To ease the health-wealth trade-off, reallocate digital property rights

Dennis J. Snower (Global Solutions Initiative)
July 2, 2020 | Last updated: July 7, 2020

This Policy Brief is offered to the Saudi T20 process, as a recommendation to the G20 in 2020.

Contact-tracing and risk-tracing technologies could help ease the ‘health–wealth trade-off’ confronting many countries in the wake of COVID-19. But privacy and security concerns are preventing such technologies from being widely adopted. This Policy Brief suggests a way to ease those concerns by endowing individuals with property rights to the digital information that concerns them. A ‘self-sovereign identity system’ could assure users that their data would be exploited only for specified purposes, such as containing a pandemic. The data would revert to being private property once the pandemic is over.

Challenge

At present, countries around the world face a terrible trade-off between a health crisis and an economic crisis, which can be called the ‘health–wealth trade-off’. To avoid the health crisis, many countries have implemented lockdowns, which generate an enormous economic cost in terms of lost income and output (e.g. Portes 2020). This trade-off could be eased substantially through contact tracing, risk tracing, testing, isolating, and treatment.

‘Contact tracing’ involves identifying people who may have come into contact, directly or indirectly, with an infected person. The contacts of infected people can then be tested for infection; those infected can be isolated and treated; their contacts can be traced, and so on (Galeotti et al. 2020). Implementing contact-tracing would greatly reduce the need for social distancing, particularly if contact-tracing were supplemented by ‘risk tracing’, which involves dividing people into risk categories on the basis of readily available information, such as age, occupation, residence, workplace, and pre-existing health conditions (Mesnard and Seabright 2020). The effectiveness of contact- and risk-tracing can be enhanced significantly through the application of AI technologies in areas such as early warnings, tracking and prediction, visualisation, diagnosis and prognosis, monitoring crowds, and treatment support (e.g. Vaishya et al. 2020).

If AI-enhanced contact and risk tracing were implemented, social distancing would be necessary primarily for people who have not been tested and are in high-risk categories. Consequently, the health–wealth trade-off would be vastly improved because it would no longer be necessary for countries to send most of their residents into lockdown. Many people would return to work, with social distancing regulations becoming more stringent for the more vulnerable groups.

For countries where contact and risk tracing are feasible, people are generally willing to provide the requisite data in return for protection from infection, with three provisos: that others do the same, that their data are used only for the purpose of containing the pandemic, and that their data are adequately protected from hacking and malicious use. The great interest in providing data in return for health security is exemplified by the widespread attention and positive response PwC has received for its plans to deploy an Automatic Contact Tracing check-in app for its employees, also to be made available to its clients (e.g. Leswing 2020). Other companies, such as Locix and Microshare, are working on tools permitting not only people but the surfaces with which infected people have come into contact to be retraced. Such
initiatives will help companies reopen operations after lockdown by ensuring employees’ workplace safety. Though contact tracing at the workplace is certainly welcome, it is far less effective than systems providing comprehensive contact tracing throughout time and space.

In order for contact and risk tracing to become manageable in countries with significant infection rates, it needs to be done automatically through digital technologies rather than through personal interviews. Apple and Google have partnered to assist in contact-tracing through a system that includes application programming interfaces (APIs) and operating system-level technology. These companies also plan to offer a Bluetooth-based contact-tracing platform “that would allow more individuals to participate, if they choose to opt in, as well as enable interaction with a broader ecosystem of apps and government health authorities” (Government Technology 2020). The opt-in condition is meant to overcome privacy and security concerns. As Apple and Google emphasise, “privacy, transparency and consent are of utmost importance in this effort” (Apple 2020).

But the opt-in condition is expected to limit severely the uptake of this system. Opt-in policies produce far lower participation rates than opt-out policies in a wide variety of settings, from organ donations to pensions. This is so for a variety of well-known reasons: changing the default requires mental effort; the default is usually considered the preferable or acceptable choice; and people are more sensitive to losses than to gains relative to the default, making them more likely to retain the default. Governments and businesses are increasingly using opt-out design to promote socially desirable outcomes in many domains though not, as noted, in pandemic containment (e.g. Johnson and Goldstein 2003, Sunstein 2017, Thaler and Sunstein 2008).

Needless to say, contact tracing software is effective only when it is widely deployed. The system only has a high chance of detecting when a person in the system has been in contact with an infected person if a large proportion of the population has signal-emitting devices. Thus, the Apple-Google contact-tracing system is widely deemed unlikely to play a major role in tackling the Covid-19 pandemic in many Western countries.

