FUTURE AGENDA

Open Foresight

FUTURE OF DIGITAL IDENTITY

Insights from Multiple Expert Discussions Around the World

FUTURE AGENDA

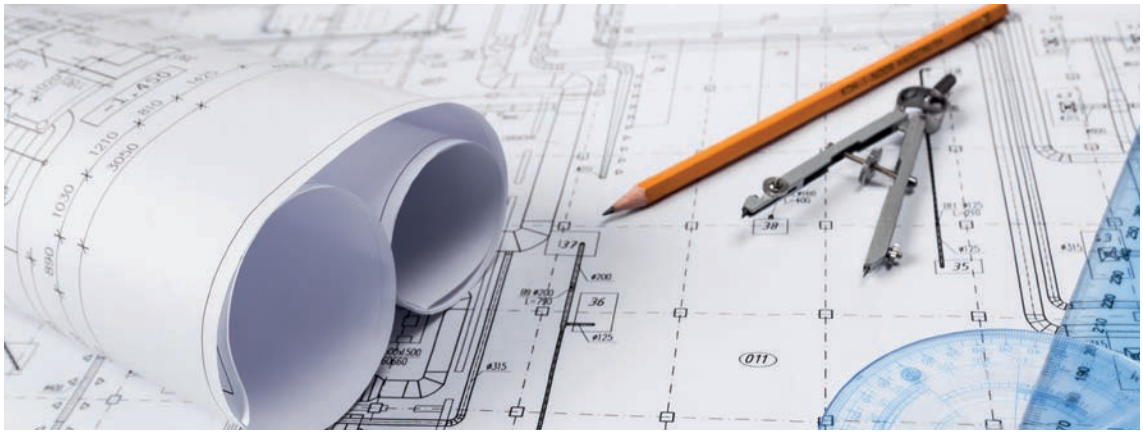
Open Foresight

FUTURE OF DIGITAL IDENTITY

Insights from Multiple Expert Discussions Around the World

Eco-system development

At the time of writing, the number of Digital ID technologists and technologies, investors and stakeholders, interested parties, working papers, white papers, and fledgling products and services is mushrooming. Given that the idea of Digital ID (especially with regard to more mundane IT access-management technologies) has been around for a long time, and its history is already littered with aborted attempts to get it off the ground, it is unclear where exactly we might be in a putative Digital ID 'hype-cycle'. No doubt many of the current crop of ideas and initiatives (good and bad) will inevitably fall by the way side. Further, given rapidly changing public attitudes to the use of personal data, and the global rush to regulate the same, uncertainty is perhaps the only certainty going forward. That said, it is interesting to consider the less-immediate possibilities for future Digital ID eco-systems. Some may be more likely, others may be more interesting, each could provide a potential strategic direction or way-point for different stakeholders.



Development overview of digital identity

Microsoft Passport

Identity 1.0 – First stage Single Sign On (SSO) technology

c.1995

facebook

Identity 2.0 – Social identity used for logins

c.2010

PayPal

Identity 3.0 – Real identities mixed with virtual activity

c.2015

DIGIDENTITY

Identity 4.0 – Personal identity providers & ecosystems

c.2018

Multiple bets

One perhaps surprising aspect of Digital ID to newcomers to the field, is that, despite the technological complexities involved, it can actually be approached from many different angles and by many different types of organisation. This has meant that there is now a panoply of Digital ID stakeholders and participants that come from many different industries and sectors, each with their own particular take on what should be done, and for which set of reasons. One way of characterising this might be to say that it is a landscape of 'multiple bets'. These bets aren't just about which particular 'horse' to back in a race however, they are also about which type of race has the right type of horses, and whether the gambler shouldn't also be considering greyhounds.

