Self-sovereign Identity: Opportunities and Challenges for the Digital Revolution", Computers and Society, Cornell University Library. https://arxiv.org/abs/1712.01767
3. ID2020 (2017), An Alliance Committed to Improving Lives Through Digital Identity. http://id2020.org/
4. Jacobovitz, O (2016), "Blockchain for Identity Management," Department of Computer Science, Ben Gurion University.
5. Meitinger, T H (2017), "Smart Contracts", Informatik-Spektrum 40: 371-375.

6. Posener, E A and G Weyl (2018), Radical Markets: Uprooting Captalism and Democracy for a Just Society, Princeton: Princeton University Press.
7. Rannenberg, K., J. Camenisch, and A. Sabouri (eds), Atrribute-based Credentials for Trust: Identity in the Information Society, Springer.
8. Tobin, A. and D. Reed (2017), The Inevitable rise of Self-Sovereign Identity, Sovrin Foundation, https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/