FUTURE AGENDA

Open Foresight

FUTURE OF DIGITAL IDENTITY

Insights from Multiple Expert Discussions Around the World

FUTURE AGENDA

Open Foresight

FUTURE OF DIGITAL IDENTITY

Insights from Multiple Expert Discussions Around the World

Empowering the individual

After a first encounter with the idea of Digital ID as a digitised passport or ID card, it is easy to miss the ways in which it could fundamentally transform the human digital experience, and our future in a data-driven society. But it could, and likely will. In this section we explore the emerging view that Digital ID could be a tool of empowerment, providing, for example, universal access to services, or by rebalancing the current digital and data paradigm in favour of consumers and citizens.

Re-assessing self-sovereignty

The idea of 'self-sovereignty' has taken on something of a life of its own in relation to Digital IDs. The introduction of an idea as lofty as 'sovereignty' can be both a help and a hindrance in understanding such a complex subject. On the one hand, it helps to introduce the importance and centrality of both agency and control. On the other, it brings yet another contentious concept to an already crowded field. Perhaps the desire to talk about sovereignty stems from two things: 1) the loss of control that many feel in the current development of digital societies, and 2) that if we are to have sovereignty over anything in a digital world, it should surely be 'who we are'.

Without wishing to get lost in the arguments and counter-arguments over whether a truly 'self-sovereign' ID can really exist (can we really self-certify?), there are two practical aspects of the debate that might be useful to borrow from. The first is in relation to the control and management of an ID itself i.e. where it is physically located, and where attributes are stored. The second is to do with how much control we might have when sharing those attributes.[27]

such as storing data on individual devices and/or various models of distributed and decentralised networks and ledgers, encryption tools, blockchain implementations and so on. Each presents challenges in terms of implementation and each has flaws when considered either against an idea of absolute sovereignty, or the need to recognise the fundamentally social aspect of ID (namely, that our claims to being who we are don't mean much if no one else agrees with us)[28]. However, they are bound together by the ambition to decentralise the Digital ID eco-system, keeping individual ID data packages out of centralised databases controlled by large organisations (corporate or governmental). The most important aspects of all of these proposals then, is that they each aim to enable the second aspect of Digital ID sovereignty: giving individuals a measure of control over how data is accessed and shared.

Agency and control will not just be about allowing individuals to store or move their data however, it will also be about how Digital ID applications are designed and built. For example, attributes within Digital IDs could be constructed so as to protect certain fundamental aspects of our identity, and yet still give the necessary confidence to others that we are who we say we are or have the rights and attributes we claim to have. Our dates of birth could be translated into the 'entitlement to buy alcohol' or the 'right to a child's fare'; our names could be obscured by unique identifiers, and so on.

Further, the interfaces of Digital ID applications could help to provide individuals with a far greater level of transparency when taking part in personal-data transactions than is currently the case. For example, Digital ID transactions could be designed such that they must involve ID holders being told exactly which attributes they are being asked to share, when, with whom, and for what purposes. Individuals could then also be given granular control over whether to share some, all or none of the attributes, as they wish.

These kinds of mechanisms would vastly increase an individual's control over the amount of personal data and information that flows from them, to others[1], and building on this principle, we can imagine significant changes to what is currently considered normal during digital interactions. Digital ID driven digital journeys could involve for example, regular and secure access to digitally-delivered services without disclosure of who we are, the ability to navigate social or commercial digital spaces 'incognito', and/or regular alerts to notify individuals when their data is being requested, used or gathered[2].

The importance, as one advocate of self-sovereignty in our Australian workshop argued, is not to consider sovereignty in its strictest sense, but to distinguish between the ways personal data is currently allowed to flow unhindered in the data-economy, and the ways that Digital IDs could change this: "Digital ID data will (need to) be removed from the data stream, in order to protect it from the 'open' ways in which the digital economy is developing." The way to achieve this is to allow individuals to be the gatekeepers of their personal data. At its simplest, this is an expression of the idea that the proofs of who we are, should not reside in the hands of those who can exploit, process (to their own ends), share and even lose them.

