



# 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



## Social identities

In social, cultural and psychological terms, the questions around what our identities are and how we construct and maintain them, are among the most difficult we could ask. We won't even attempt cursory answers here. However, as Digital ID becomes more and more embedded in our lives, it is worth thinking about how some of the socio-cultural aspects of identity could influence our technological IDs in the future.

# It's social not technical

*“Properly speaking, a man [sic] has as many social selves as there are individuals who recognize him...”*  
- The Principles of Psychology (William James, 1890)

We have tried to keep a definitional separation between the social/cultural idea of digital identity expressed through our multiple digital personae, and the more attributes-based proof mechanisms of Digital ID. In the future however, it may become more and more difficult to separate the two. There are a number of reasons for this, though the simplest to grasp might be that, just because Digital ID is concerned with ‘attributes’ and standardised storage formats, that does not mean that the information being stored and exchanged has no psychological or sociological resonance. An attribute that suggests we are ‘female’ for example, might be a ‘fact’, ‘claim’ or ‘sensitive data’ when devising a digital system, but it may also be something that is critical to the way we think about ourselves, or equally, something that others use to construct their perceptions or judgments of us. Conversely, attributes may contain a ‘fact’ that we feel does not represent, or even actively mis-represents, our ‘true’ identity. Gender assignment may be one obvious example in which this could happen, but there will be many others going forward, since assigned attributes (determined by authorities external to us) could often conflict with how we understand, or would wish to project, ourselves.

In the short-term this may not seem to be anything new. As Digital IDs begin to enter common usage, it is likely that they will be initially understood as simple digital versions of offline ID documents, and the relationship they have with our social identities will be seen as similar to those documents. Over time however, this could change significantly. Digital IDs are fundamentally different to the documents they replace.

For one thing, paper IDs are relatively limited. They contain only a small number of attributes. As such, they could never be mistaken for being anything more than a crude representation of who we are. Secondly, the nature of the attributes they contain are necessarily limited and are often devoid of context or nuance. Neither of these things need be true of Digital IDs. Digital IDs could gather together, or be a conduit for, many different types of attributes, from a number of different sources, for use in different contexts. Furthermore, Digital IDs are likely to start to build up, either by association, or directly within, a vast number of more qualitative kinds of contextual data such as behavioural data, preferences, purchase histories, medical histories and so on. Some of these we may have direct control over (a preference for certain brands of clothing, for example), and some we may not because they are about how others see us (which marketing segments we fit in, say). In other words, over time, Digital IDs will start to merge our social identities with our ID. The long-term consequences of this are difficult to gauge.

One potential benefit of Digital ID in this regard is that it could help us to understand how all of these different kinds of ‘data about us’ are gathered, used and pieced together in the digital realm. We might begin to learn which kinds of data different service providers are seeking, and for what purposes, and begin to see direct correlations between the data we share and the outcomes of that sharing. This could, depending on how Digital ID systems are built and evolve, allow us to take a more active role in determining the nature of the digital identities that others are ascribing to us. In the same way that we have a measure of control over how we are perceived in the real world, by selectively sharing different pieces of information about ourselves, enabled by our Digital ID, so we could have a greater measure of control in the digital world<sup>66</sup>.



One thing is surely certain in this regard, as Digital IDs merge social and 'official' attributes, people are likely to bring the behaviours associated with one kind of identity, to the other. There are, and always have been, countless socially complex ways in which people seek to 'manage' their identities on and off line. Digital ID eco-systems will not escape these efforts.

The first, and perhaps most predictable of the ways in which people might seek to do this, will be by creating multiple Digital IDs. People already have multiple digital personae<sup>67</sup>, and have done since the days of the very first 'usenet'<sup>68</sup> forums; presenting different 'social selves' in different contexts, to achieve different aims<sup>69</sup>. Approaches to Digital IDs are likely to be no different. The only question is how this might manifest in the longer term. Users may for example, seek to have different Digital IDs for use in different context 'buckets': 'social', 'business' and 'commercial', in much the same way that they maintain different email addresses for this purpose today. But the future may also be far more complicated than this. Different Digital IDs may be used to create completely different identities (in **every** sense of the word), for use in different contexts, with no apparent connections between them. This would mirror, perhaps, those who today seek to hold more than one passport in order to skip immigration queues, enjoy the benefits of dual citizenship, or hide their travel histories at specific moments of passport presentation. Or, users may seek to create different 'profiles' from within a single Digital ID, each with its own set of consent preferences and unique collection of associated attributes, but keeping the advantages of interoperability offered by a consolidated ID. Or they might do both of these things simultaneously.