'Digital ID stakeholders' is perhaps too broad a term to describe those that are actually placing bets in the market, as there are many potential stakeholders who, while interested in the outcomes and likely to make use of emerging technologies, are not interested in actively playing a part in development. Those stakeholders that are more active however, might be (very) crudely placed into a typology something like this:

Type	Description	Examples
Incumbents	Bigger organisations that already play a significant role in traditional identity systems and/or already carry out a large number of identity transactions, as well as: assigning and verifying attributes, controlling secure and authenticated digital transactions, collecting large amounts of personal data that could be used to identify people in different digital contexts.	Governments and public service providers Banks and financial institutions Payments providers Personal-data-driven tech companies Telcos Device manufacturers Credit and other data bureaus Retailers
Idealists	Those motivated to create Digital ID products and services that serve an ideologically-driven or politically-driven purpose such as: enfranchising undocumented populations, preserving privacy in surveillance societies, or enhancing cyber-security, self-sovereignty and data control.	Digital activists Rights activists Ethical tech start-ups Third sector organisations UN World Bank
Technologists	Those with access to expert technical knowledge or technologies that are critical to the development of strong Digital ID systems.	App and systems developers Cryptographers Cyber-security and access-management experts Blockchain advocates System hardware providers
Opportunists*	Those with access to useful components of a Digital ID system, such as large quantities of personal or identifying data, other large data-bases that could form the basis of an identity system, an existing form of ID or ID service, a compelling use-case or view of an unexploited market segment, and/or an abundance of public trust in a brand.	Cloud service providers Entrepreneurs Postal services Niche legally-restricted service providers (gambling, adult entertainment etc.) Internet of Things ecosystem participants Government service providers (including QUANGOs, NGOs and private sector providers)

*We intend absolutely no negative connotation to this term whatsoever

There will be active stakeholders who overlap these different segments of course, but these crude generalisations perhaps provide a useful way of demonstrating the number of different potential entry points into the field.

For the incumbents, aside from National ID schemes, perhaps the clearest currently available articulation of the options for a fully functioning interoperable Digital ID system, are laid out in the World Economics Forum's "A blueprint for digital identity" (2016). This enormously comprehensive document lays out both the technical components of an interoperable Digital ID system that would realise many of the ambitions for Digital ID, but also a clear argument that the sector best placed to make this happen is the financial services sector. There are roles for others in the system, but ultimately the primary focus is on leveraging both the existing financial digital infrastructure and the experience in building robust identity authentication systems, to build the functional 'rails' for a truly interoperable Digital ID system. Similar arguments could perhaps also be made for the potential role of Telcos[56].

A different kind of case for a central role in the development and delivery of a national, interoperable Digital ID system on the other hand, might be that made in the Australia Postal Corporation's "A frictionless future for identity management" (2016), which focuses not on any existing management of authentication or identity but instead on their unique position as an intermediary between public sector and consumer services: *"Australia Post has an incredible, trusted brand, which is really important when it comes to identity, but it also has unrivalled footprint through physical shopfronts and online engagement," comments BCG's Schwartz on the partnership. "It's hard to think of an organisation that's better placed to realise the vision."*[57] This might be an example of 'opportunism' in the market.

What each of these larger visions has in common is the assumption that governments will play a key role in the development of any meaningfully comprehensive Digital ID eco-system. During our programme, participants from across different markets seemed to concur with the inevitability of a twin-track for government and private sector in the development of Digital IDs. Interestingly these pathways didn't always relate to the same facet of the Digital ID eco-system. For example, in one conversation in Australia the twin-track approach was applied to the development of protocols and standards, whilst in London the same twin track was seen as necessary to the development of ethical standards and regulations, whilst in Singapore it was seen as a necessary path to user adoption. As was pointed out more than once, it is not just about the likely necessity for government and government services to be involved in contributing and verifying individual attributes in individual IDs, it is also about incentivising the market (through investments), leading the development or endorsement of regulatory frameworks and protocols, and even catalysing the whole process by using the blunt instrument of a simple mandate for citizens to have Digital IDs.

