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

# System design

For the most part we have tried to avoid diving into the technical aspects of designing and building fully functional and interoperable Digital ID systems. For one thing, there is a lack of consensus around exactly how this might be achieved. For another, the focus of our work is the future of Digital ID, the meta-factors that will drive future directions and foresight of the likely impacts and implications. In this section however, we touch on some of the questions around Digital ID system design being asked today, and how the answers and solutions that are being explored will affect the future.

# The basic building blocks still matter

Expert participants in our programme were given the task of thinking ten years out. But dealing with uncertainties, especially when it comes to technological development, means that such an instruction is more about thinking beyond today's challenges than about specific timescales. With this in mind, it is interesting that there was wide agreement that whilst certain aspects of Digital ID, particularly around its functions and roles in society, could and would change dramatically, other aspects would look very much like today. We outlined many of these issues in our **initial perspective** document under the heading 'implementation matters' and it is worth reproducing those that were identified as 'not going away', alongside the new thoughts that emerged during our conversations.

**Security**

The processes by which digital identities are presented and authenticated digitally will need to have a high level of ongoing security. This is necessary to ensure both that personal data is kept private, but also that authentication does in fact foster trust among all parties in a transaction. It will become less acceptable to find that breaches of security were due to lapses in, for example, keeping systems up to date with the latest security technologies. For some Digital ID stakeholders these ideas are second nature, for others it may require significant culture change and a rebalancing of priorities.

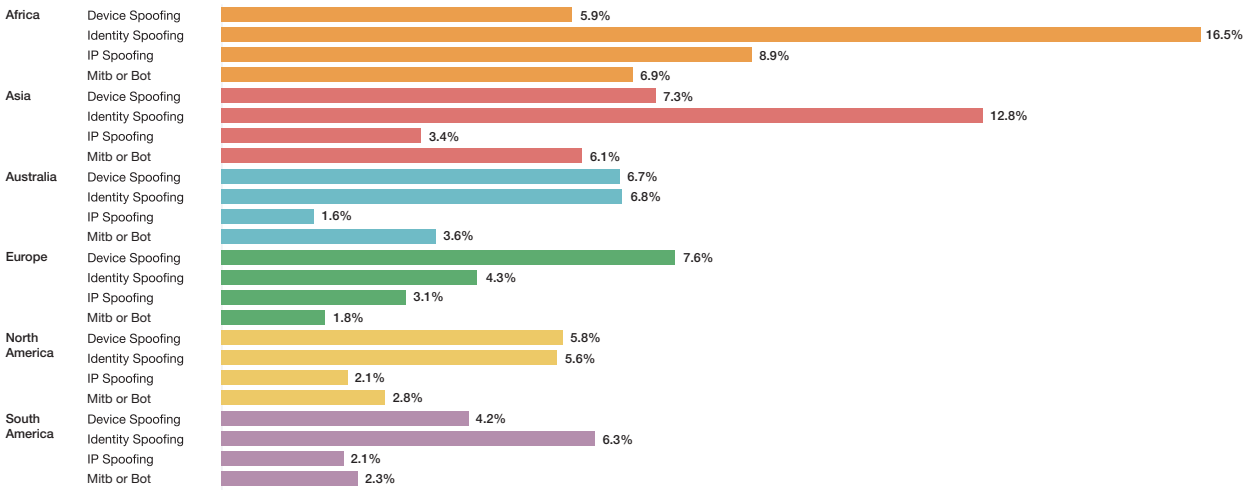
Encryption is a given, but there is more than one way to implement encrypted exchanges of information, and key decisions will need to be made over what is (and is not) kept 'secret', the precise moments within a process that encryption and decryption occur, which parties can and can't encrypt and decrypt, and the physical locations in which encryption and decryption are handled. Different protocols have different implications in terms of convenience and usability, but also in terms of both security and privacy. Wider public understanding around these issues is likely to increase from today, changing user expectations. For example, the current furore around end-to-end encryption could soon give way to more sophisticated public debate around the different implementations of end-to-end encryption protocols, some of which allow service providers to still collect user data, versus others that don't. Digital ID implementations that allow for misuse, irresponsible use or even non-transparent use of personal data could lead to a break down in trust in Digital ID providers. Worse, poorly handled implementations could lead to catastrophic data breaches and, potentially, a loss of faith in the whole principle of Digital ID.