Looking further out, and given that Digital IDs may come to house many different kinds of data, it is not at all impossible to imagine that users may start to find ways of presenting contradictory identities, in which, for example, assigned attributes are countered by preferences or behavioural history attributes. The

imagined neatness and cleanness of Digital IDs could give way to the messiness of identity politics in the offline world, and yet still very effectively fulfil their originating function of verifying that 'we are who we say we are' in digital contexts. In all likelihood, and in time, we will see a combination of all of these things, coupled with entirely new digital identity innovations that are as yet unknowable. After all, who we are, never has been simple.

We should also consider the question of which parties will play the role of trusted attribute providers and verifiers in a Digital ID eco-system in the future, especially as the social and the technical merge. Which institutions will provide the necessary level of confidence to third parties that we have the attributes that we claim to have? In the first instance, and with the analogue of passports and ID cards in mind, the most natural answer to this question is that it will be the same kinds of institutions who fulfil that role today: governments, banks, universities, payment providers etc. But as the centrality of Digital IDs to the human digital experience grows, so those locations of trust could expand.

Leaving aside the purely technical questions of 'how it could be done' for a moment, it is possible to imagine that other, less imposing and more local sources of trust could grow in importance. The analogy might be with the meaningful trust ratings delivered by existing digital communities that have emerged around digital commerce such as eBay ratings, Tripadvisor reviews and LinkedIn references. In everyday life, in non-digital contexts, trust is common currency, and only rarely does it involve reference to the kinds of verifiability contained in large-scale, institutionally sanctioned, documents. For example, when welcoming new members to a local football club, or finding a babysitter, or getting recommendations on which cafes to get a good cup of coffee, we rely instead on the collective wisdom of the communities that we live in, or *they* come from.



Furthermore, we surely often feel that it is in the various localised communities we live and spend time in that we find people whose understanding of us comes closest to our own sense of ourselves<sup>70</sup>. In the future might these communities also play a role in providing and verifying attributes to Digital IDs? The kinds of attributes such communities could confer (that someone is a regular churchgoer, that someone is a regular volunteer, that someone makes extremely tasty cakes, etc.) may have more limited spheres of operability than a government-assigned attribute, since they will likely become less meaningful or trustworthy the ‘further away’ from a community that they are applied<sup>71</sup>; but ‘community endorsement’ may well provide the means for people to construct their Digital IDs in a way they feel more accurately reflects their identity. If anything, in an era of declining trust in large and remote institutions, this scenario seems ever more likely. Considered another way, in the future, those Digital ID service providers that enabled, and were able to draw from, the inherent trust pools of local communities may well be seen as a powerful counter-proposition to providers that relied on, say, opaque processes of passive data collection.

This idea of community affirmation also reminds us that the cultural specificity of certain attributes is also important. Again, to fully tackle this topic would require more space than we have here, but it is worth bearing in mind when talking about the ambitions for a globally interoperable Digital ID. Not only will different societies, cultures and communities consider different kinds of attributes to be important, but also the ways in which the similar attributes are understood could differ markedly from one context to another. Something considered a relatively mundane or harmless characteristic in one culture, could have serious social implications in another. For example, in some societies religious affiliation is seen as a critical aspect of identity and is tied to various access rights. In other societies religious affiliation has no relevance in terms of access to government services, but has great social resonance. And in yet other societies religious affiliation is simply not important at all. Decisions made today around how to deal with attributes that have vastly different connotations and implications in different contexts could have far reaching consequences indeed.

Today, the development of Digital ID systems is largely understood as a technical challenge, but in all likelihood, we will soon come to understand it as a social one.

Today, the development of Digital ID systems is largely understood as a technical challenge, but in all likelihood, we will soon come to understand it as a social one.