Of course, National ID schemes have been in the realm of many government plans for some time. Consider, for example, that when governments focus on digitising services and require secure identification during sign-up and login processes, or when they include an electronic component in a National ID Card (or eID), they are in effect already pursuing a version of Digital ID. Some governments are also already leveraging the market penetration of mobile devices to introduce m-IDs. The digital security company Gemalto claim that over 60 countries have put in place digital national identity schemes and that most of these already also issue eIDs[58]. A 'compare and contrast' of all these systems is difficult, thanks again to the technical complexities and shades of grey when it comes to defining Digital ID, but it is safe to say that results have varied considerably. In the chart below, we have illustrated a selection of national ID schemes in order to give a sense of the range of offers.

System	Location	Of note
DigiID	The Netherlands	Has been mandatory for tax form submissions since 2006
.beID & itsme	Belgium	Both Ecard (.beID) and mobile-based (itsme) digital identity are present
eCitizen	Kenya	One login to access all government services
EEsti	Estonia	Seen by many as at the vanguard of National ID schemes, 98% of Estonians have an eID card and 67% use it regularly.
Nadra	Pakistan	National Database and Registration Authority (NADRA) was established in 2000 with aim to build a civil register of all Pakistanis. Among other features are a centralized Data Warehouse, supporting Network Infrastructure and National ID cards. Over 100m cards have been issued.
BankID	Sweden	BankID is the leading electronic identification in Sweden, with circa 7.5m people using it for a variety of private and government services. A signature made with a BankID is legally binding.
Singpass	Singapore	Launched in 2003, users gain access to over 60 gov agencies
My Number	Japan	Introduced around the end of 2015 with the aim of providing all residents of Japan with an individual number ID. While not mandatory, residents are encouraged to apply as the government hopes the system will help to reduce red tape and bureaucracy. A 2018 survey indicates that just over half of citizens haven't yet taken the offer of the card, nor do they intend to.
Gov.UK Verify	UK	Verify went live in 2016 as a means of providing online identity assurance for government services – has not yet been widely used. The government recently announced a policy shift to focus more on private sector taking greater responsibility for its development and usage.
Aadhaar	India	Any resident of India, may voluntarily enrol to obtain Aadhaar number. It is only program of its kind where a digital and online ID is being provided free of charge at great scale. In early 2018, there were 1.17bn Aadhaars assigned; just over 89% of the population.

Beyond nation state identity programmes, the UN in particular is a key driving force behind a different narrative describing the urgent need for Digital ID to provide a solution to the humanitarian issues around displaced and stateless people who lack access to legal identity documents and therefore critical services. Their calls are echoed by the World Bank and their "ID for Development" (ID4D[59]) programme. These supra-national voices are joined by independent funders and investors such as the Omidyar Network[60] and their work on developing the principles of 'Good ID'. By the standards of national ID schemes and the vision of globally interoperable Digital ID systems based on international financial mechanisms, these efforts may appear smaller, but large-scale, global institutions like the UN may also bring the power of governments to bare on their particular project.

Outside of these larger efforts, and among the idealists and technologists, there are countless smaller, ethical-, technology- and market- driven start-ups and projects, as well as a collection of long-standing identity protocols and initiatives (such as the FIDO Alliance[61]), each with different stated goals and missions. These are likely to continue with or without immediate government intervention and partnership, and may have as yet unknown roles to play in the future, as larger schemes come to fruition.

The landscape is rich indeed and it is hard to believe that, given current momentum, all will fail. Following various interviews with stakeholders from across the spectrum however, we were left with the impression that there was a risk of different stakeholders not fully understanding the motivations and missions of other stakeholders. This was especially true when it came to understanding those stakeholders who were coming at the Digital ID challenge from different perspectives to their own. This has implications for the speed at which different stakeholders might come to the point of co-operation. It may also mean that different

players may not fully recognise the successes or breakthroughs others may have already made, due to misunderstanding what success looks like from a different perspective.

The point of characterising the landscape in terms of 'multiple bets' then, is to suggest that we cannot well predict who the winners might be, or rather which models, which technologies, which priorities and which collaborations will come to dominate in the future.