The opt-in policy of Apple and Google with respect to their contact-tracing app stands in stark contrast to their standard policy with regard to the use of private data for advertising purposes, as well as derivative digital strategies designed to attract user attention. In practice, smartphones can be understood as surveillance devices, used by digital network providers (such as Amazon, Apple, Facebook, Google, Microsoft, and others) to target advertising individually to users. These users implicitly consent to this surveillance by agreeing to the digital services’ terms and conditions, which they rarely attempt to read and which they would be unable to read (with all hyperlinks to other relevant documents) even if they wished to, due to the time and effort required. In some cases, users have the possibility of opting out of some surveillance, but often in return for significant loss of service.

Currently, most people are highly sensitive to the potential misuse of their data with regard to contact tracing, but remain largely unaware that their smartphones are de facto surveillance devices for advertising and attention-capturing purposes. Since the digital network providers earn their incomes from pursuing these purposes, they have a natural incentive to keep this asymmetric awareness intact. Apple, Google, and other digital network providers’ sensitivity to privacy and security concerns in contact tracing is understandable.

Because policymakers are often afflicted with the same asymmetric awareness, or are unwilling to address the problem of surveillance for advertising openly, the central questions concerning the future of contact and risk tracing are never asked. How can users be given the opportunity to share information for containing the pandemic while safeguarding their privacy and security? Can the degree of surveillance that is standard for advertising also be applied to saving lives?

Proposal

To address these questions productively, we need to think beyond the existing institutional framework. The critical insight is simple: the current obstacles to trustworthy information sharing arise from a fundamental misallocation of digital property rights. In the current digital world, users generally do not have property rights to the data about them, not even to the data that they generate about themselves. This data usually belongs to digital network providers, such as Apple, Amazon, Facebook, Google, and Microsoft. Users are free to leave these networks, but information about users remains in the hands of the networks.

In the absence of individual digital property rights, it is not surprising that users are highly concerned about the privacy and security of their data. Living in a world in which much of the data about themselves are not in their own hands, they are understandably worried about the
possibility of making these data available to a new set of decision makers, including government agencies fighting the pandemic. After all, it is difficult to assure them that data which do not belong to them will not be used by third parties for other purposes.

The straightforward way of tackling this problem is to give users residual property rights to the digital information about them. This solution is feasible and implementable. People can be made ‘sovereign’ over their digital identities (i.e. the information representing them) by implementing a ‘self-sovereign identity system’ whose properties have been well-explored (Der et al. 2017, Tobin and Reed 2017; the economic implications of a self-sovereign identity system are described in Snower 2018). In such a system, each person is given a private digital key to certified, encrypted data about himself or herself for a potentially unlimited number of recipients who can access the data, provided that they have the corresponding public key. The system can be implemented through distributed ledger applications (such as blockchain) and smart contracts (e.g. Jacobovitz 2016, Meitinger 2017). These applications permit search for decentralised identifiers without centralised directory, so that data can be authenticated with decentralised, verifiable credentials. Digital identities need to be persistent, portable, interoperable, and secure (see Allen 2016 for a more detailed description of these requirements). Then each person can choose what information to share with whom and when.

The implications of giving users digital property rights

Property rights – in the digital world like in the physical one – are necessary for the proper functioning of market systems. For example, since we have property rights in our labour services, we are able to decide what work to do, when, and for whom. Without such property rights we would be slaves. Slavery is not only grossly inequitable (since slave owners have overwhelming market power over their human property), it is also grossly inefficient (since there is nothing to ensure that the slaves’ free sustenance – their food and lodging – reflects the value of their labour services). The current digital regime is also inequitable (since digital network providers have vastly more market power than their users) and inefficient (since there is nothing to ensure that the users’ free apps and other digital services reflect the value of the data about them).

The existence of property rights promotes efficiency and equity not just with regard to private goods and services, but also with regard to collective goods, such as contact and risk tracing, which could be used to contain the pandemic. As Elinor Ostrom and others have shown (Ostrom 1990, 2010, and Wilson et al. 2013), the commons can be managed efficiently and equitably when the participants affected by the rules participate (directly or indirectly) in making the rules; their rule-making rights are respected by outside authorities; behaviour is monitored; rule breakers face graduated incentives (sanctions or rewards); and dispute resolution is accessible and low-cost. For contact and risk tracing, along with the supportive AI architecture, this means that the technology needs to be transparent, time-limited, fair and inclusive, and accountable. Digital property rights provide a basis for meeting these objectives.