One other potential aspect of future Digital IDs that could see individuals empowered is the ability, during a digital transaction, not just to have control over the requests made by others, but also to make requests of our own. Just as others may want to verify that we are who we say we are, we may equally wish to verify that the other side of a transaction are who they say they are. There are huge benefits to this in terms of cybersecurity, with many standard phishing attacks, for example, being potentially rendered obsolete by such requests. Most criminals would likely be unable to prove that their nefarious digital properties (emails, websites etc.) actually are what they pretend to be, for instance.

At an everyday level too, there could be very practical benefits to this two-way exchange of identity. Imagine, for example, finding health advice online and being able to verify that an advice-giver really does have the associated medical training, as proven by their Digital ID; or confirming that a local plumber has the right certifications for the job in hand; or that someone you are speaking with is a person and not a robot. The list is potentially endless. Even in our relationships with bigger organisations and corporations, the ability to demand proofs could foment a wider cultural change. We may begin to demand and expect more transparency; first in terms of credentials perhaps, but later in terms of the longer-term uses of our behavioural data, and whether or not so much of our data is needed in order to deliver the service we are seeking.

Perhaps, the most important aspect of all the excitement around the concept of 'self-sovereignty', is not in whether or not a given implementation is practical or possible or 'true', but in its ability to provide a benchmark for Digital ID propositions. 'Sovereignty' could be seen as an idealised standard around individual agency and control against which new Digital ID innovations and technologies can be measured, alongside existing measures such as privacy, security and trust.

Digital rights and consent management

Up to now, we have largely discussed the role of Digital ID in terms of its ability to provide digital assurances during digital transactions, but there are other powerful things that a Digital ID in an interoperable system could do. Building on two ideas that we have already introduced - 1) that trusted systems of digital attribute sharing could mean that we need give far less information than is currently the case, and 2) that Digital IDs might be able to attach 'provenance notes' along with data or attributes - it is possible to imagine a future for Digital ID as a kind of digital rights manager and monitor. The easiest way to illustrate how this might change things is to compare against the way things often work today.

When we choose to access digital services today, we are often asked to create accounts. In fact, each account we create actually gives rise to a new digital identity. Accounts give us certain benefits, such as being able to store photos, or allow communications and connections with the service provider or other account holders, store transaction histories etc. Accounts are also of great benefit to service providers. They provide the ability to track individual user behaviours, and deliver more personalised services, or more targeted advertising.

In the case of the tech giants, this assigned identity (like the digital entities described in the opening chapter) means they can monitor our use of a whole eco-system of different services, triangulating data to create an ever deeper and richer picture of who we are. These deep and rich data sets in turn give those companies the power to explore new kinds of products and services, or even enter into and disrupt other industries. The more accurately we can be identified within digital spaces, and the more accurate the personal information associated with us is, the more valuable all of the vast amounts of associated data collection becomes. The question is whether the value exchange is truly transparent, whether we can weigh the future consequences of immediate decisions around sharing data and creating a digital identity and whether we have as much ongoing control over these new identities as we might want.

Often, if we want to access digital services, we have little choice but to agree to the terms and conditions that allow this invasion of our privacy and the creation of a digital identity on our behalf. And if the sign-up process also demands that we give certain stronger identifiers such as our phone number, we have little choice but to comply. Furthermore, having done these things, the conditions for a 'lock-in' situation in which we have invested so much into one service that it becomes more difficult to move out, or to another, are also created.

Digital ID has the potential to change this paradigm. In one simple scenario, we can imagine being given an option, during sign-up, to use our Digital ID instead of creating a user name and password (or whatever is being asked for). The service provider could then send an instruction to our Digital ID asking for certain identity attributes from within it in order to set up an account. At this point the Digital ID presents us with a series of options for using the service. Would we like to do so anonymously, without sharing any personally identifiable attributes, or only some? Or do we want to be clearly identified (perhaps in order to access or make best use of certain aspects of the services on offer)? Do we want the service to monitor, store and process our usage data or not? Do we want our data to be made available to other parts of the company's eco-system, or external partners? Would we like to move our data wholesale from this service to another? And so on, depending on the particular service being offered. It is worth remembering that even if we opted to remain relatively anonymous, the service provider would still be getting the advantages of confidence that they can strongly identify us as returning entities, due to the use of a Digital ID as a way of signing in.