Promises around the security and privacy of Digital ID transactions could be enhanced by new technologies going forward, but again, transparency around what can and can't be done will be key. During our programme for example, opinion on the future use of 'zero-knowledge proofs' (ZKPs) in Digital ID transactions, was sharply divided. The term is used slightly more widely in the field than the mathematical and logic theories behind it suggest it should be. We found various different uses of the term being used in different contexts to mean different things. It also seemed to be confused at times for the 'zero knowledge' principles that some pioneering, privacy-focussed digital service providers claim to employ. These principles are more about the promise that a digital service provider either has no sight of the data that service users create while using their service (thanks to encryption) and/or deletes any meta-data generated by data processing[38]. The over-use of the term ZKP then, may actually be arising from a more generalised desire to see the development of future technologies that necessarily limit the amount of knowledge that is shared between digital transactors, and/or is visible to mediators of digital transactions[39]. The key will be in making the capabilities and functions of any given data minimisation implementation transparent to users.

As a counter to this idealised goal of knowledge minimisation however, it should be remembered that many of the promises of Digital ID are made on the back of data collection, rather than data minimisation. Personalised services, new methods of biometric authentication, cross-border interoperability etc. all involve significant amounts of data capture and storage.

Digital ID will almost certainly have an impact on both data security and data privacy, but in exactly what ways will most likely be determined by early design decisions made in the development of those systems that eventually come to dominate. The decisions that end up mattering most may be being taken as we write these words. Ill-considered, short-termist implementation choices could adversely impact the future efficacy and potential of Digital ID.

Of course, Digital IDs actually have the potential to provide not only more security during digital transactions than their paper-based counterparts but also a boon to cyber-security more generally. In the future, many forms of digital identity are likely to include identity attributes that are much harder to mimic or steal (such as AI-determined behavioural biometrics). They can be used in highly secure authentication protocols, or leveraged in real time to determine suspicious attempts to access any given system. The prevention of identity theft in particular, was seen by programme participants as one of the key driving motivations behind the development of Digital ID systems, particularly from those within the financial sector where the impacts of identity theft are most directly understood.




Percentage of digital financial transactions recognised as crime, by region[40]

Digital ID was not seen by any means to be a panacea to cyber-crime and attack but rather a new frontline[41] in an ongoing battle between malicious hacking technologies and cutting-edge security and authentication technologies. Ultimately, security is likely to be a major focus (possibly to the exclusion of other considerations) in the early development of Digital ID systems, and with good reason. Digital ID systems will likely stand or fall on their long-term security record.

**Multiple partners and stakeholders**

Any digital identity eco-system is going to require a number of different stakeholders and partners. Aside from the users/holders of Digital IDs, we will need: institutions that can initially collect and verify the attributes that are going into the ID; institutions and organisations that can manage the authentication process across a wide range of contexts; and, of course, institutions and organisations that will accept and trust Digital IDs to do the job of ensuring that individuals and entities are who they say they are and have the attributes they claim to have.

Trust - on a number of levels - is the key factor here for all parties. There is the question of who we, as users, trust to collect and verify our identity attributes, who we trust with the task of keeping those attributes safe during different types of transactions, and who we trust in terms of giving access to our identity attributes. For co-operating organisational or institutional parties in the system the same questions will apply.

Whilst the need for multiple stakeholders to co-operate towards a coherent vision of a Digital ID system is widely recognised, and pathways for that co-operation were modelled in some detail, several of our participants pointed out that the role of users is too often over-looked or taken for granted. As with any technology, the ways in which end-users adapt and innovate new technological capabilities to their own ends are difficult to predict. We can be sure that individuals will find ways of using Digital IDs that are not part of original designs, we just can't yet be sure what they will be. Early providers are likely to be taken by surprise.

**Centralised or distributed?**

The question of whether a centralised system or a de-centralised system for the management of digital identities is more preferable, is still technically open to debate. A distributed implementation might remove the need for users to place their trust in a single specific institution, but may also be a barrier to seeding and developing the wide-spread uptake and interoperability critical to the development of a fully functioning digital identity eco-system.

Digital ID will almost certainly have an impact on both data security and data privacy, but in exactly what ways will most likely be determined by early design decisions made in the development of those systems that eventually come to dominate.