If people have residual control over their data – after the public interest in pandemic containment has been met – they will be more willing to make relevant data about themselves available for contact and risk tracing. After all, the self-sovereign identity system permits them to ensure that their data are used only for specified purposes and that the data become their private property again as soon as the pandemic is over. Their privacy and security concerns are powerfully addressed through the distributed ledger technology, which is far less vulnerable to hacking than the current digital networks, in which information is centralised.

Furthermore, once people have residual private digital property rights to the data about them, it becomes far easier to deliberate publicly through democratic processes about the circumstances under which these property rights need to be constrained in the national or global interest. The dividing line between private and social objectives becomes easier to draw, since the digital property rights permit the pursuit of private objectives. By contrast, users do not own much of the digital data about themselves in the current digital regime, leaving the distinction between the rights of the individual versus the collective blurred by privacy and security concerns.

Prerequisites for self-sovereign identity

In order to make a full-fledged self-sovereign identity system operable, governments need to provide the necessary infrastructure. This involves giving people access to convenient digital sources of evidence for the correctness of the information they provide and receive, procedures ensuring transparent consensus concerning the content and conduct of transactions, and systems ensuring consistent usage rights for the individual’s data (for how to implement this, see Rannenberg et al. 2015). Furthermore, governments need to agree on an international legal framework concerning certification, transactions procedures, and usage rights, in order for digital identities to function across legal jurisdictions.
However, there is no reason why a self-sovereign identity system has to be implemented comprehensively with respect to all goods and services, physical and digital, right away. As a first step, the system could be applied only to digital information relevant to contact and risk tracing. For these data, the underlying infrastructure should be readily achievable in many countries. In the most modest version of this system, individuals would own their own health records, which they could provide freely for research as well as for contact- and risk-tracing purposes (e.g. Tapscott 2020). In a more ambitious version, people could decide democratically to relinquish their digital property rights for pandemic-containment purposes.

In sum, without such a limited self-sovereign identity system, countries worldwide face an extremely adverse health–wealth trade-off, since a large-scale health crisis can be averted only through a large-scale lockdown that causes large-scale economic damage. This trade-off could be relaxed substantially through contact and risk tracing, together with testing, isolating, and treatment. The security concerns associated with contract- and risk-tracing technologies can be addressed through a self-sovereign identity system, applied in the first instance to fighting the pandemic. This would enable many countries to limit their lockdowns primarily to high-risk individuals who have not been tested for antibodies.

Even these lockdowns could be reduced further if countries would redirect their fiscal stimulus packages from passive support for the unemployed, furloughed workers, and struggling firms, to active support for restructuring production and consumption activities along lines compatible with social distancing. Such ‘re-adaptation policies’ (Snower 2020a, 2020b) are particularly important in recognition that the Covid-19 pandemic is accelerating the transformation of work (Baldwin 2020).

The stakes are extremely high. The time has come to address the worldwide health and economic crisis through a fundamental reform of the current digital regime.

Endnotes

1. As employees move around their workplace at PwC, their phones detect one another and the resulting data is anonymised, so that it cannot be linked back to the employees. On this basis, an infected person’s phone can be linked to all other phones that it came into contact with over the previous two weeks. The contact is rated as high, medium, or low, based on signal strength and frequency of contact. The contacted people can then be notified.

2. Furthermore, the exclusive reliance on smartphones (rather than electronic wristbands) makes the system vulnerable to misuse, since smartphones can be shared or stolen.

3. See, for example, Kaldestad (2016): “The average consumer could easily find themselves having to read more than 250,000 words of app terms and conditions. For most people this is an impossible task, and consumers are effectively giving mobile apps free rein to do almost whatever they want”.

4. In fact, these networks continue to collect information about people who are not network members, provided they interact with others who belong to the networks.

5. Examples of current initiatives in this direction are Ledger Insights (2020) and Validated ID (2020).

References


7. Kaldestad, O (2016), "250,000 words of app terms and conditions”, Forbruckerradet, 24 May.


11. Leswing, K (2020), "Companies could require employees to install coronavirus-tracing apps like this one from PwC before coming back to work", CNBC Tech, 6 May.