At first blush this scenario seems unlikely. Why would service providers allow us to remain anonymous and have privacy options so clearly demarcated? What's in it for them? And, given what we know about current digital behaviours, wouldn't consumers simply opt for the most convenient options that give them access to the greatest number of services, foregoing, as ever, the option of greater privacy?

True, if we think about the larger data-driven service providers like Google and Facebook, there is little incentive for them to create such a scenario; but for competitors, smaller providers and start-ups, giving users the ability to transparently exercise data rights might be a very positive point of differentiation. Furthermore, even if larger service providers didn't want to allow user anonymity, they might still want to allow users to create accounts using their Digital IDs[31]. This would, at the very least, trigger a transparent process around the attributes being requested, requiring users to actively engage with, and give permissions around, their usage, rather than blindly clicking an 'I agree' button. In a world of interoperable Digital ID, in which we all carry familiar tools that enable us to make fast and convenient choices around the ways our data is collected, stored and used, the idea of hiding privacy erosions behind long pages of terms and conditions will likely become less and less acceptable. Ultimately, thanks to a Digital ID eco-system, choosing privacy, and/or providing truly informed consent, could become just as convenient as not doing so.

If the above scenario applies to the passive collection of our data, then along similar lines, we can also imagine scenarios for active personal data sharing. By using a Digital ID as the interlocuter in a process of sharing personal health data with insurance companies or healthcare providers, for example, it could become possible to attach not just provenance notes along with chunks of our data (as we discussed previously) but also a set of instructions or permissions determining how the data can be used, by whom, and for how long. In an even more complicated scenario (that some Digital ID providers are already working on) Digital IDs could even act as a gatekeeper to user-controlled and maintained personal data stores. Data processors could be allowed to access the data-store, or send algorithms inside them to carry out data-processing, but only under strict and explicit conditions, such as 'no removal of raw data', 'no use of personally identifiable information (PII)' or 'only time limited use of data', etc.

An early analogue of how this might all work can be found in the more detailed cookie-consent tools that have sprung up on websites since the arrival

CASE STUDY: Personal data stores and Digi.me / Solid

Putative ownership is a helpful tool for managing personal data even if an organisation you share with goes bust, or the relationship is suspended. The control that ownership gives you is helpful for managing misuse and fraud (i.e. it is in your hands, not in the hands of multiple others).

In the case of Digi.me for example, individuals receive a copy of their data after which they can then selectively grant data access to apps that they choose from the Digi.me ecosystem. Businesses and individuals within the Digi.me environment gain access to volumes of normalised data with the possibility of creating apps – such as consolidated management of all social media history in a single location, or access to, and processing of, personal health records.

Solid, a de-centralised web movement backed by Tim Berners-Lee is part of a growing effort to reinvent the web such that it can realise the goals imagined at its inception. One of the critical components of this reinvention is identity. Solid, includes a component whereby users are given the option to login with their Solid 'Pod', instead of a myriad of web logins, with various websites/organisations. Individuals are said to truly own the data in this pod and are provided with the tools to give permissions to entities and apps to read or write to subsets of it.

of GDPR, which allow granular and transparent permissions to be set regarding the placement of cookies on web browsers. These tools are cumbersome today of course, and likewise early implementations of digital rights and consent management within Digital IDs would also exhibit signs of over-complication. But it would be wrong to dismiss these wider potential roles of Digital ID as being pie in the sky. For one thing, already today the principle of using Digital ID to manage and exercise digital and data rights (at varying scales) is being adopted by a significant number of Digital ID stakeholders, with rallying calls especially focussed on the promise of providing greater privacy. Ever more sophisticated, and user-focused consent management tools are also already being developed in both the private and public sectors. In the longer-term we could see the development of new technologies (automated AI-driven, consent managers, for example), that make even exercising complicated data rights, a matter of convenience.