# Digital life stages

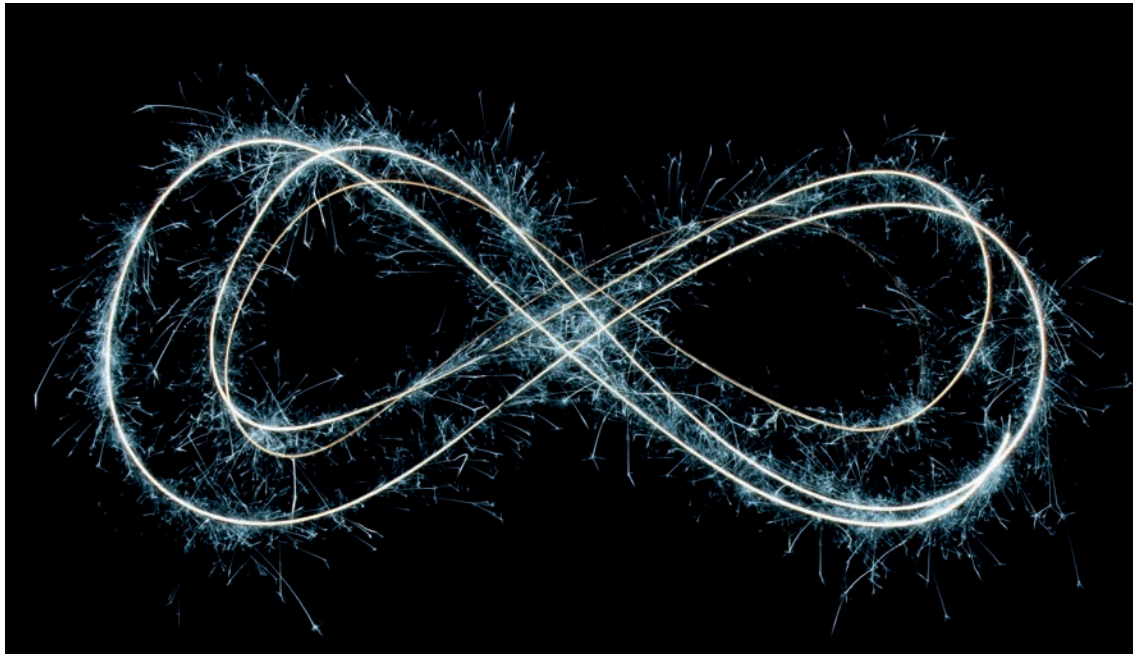
It is possible that the first immortal Digital ID already exists. This idea was suggested by a programme participant during one of our workshops. Although the comment was made with some incredulity, the thinking that led to it was sound. As Digital IDs become more and more comprehensive, becoming ever more reliable and powerful repositories and vehicles for our digital lives and digital selves, then the question of how life-stages are handled becomes more relevant. During our discussions, a number of different 'life-stage' questions were raised. Some in isolation and some in the context of a specific exploration of the subject. If access to Digital ID were to become a fundamental human right, as we have suggested elsewhere, then might they also be issued at birth, for example? How will Digital IDs handle change in our lives? What happens to our Digital IDs after we die?

There might be some pat answers to these kinds of questions today, but they perhaps require a little more thought. How we answer them today may not be how we would answer them in the future, once we have begun to see how Digital ID systems evolve and operate in society. How they are answered for different people, or from within different cultural contexts, may also differ.

It is possible that the first immortal Digital ID already exists.

No doubt we will begin to find answers only as we begin to apply them in real scenarios. Prior anthropological or philosophical research is unlikely to provide practical, or one-size-fits-all, solutions in advance. Nonetheless, in the spirit of 'forewarned is forearmed' here are some of the questions that were raised during our programme in relation to them:

- When does life begin, and therefore when could and should digital life begin?
- What are the ethics of building a Digital ID, that may have long-term impacts on life-courses, on behalf of a child?
- How will Digital ID service providers handle a user's 'right to forget' or 'right to be forgotten'?
- How will Digital ID providers enable us to change who we are? How can we 're-invent' ourselves if our Digital IDs have a persistent memory of 'who we were'?
- If we 'own' our Digital IDs, and they collect a number of valuable assets, either in the form of data or rights, then can we pass them on to our children when we die?
- How will Digital ID providers handle the issue of 'power of attorney' over Digital IDs?
- Can Digital IDs account for differing cultural significance around life-stages?
- Will Digital IDs change the way we think about life-stages, introducing new ones, and rendering others redundant?
- Who will have the right to 'terminate' a Digital ID?



There are no doubt many more such questions to be asked and discovered as Digital ID develops.

To leave on the thought with which we began, it was pointed out to us that Digital IDs created today may well have a very long lifespan. If, for example, an 18-year-old creates a Digital ID today and lives until he/she is 120 years old, then do we need to start considering what that ID might look like in 100 years' time? It could contain the summed history of almost an entire human life. Is it possible that it could have some measure of sentience? At the very least it is surely likely to have intelligence. At that point would both owner, and ID, seek to live on forever? It really does seem possible that the first immortal identity might already have been born.

It could contain the summed history of almost an entire human life. Is it possible that it could have some measure of sentience? At the very least it is surely likely to have intelligence. At that point would both owner, and ID, seek to live on forever? It really does seem possible that the first immortal identity might already have been born.



# Contact details

**To discuss this project further  
please get in touch**

Dr. Robin Pharoah  
Director | Global Insights  
Future Agenda

[robin.pharoah@futureagenda.org](mailto:robin.pharoah@futureagenda.org)  
[www.futureagenda.org](http://www.futureagenda.org)  
[@futureagenda](#)

# FUTURE AGENDA

Open Foresight