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

Unintended consequences

In collaborating with multiple Digital ID stakeholder during our programme, we developed the impression that this was a community keen to avoid the unintended consequences that have come to characterise so many of the technological innovations now embedded in our everyday lives. In this last chapter we present some of the discussions around that issue that emerged during our programme. However, it is important to caveat the seemingly pessimistic scenarios we go on to discuss, with recognition that there was broad consensus around measures that could be taken today to mitigate risks going forward.

These included:

- **Slowing down.** Slowing down the pace of technology roll-out to ensure that the serious thinking around negative consequences, that has often been missing elsewhere, can be undertaken
- **Decentralisation by design** in order to mitigate the potentially catastrophic impacts of cyber attack, data-breaches and data-misuse or abuse
- **Collaboration** with multiple Digital ID stakeholders to understand different motivations and share thinking and learning.
- **A commitment to transparency** from the outset, allowing feedback and iteration.
- **Clear lines of accountability and responsibility.** Digital ID service providers must be held accountable for the implementation decisions they make, and responsibilities for different parts of the Digital ID eco-system must be clearly delineated. Harsh punishments will discourage irresponsible actors.
- **Human-centred development** to ensure that the complexity of technical challenges do not get in the way of the far more consequential social challenges involved in Digital ID systems.
- **Universal oversight.** The creation and recognition of an international oversight body. “UN-ID”?
- **A body of Digital ID research** from the social sciences, as well as the hard sciences.
- **Participation in transparent monitoring progammes** to track the impacts and outcomes of Digital ID systems as they are rolled out.
- **Development of clear, purpose-led narratives** for Digital ID, in order to drive active user participation and engagement
- **Frameworks of rights, responsibilities and ethics** for providers and users
- **Build on catastrophe.** Learn from early mistakes and implement strong responses
- **Built-in ‘reset’ capacities and strategies.** Ensure that it is possible to re-create, revoke and destroy in order to ‘reset’ Digital ID systems in the event of disaster

System vulnerabilities

Strong and secure systems of Digital ID could play a significant future role in enhancing cyber security for individuals, organisations and states. For some, that is the primary motivating factor behind developing Digital ID in the first place. The ability to accurately identify entities within a digital system, and establish that they are behaving in ways that they are expected, or have permission, to behave, is the very essence of cyber-security, and the very thing that Digital IDs should be able to enhance. For individual consumers and citizens too, an established system of Digital ID could help to bring about a digital world in which we can, and indeed demand to, be sure of who we interact with and who we pass information to. Of course, human fallibility, and the complexity of any digital eco-system, mean that no digital system will ever be 100% secure, enhanced by strong Digital IDs or not.

In the case of Digital ID systems themselves, the impacts of a data-breach or attack (cyber or physical) could be catastrophic. At an individual level, we already know that the risks of reputational harm, identity theft or data misuse, when personal data is stolen, is enormous. If the contents (or access to) a Digital ID were stolen, these risks would be multiplied, primarily due to the accuracy and quantity of personal data a bad actor could control. Worse, if Digital IDs do indeed become critical to the ways in which we access basic services, and an attack or breaching of a Digital ID system made them unusable, then there may be even more immediate and potentially life-threatening problems for affected individuals. How, for example, could a person ever prove that they are who they claim to be in a digital context or when trying to access a service digitally? Further, how could they prove that the person claiming to be them, wasn't in fact them?

At an organisational or state level, breaches or attacks in identity systems could have similar catastrophic impacts. Critical national infrastructures, once protected by a functioning Digital ID system, could be infiltrated by malign actors or rendered unusable until a reliable mechanism for safely allowing entities back into the digital systems was in place . There are precedents for just about every worst-case scenario already. As the cyber-security expert John Carlin said of his book about the realities of state-sponsored cyber-attack[73]: *"One of the reasons I wrote the book is that there are so many instances that people think are science fiction that have already happened…"*

In an analogue to the idea of 'stateless netizens' that we introduced earlier, it was suggested in one of our workshops that this kind of virtual citizenship could theoretically be applied to whole states, perhaps as a way of mitigating the impacts of attack. In the future, states could prepare for a scenario in which they are subjected to physical attack and even destruction, by off-shoring Digital ID and digital public service delivery functions elsewhere, creating, in effect, a virtual, dislocated state. This may sound like science fiction, but Estonia's dramatic shift towards wholesale digitisation already involves such contingencies. The first step has been to explore the possibilities of creating a 'data embassy' (a kind of digital state 'backup') in Luxembourg[74]. Further forward, deep sea and off-world storage may stand in for this friendly nearby nation.

Complete digital security should probably be seen as a permanent aspiration rather than a state that has ever been achieved, and, as we have already said, cyber-security is already in the DNA of most attempts to develop Digital ID systems. That said, the consequences of poor design of digital identity systems are already in evidence. Large-scale digital attribute stores, of exactly the kind that a centralised, interoperable Digital ID system might make use of, have been breached in recent years. Of those, some of the highest profile - such as the leaking of data from the Aadhaar system in India[75], the breach of the Comelec database in the Philippines[76], the hack of the Office of Personnel Management (OPM) in the US[77], the Equifax credit ratings agency data breach[78] and the personal data leaks and breaches at Facebook[79] and Google[80] - involve the very institutions that may be major stakeholders in future Digital ID systems. The long-term consequences of even these breaches that have already taken place may never be fully quantifiable.

There is much more that can be, and has been, said about the relationship between Digital ID systems and cyber-security. However, during our workshop discussions there were three aspects of cyber-security that were highlighted as being unique, or of particular importance, when thinking about the future vulnerabilities of Digital ID.