One possible scenario is that a number of different bets pay off, not just because they are not necessarily mutually exclusive, but because the apparently monolithic nature of the internet will begin to show its cracks and seams, splitting into different islands, with different regulatory frameworks, data siloes, and digital-cultural norms. As we write, there are a number of factors pushing in that direction, such as concerns over data sovereignty, the increasing desire by governments to control the flow of information across borders, fears over cyber security, a growing citizen and consumer led movement to opt-out of surveillance economies and polities, etc. The internet is perhaps already an agglomeration of different connected systems, rather than a monolithic whole, but in this scenario the splits will become very real, and the boundaries will become more significant thresholds marking out different worlds. In each world, different norms and protocols around identification and the use of Digital ID could dictate which models (and Digital ID products and services) can be used where, and which can operate across boundaries, and which cannot.

We can already see nascent signs of this happening, with digital walled-gardens already being planted: China's great firewall, the dark web (with Tor encryption protocols acting as a gateway), and the beginnings of distributed internet models such as IPFS[62] and Sir Tim Berners-Lee's work with Inrupt and Solid[63]. In this scenario, it is possible that regional or contextual partnerships and alliances could provide the biggest driver of regionally, rather than universally, interoperable Digital ID systems. Trade-blocs for example, could be instrumental in the drive to develop Digital IDs that are interoperable within their borders in order to facilitate economic activity among partners[64].

Different bets could also lead to the rapid emergence of new and disruptive business models, standards and protocols either directly or indirectly related to Digital ID. For example, the ever-growing number of 'smart' objects that contribute to the Internet of Things (IoT) is already requiring a massive expansion in digital infrastructure to accommodate vast increases in the number of connected digital entities (and therefore identities), often occupying the same digital spaces as people. Could the globally recognised protocols and standards around IoT identity management be built and adopted at scale far more quickly than those necessary for interoperable human Digital ID systems? Thereby providing a framework into which Digital ID could eventually be 'reversed'? Even more speculatively perhaps, could the advent of digital technologies implanted in human bodies mean that the IoT, and its identity management systems, simply come to include people, precluding the need for Digital IDs?

More realistically (although equally controversial to participants in our programme) is the idea that if Digital ID products and services increasingly become the means by which personal data is stored and shared, a growing number of businesses could opt to create 'data-less' business models, reversing the current land grab for personal data, reducing business' personal data liabilities, offering privacy and security to customers, and yet still offering powerful services, in some cases even highly personalised services enabled by ad-hoc, and temporary, algorithmic access to personal data-stores.

The point perhaps, is that Digital ID, in whatever forms it comes to fruition in various markets, could come to be the pivot around which significant changes to the data marketplace take place. It is a powerful technology and as such is likely to usher in a whole new breed of data services, and digital cultures, some of which might look quite unlike those that dominate today.

Could the globally recognised protocols and standards around IoT identity management be built and adopted at scale far more quickly than those necessary for interoperable human Digital ID systems?

Power and influence

Throughout this report we have hinted at the different ways in which Digital ID could either empower individuals (through the transference of control over their data to them) or further empower those interested in ever more accurate identification. Throughout our wider programme we were given little sense from contributors that there was an easy and happy medium on offer.

Where the balance of power offered by Digital ID finally comes to rest will be determined by the design of the models and systems they come to be situated in, and in particular, by the objectives of those who do the designing. If Digital IDs are to become the primary means of storing, or providing access to, personal data, then the legibility of those stores to Digital ID providers becomes the key site for the exercise of power. Personal data stores mediated by Digital IDs would be among the cleanest, most accurate and most wide-ranging of data-sets that related to specific individuals. Where they included, for example, health data, or data around how users accessed restricted services, they would also contain some of the most sensitive types of data. If Digital ID providers, governments or corporations say, retained access rights, then that is where the power will lie; not with individuals who could never compete with the data processing capacities of these centralised providers.