The immediate future is not likely to be a sudden change in the data economy paradigms of today, but about recognising the critical role of Digital ID in giving power back to individuals in an ever-evolving data infrastructure. Of course, this will require today's fast-moving inventors and entrepreneurs to think carefully about the tools they are creating. Ensuring that they will deliver on the promise. AI-driven Digital ID assistants or consent-managers for example, should not further erode individual agency

CASE STUDY: Digital consent management and Hu-manity.co

Digital consent management is the ability for entities to grant permissions with regard to use of their data. This issue has received greater awareness in recent times by the arrival of legislation like GDPR in Europe. A typical exchange when a first-time visitor visits a website for example, involves a pop-up window asking about use of their data with, say, advertising partners.

In some cases, users are given a 'pick list' where they can choose options on what data is shared with which partners. But outside of this system, vast volumes of inherent user data – driver and vehicle history, consumer spending habits, medical history, etc. - is gathered, bought and sold by various parties on a regular basis, without much in the way of meaningfully informed consent or transparency.

Consent management could be an important aspect of digital identity. Of particular interest to some is the ability to alter consent details over time and critically, to be able to 'walk away' and not be tied sharing data endlessly.

Hu-manity.co have built a mobile app, #My31, that gives users enhanced ability to control their data and to have a say in how it is used by others. They see users having ever greater awareness of how their data is being used and aim to meet a growing demand to be able to manage this. They see this as the '31st Human Right'. The core of the mission of Hu-manity.co is to ensure that individuals can claim, via #My31, that their data is respected as their legal property.

The result for users is that they can grant explicit consent to organisations on specific use of data, and enjoy a greater level of informed consent or privacy. Once a critical mass of users join the movement, Hu-manity.co claims that it will fight on behalf of users for reward /compensation opportunities with key industries, such as healthcare and insurance.

by allowing an all too *convenient* outsourcing of decision-making. But with due consideration (and there are many voices or parallels from other sectors[32] to help guide in this regard) Digital IDs and suites of Digital ID tools could change our digital futures for the better.

There is one final and different sense in which future Digital IDs are likely to act as rights managers. Most of the documents that we currently use to prove our identity today are actually primarily the means by which we can demonstrate various entitlements: a library card entitles us to access libraries and borrow books; a passport entitles us to travel freely across borders; and national ID (digital or otherwise) confers the rights associated with citizenship etc. The other attributes they contain are used to establish our identity; that we are indeed the holders of those entitlements. In the future, a single Digital ID might be able to do the job of identification for a number of different institutions, organisations in a number of different contexts, allowing us to combine the proofs of many different entitlements in a single place (or into a single tool).

In this way, much the same as a lack of access to legal identity documents today can hinder people's ability to access services, so too a lack of access to Digital ID in the future could become detrimental to a person's ability to get on in life. Ironically perhaps, whilst many of the access rights and entitlements that a Digital ID accumulates may never be considered fundamental rights on their own, the right of access to a Digital ID itself, could well become so[33]. Digital ID systems could come to be seen as being part of a society's critical infrastructure, with wide-ranging implications for the ways in which public, private and third sector Digital ID stakeholders are managed and regulated.

This normalisation and centralisation of Digital ID to society would have an impact on the day-to-day realities for Digital ID stakeholders. With an ever-growing user-base, inflating lists of attributes, and an emergent set of Digital ID rights, the future might not be one of constant user amazement at miraculous instant access to digitally delivered services, but rather the more mundane management of a growing set of issues around how access rights and entitlements are issued, revoked, restored and redressed in a Digital ID eco-system. Even today it is possible to see how messy some of these day-to-day issues are likely to become.

Theoretically a Digital ID could contain attributes gleaned from multiple sources, and even some which are extrapolations of other attributes. If so, where would responsibility lie for ensuring that each one is properly maintained? As one participant in our London workshop pointed out, with reference to a real-life case-study, such issues could become very tricky indeed. If someone, for example, demonstrates a repeated pattern of behaviour which involves abuse of their Digital ID and the attributes it contains, should they have their right of access to a Digital ID permanently revoked, or only parts of it? And what is the relationship between any actions taken in regard to their specific Digital ID, and other forms of ID (digital or otherwise)? Should records of whatever action is taken against them be kept in the ID itself, or removed elsewhere? And should such records be permanent or temporary? Would there be duties of disclosure and how could they be enforced? All of these issues will need to be thought about carefully in the rush to create new Digital ID products, in order to avoid the need for radical re-engineering down the line.