The first is the obvious need to avoid data 'honeypots'. This is old news to those who work in the field of cyber-security, but the nature of Digital ID, and the data sets associated with it, mean that any Digital ID data-stores are particularly likely to attract the attentions of cyber criminals or digital adversaries. With this in mind, there was near universal agreement during our programme that universal deployment of encryption, disaggregated data sets, decentralised attribute stores and data minimisation were all critical to the resilience (and ultimate success) of Digital ID systems. The most obvious vulnerability, when it comes to the future of Digital ID systems then, is that less competent Digital ID service providers are not aware of the honeypot problem or do not take it seriously enough.

Second is the potential for Digital ID abuse. It would be naïve to imagine that any digital identity system will be immune to abuse. For example, fake ID, long the goal of every would-be alcohol-drinking teenager as well as bad actors seeking access to services they would not normally be allowed to access, is bound to play a part in any system of digital identification. Fake Digital ID could manifest in three ways: 1) Entirely fake Digital IDs that bear no relation to any real entity, 2) Authentic digital identities augmented with fake attributes, and 3) Adoption, theft or use of an authentic Digital ID, by someone other than its owner. As with all digital manifestations of physical world problems, the particular problem with fake digital ID, is scale. Where a fake passport can only really be used in a single context at any given moment, fake Digital IDs have the potential to be used in hundreds of different contexts at the same time, scaling up the consequences in kind.

Third, is the possibility that attributes associated with authentication, including biometrics, could become unusable over time as they are lost, stolen or misused. During workshop discussions there was some measure of disagreement over this issue. For some, this was no more than a part of the ongoing race between security and criminality in the cyber-world. For others, the very idea of biometric redundancy was a misunderstanding of how biometrics actually work within a digital security system. They argued that the mathematical functions which use topological aspects of, say, a face, as inputs, could simply and easily be changed. Counter arguments suggested that the problem was not with creating secure biometric systems of authentication, but with the normalisation of the use of biometrics. Normalisation, it was argued, would likely lead to their use in poorly implemented, and insecure systems. And when such systems were inevitably breached, more secure Digital ID systems would no longer be able to rely on presentations of biometric authentications. As the cyber-security security writer Bruce Schneier put it after the theft of biometrics in the OPM data breach: *"…many systems don't store the biometric data at all, only a mathematical function of the data that can be used for authentication but can't be used to reconstruct the actual biometric. Unfortunately, OPM stored copies of actual fingerprints.*[81]*"*

There is perhaps one other factor to consider in the argument about the use of biometrics, and that is the user-experience around them. Whilst fingerprints have a long history of use in authentication and identification, and digital facial recognition in many ways simply replaces visual examination by others, it remains to be seen whether wider roll-out will see public reaction to the 'creepiness' of automated recognition. Furthermore, having biometric data exposed or stolen, whether or not systems remain secure, and whether or not cyber-security professionals feel that a particular breach is important or not, could give rise to feelings of insecurity associated with having such personal characteristics violated, in much the same way that victims of burglary can feel the effects for many years after the event. Reactions like this could seriously damage faith in Digital ID systems or Digital ID providers.

Identity victims

One of the recurring issues during Future Agenda's "Future Value of Data" programme was the issue of 'data literacy'. The topic was also explored during conversations around Digital ID. Many of the discussions actually covered the same ground, and we won't recreate them here, but one particular conversation in Australia led to a powerful observation: *"Part of Digital ID literacy should include compulsory history lessons for Digital ID builders on the dangers and historical horrors that have resulted from different identification systems/implementations."*

The caution came from the observation that history is littered with examples of human tragedy that have been driven by the formalisation of discriminatory cultural or political beliefs about identity. Perhaps the most relevant lesson for those constructing Digital ID systems comes from what is now known as the 'Rwandan Genocide' in the late 20th century. Arguably, the genocide took place during what might be described as an 'identity war'. The role of formal ID documents in the processes that led directly to thousands being killed is widely recognised[82].

The holocaust too, of course, also provides examples of the use of identity markers and attribute stores to effect mass human horror[83], and there are countless other cases from around the world, even today, in which identity attributes are used as a justification for oppression, discrimination and social control. In the case of China's social credit scoring system, social value is being formally ascribed to all manner of identity attributes, with the long-term consequences for Chinese society largely unknown. Sadly, history tells us that humans will find all manner of ways to use formally ascribed identity attributes to discriminate against each other.

Sadly, history tells us that humans will find all manner of ways to use formally ascribed identity attributes to discriminate against each other.

Of course, Digital ID might actually provide a better situation in this regard than paper documents do. Depending on how systems are built, and who is able to control and view the attributes they contain, users may be able to have more control over the presentation of potentially harmful identity attributes. The danger comes where individuals cannot control which attributes a Digital ID contains, or which are revealed in different digital contexts. The ways in which certain attributes that may seem innocuous to Digital ID builders, are collected, stored, remembered and shared, may have serious consequences for individuals in the future. No single Digital ID provider is ever likely to be able to foresee or understand every potentially negative scenario, but they can (and should) recognise the need to design systems that will allow individuals to protect themselves.

No single Digital ID provider is ever likely to be able to foresee or understand every potentially negative scenario, but they can (and should) recognise the need to design systems that will allow individuals to protect themselves.

With this in mind, a warning that came from one of our early workshops takes on a new significance: beware the ‘costs of convenience’. When it comes to Digital ID, the drive to create ever more convenience and ease of use for, say, mass market payment transactions, may have unintended consequences down the line, or for those deemed to be on the margins, or undesirable, in the future. That could be any of us. In the end, Digital ID may not be like other consumer products. It simply carries much more significance. Once Digital IDs exist at scale, they are likely to become a permanent feature of our digital future, the most powerful expression of our digital, and therefore real, selves. Convenience on its own may not be enough of a principle to base the development of such an important technology.

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