Even in decentralised systems there is still potential for intermediaries or those that provide the infrastructure, to syphon away large amounts of data about individuals' digital behaviours, depending on the protocols involved. And curiously, there are also decentralised models that could inadvertently disempower individuals even as they try to empower them. The permanence of a blockchain implementation, for example, might interfere with an individual's 'right to forget or be forgotten'. As we wrote in our initial perspective it is not hard to imagine someone wanting to have their gender re-assigned, and that being a relatively trivial thing to change within a Digital ID. But what if that person also wanted any previous record of their originally-assigned gender removed, as would be required under current UK data laws?

Further, whilst we currently tend to imagine idealised versions of Digital ID-enabled personal data management and transactions, the future (and reality) may actually be far messier. We may wish to have multiple different Digital IDs for use in different contexts. Different IDs may be provided by different organisations, may require different kinds of maintenance, and may have different kinds of data policies and capabilities. The realities of wanting to use multiple Digital IDs may involve us having to navigate different interfaces, understand different language used to describe similar requests for attributes and information, take different approaches to data permissions and consent, and so on.

In such a scenario it is highly likely that services designed to help us navigate and best exploit the power of Digital-ID-enabled environments would also likely emerge. We have already talked about Digital IDs with built-in, AI-assisted consent managers, but this could expand into other kinds of Digital ID management services such as delegated Digital ID managers and/or legal Digital ID guardians. Platforms which act as brokers between different Digital IDs could also emerge, allowing us to use, and seamlessly deploy, different Digital IDs in different contexts. Although subtle, it is important to understand that the locus of power shifts in each case: from individuals to guardians, to AI-assistants or to brokers. Just as we must be careful today when making decisions around what permissions to give to apps we download to our phones, the permissions we give around access to our Digital IDs could also have a huge impact on our lives.

Shifting perspective again, a number of subtly different cases were made during the programme for a future that involved some kind of formal aggregation and cooperation between different services and service providers. Initially such aggregation might be driven by the need to offer consumers a more truly interoperable environment, but over time could also lead to the consolidation of power over Digital ID eco-systems by federated Digital ID alliances. These might look similar to, but would be an evolution of, current federated authentication systems. The key shift is that federated Digital ID alliances would allow for a single Digital ID to cross the borders of its own eco-system and be used in the eco-systems of those it was in alliance with, much as airline loyalty schemes do today in alliances such as OneWorld or Star Alliance. Such federations could also provide the bridge between commercial and government Digital ID systems, allowing even national IDs to cross borders by operating in commercial markets, rather than only within national borders, via the federation. The motivation for different Digital ID providers to participate in such alliances is that they could provide their customers with access to services that might otherwise require a completely different kind of ID. The technicalities (and politics) behind creating such systems are complex, and there are implications for privacy and security in the short-term. If solved however, the benefits to both consumers and Digital ID providers alike, could be great.

The scale of federated Digital ID alliances would also likely have a profound influence on the Digital ID eco-system writ-large. As with the foundational and heuristic behaviours developed when we first set digital feet on the internet (discussed in the introduction to this report), these agglomerations of Digital ID service provision (into which we would likely be drawn) could also start to determine the norms and behaviours around the use of Digital ID, in ways that would be less likely in a world of myriad differentiated and unique Digital ID propositions.

Digital ID alliances could perhaps begin to replicate the influence of the large-scale national ID schemes in India and China. In Singapore for example, workshop participants were quite clear that whilst building local Digital ID propositions and systems was desirable, it would become ever more difficult to avoid the influence of a Chinese, WeChat-enabled, identity system, due to widespread use of the app by the local population and the potential therefore, for widespread interoperability. Similarly, with over 90% of the Indian population enrolled on to the Aadhaar system, and the Indian government and Aadhaar stakeholders keen to export the technology and learnings, those other governmental organisations (especially in nearby geographies) seeking off-the-shelf Digital ID solutions could well be tempted to adopt the Aadhaar model[65]. We can only hope that lessons are being learned before adoption if this is to be the case. The effect of scale when it comes to Digital ID, as with many other technologies, is difficult to replicate, and gives enormous influence to larger stakeholders.

FUTURE AGENDA

Open Foresight

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