As a final addendum to the idea of digital rights and identities, we perhaps should also consider the right to be 'un-digital'? The arrival of Digital ID as a channel for individuals to express their desires to opt in or out of various digital exchanges and transactions, is likely to raise the idea of being allowed to opt-out completely. How this might be effected in a world of spreading sensors, mass data collection and biometric recognition is not clear today, but the need to serve those who wish to do so may come with a moral imperative if not yet a practical solution. Could Digital IDs become a mechanism for monitoring the erasure someone's wider digital identity?

The inclusion illusion

During our workshops there were varied and contradictory responses to the idea that the clearest need, and perhaps even earliest true Digital ID implementations, would be found in non-traditional markets for new technologies; namely, those who are most socially and economically disenfranchised. Roughly speaking, there were three types of responses to the case for 'digital inclusion':

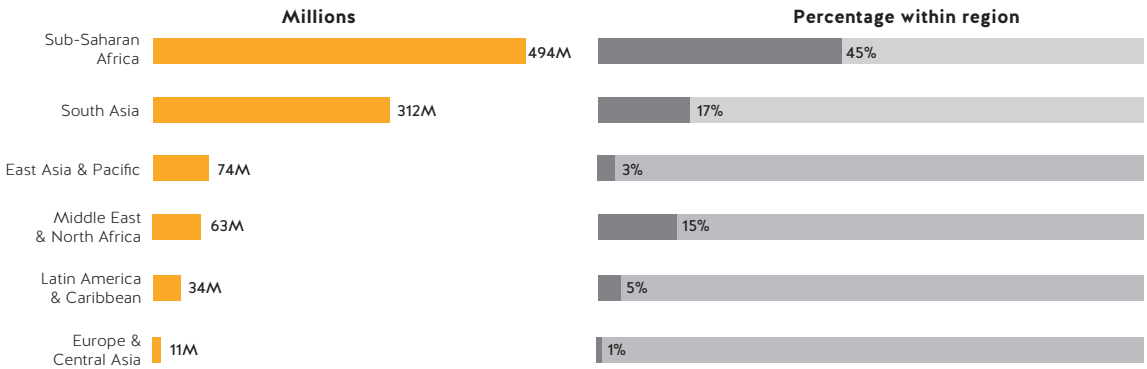
1. We should follow the UN's development goals in recognising that the vast movements and forced displacements of populations all around the world is creating a crisis in terms of legal identity. Those developing the future of Digital ID should make addressing the issue a high priority, since it is the most obvious area of consumer (or rather 'citizen') need.

2. Providing legal identity to the millions of people who currently lack access to legal identity services is important, but their needs are not enough to lead them to being among the first wave of Digital ID users.

3. Digital ID is a red herring in the issue of societal inclusion (or vice versa). Digital ID has long been touted as a solution to the identity access problem, without leading to any clear solutions. Access to Digital ID will ultimately follow on from conditions of greater social inclusion and equality of access, and the maturity of a Digital ID system to the point of being able to facilitate this, rather than the other way round.

There is validity to all of these positions. It is ultimately a question of emphasis. Is the future of Digital ID inclusion going to be most influenced by the technical and social difficulties of implementing robust enough Digital ID solutions for marginalised populations? Or is the future of Digital ID inclusion going to be primarily driven by the need to address an urgent societal problem[35]?

There are an estimated 1 billion people without an official proof of identity worldwide. Close to half of them live in Sub-Saharan Africa, where almost one in two people lack a form of ID



Source: ID4D-Findex Survey Data 2018[a]

[a] The report and data presents economy-level aggregates on the share and number of the population without a foundational/national ID, based on surveys covering over 100,000 people in 99 economies—representing 74 percent of the world's population.

There is perhaps another red herring hiding in this whole question however; in the language used to describe the socially disenfranchised. By referring to the idea of 'inclusion' or to the 'marginalised', or 'disenfranchised', we set up a false dichotomy between an idealised 'consumer' or 'citizen' on the one hand, and 'people in need of help to access' on the other. When it comes to Digital ID this is misleading in a number of ways. First, there is no a hard relationship between people's ability to access services and their need for them. In any society people have greater and lesser access to, and need for, different services, and are more and less engaged with existing digital services. Second, if we consider the populations of (even undocumented) migrants living outside of their home states, then in many cases we are talking about people who may have once had far more privileges than they do now. In fact, they may at one time, have enjoyed far more access to various opportunities and services than do parts of the population in the states they now find themselves in. This means that they should not necessarily be sharply distinguished from those more naturally considered the most natural markets for Digital ID. Third, if markets are at least in part about demand, then what matters might not be who is 'different' or which market segment is 'difficult to address' or who needs to be 'included', but rather where that market demand lies.

Whilst it is easy to think of situations in which a Digital ID would be useful, or more convenient, for many of us, it is harder to think of single use-cases that are 'vital', or that might require us to produce our Digital IDs frequently. Indeed, the more ambitious Digital ID stakeholders are seeking to circumvent this problem by solving for many use-cases at once. The situation and demand profile might be look different however, among those who rely on, say, government services to meet basic needs. We need not look to populations of undocumented migrants or displaced populations

CASE STUDY: Welfare delivery and UK Universal Credit

The UK's Universal Credit (UC) programme is one example of Digital ID assisting with welfare delivery. At its core UC aims to combine six welfare payments into one and in theory represents efficiencies in service delivery for both government departments as well as recipients.

The programme has however suffered from delays. Some of that rollout delay has been due to the attempted incorporation of a Digital ID. Issues – understandably perhaps - include users not always having access to key information or documents - such as a passport or driving licence or other photo identification - which can hamper their success when signing up to the digital system.

At the outset, Universal Credit used Verify, the UK Government's digital identity service, as an alternative for face-to-face identification, but only 1/3 of welfare applicants were successful in using that system. The Department for Work and Pensions (DWP) responded by creating an in-house verification system – "Prove your Identity". However even this only brought the digital user sign-up success rate to c. 50%.

alone to find those who *are* frequently asked to produce identity documents to unlock access to services today. They live everywhere. The illusion lies in the idea that 'inclusion' is only about those at the extremes.

In fact, it is this level of need amongst those who frequently use public services that is perhaps driving the development of government ID solutions around the world. The best example, for all its faults[36], is perhaps the "Aadhaar" ID system in India. The driving purposes and goals behind the development of Aadhaar were as diverse as described in the opening sections of this report, but the potential for the system to give efficient access to government services and enhance the delivery of welfare provisions by the state, were front and centre. Aadhaar may not present an ideal form of a Digital ID eco-system to many Digital ID technologists and stakeholders, but what it is, is a Digital ID system that has seen mass-adoption and usage[37]. Following Aadhaar's lead, it is perhaps no surprise that today, one of the first places to look for functioning Digital ID systems (if not interoperable systems) in any country, would be in their processes of welfare delivery.

Arguments over the need to focus on 'digital inclusion' aside, the longer-term impacts of Digital ID for disenfranchised populations are worth considering. If access to large-scale Digital ID eco-systems remained off the table for stateless, itinerant or marginalised people, then could smaller-scale initiatives temporarily fill that gap? Rudimentary Digital IDs that allowed people to verify themselves as 'returning customers' through the use of digital tokens, or Digital IDs with very few attributes that could be used to provide access to basic humanitarian services, for example, could see wide-spread adoption. This might in turn lead to increasing participation by larger ID providers, growing the legitimacy of such systems over time. This raises an intriguing prospect, particularly for stateless people, that the 'pseudo-citizenship of nowhere' that a Digital ID may itself provide, could come to be seen as the focal point for a new form of social identity, belonging and even organisation: formally ascribed 'stateless netizens' for instance (?).

Contact details

To discuss this project further please get in touch

Dr. Robin Pharoah

Director | Global Insights

Future Agenda

robin.pharoah@futureagenda.org

www.futureagenda.org

@futureagenda

FUTURE AGENDA

Open Foresight