For those advocating any measure of self-sovereignty in Digital ID, it would seem that decentralised Digital ID systems are the only option, since centralised systems imply centrally controlled and monitored attribute stores. It should be remembered however, that even in decentralised systems, users may not always have full control over their IDs, or the ways in which their data is handled. How for example could a blockchain implementation truly enable a 'right to be forgotten' or address the frequent real-world need to amend a record and delete a false history? Even if sensitive data were deliberately kept separate from a particular blockchain, it is perfectly conceivable that the history of transactions it contains could become the very point at issue. Distributed network models will also still require users to trust the security and honesty of other players within the network, and the complex technical protocols of the system itself. This trust may not come as easily as some technologists hope.

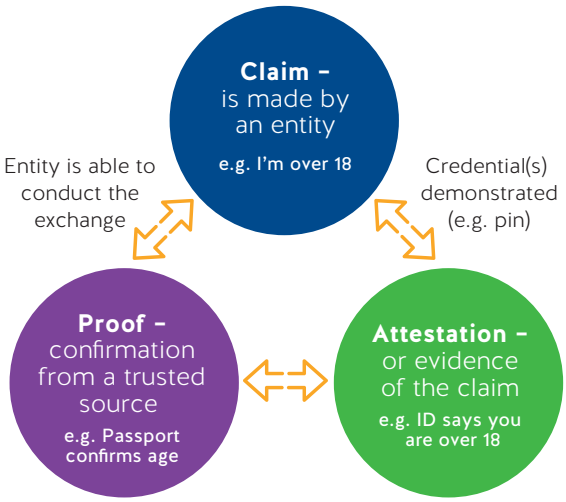
Conversely, more centralised Digital ID systems will aid the development of an interoperable and widely accepted eco-system (Aadhaar and even organisational identity systems provide cases in point). But they will require us to ask the question, assuming we have the choice, of which (few) institutions we trust to hold the keys to our identity? This question is unlikely to yield a single or unchanging answer, particularly when we consider the question in a global context. Furthermore, centralised systems create 'honeypots' of temptation for cyber-criminals, monetisers, and would-be authoritarians. They may also, albeit unwittingly, create the conditions for the emergence of new Digital ID monopolies every bit as powerful as the larger players in the current personal data landscape. There are certainly short-term gains in conceiving centralised ID systems, but these are surely balanced by long-term risks.

During the programme there were very few (if any) participants who advocated the development of centralised Digital ID systems. Most saw the risk/reward profile as being too heavily weighted towards the former. However, we should note that workshops were not held in, for example, India or China, where views might have been significantly different. The power of centralised, state-backed Digital ID systems was perhaps most keenly felt, and feared and respected in equal measure, by participants in our Singapore workshop, where the influence of both Indian and Chinese centralised data technologies loomed larger than in other locations we visited.

**Biometrics**

The development of new biometric identity markers will continue. Initial forays into fingerprint and 'faceprint' recognition technologies could lead to the evolution of a whole eco-system of different kinds of unique biometric markers designed to increase security. One interesting consideration here is the extent to which future Digital ID systems continue to adhere to the presumptive identity markers of traditional, real world, ID presentations. Faces, for example, are important for humans taking part in an offline transaction, but less important perhaps once authentication processes become fully digital. Of course, faces can easily be presented to cameras, but over time, we might become familiar with authenticating ourselves in multiple different ways, and biometrics that are less 'visible' to humans in the real world, such as gait analysis or keyboard typing cadence, could become commonplace in digital contexts. Beyond behavioural biometrics there may even be others that have not yet been explored. AI and machine learning techniques could potentially uncover hundreds, if not thousands, of currently unknown ways in which we are uniquely identifiable.


There was also a minority view among those who participated in our programme that was less comfortable with the widespread deployment and uptake of biometrics in authentication systems. There were perhaps two concerns: 1) Familiarising people with the use of biometrics may lead to them placing trust in their use in all contexts. As one participant noted, a greater abundance of trivial biometric use-cases could lead to more data and security breaches, and the eventual redundancy of the authentication method[42] and 2) That the use of biometrics could lead to a world in which we cannot escape identification, leading to the ultimate death of privacy, and/or the risk of behavioural control. For one Digital ID innovator who attended our Australian workshop: *"… the use of biometrics is just lazy thinking. There are surely still plenty of other secure and reliable ways of authenticating parties in a transaction that would preserve privacy with only a small loss of convenience."*




**Claims, attestations and proofs.**

Howsoever Digital ID functions grow and evolve, their basic role as a way of proving claims in a digital environment is unlikely to change. Given the number of contested terms and controversial concepts that bedevil conversations about Digital ID, the basic *'claim, attestation, proof'* model, it was felt, would be unlikely to change in the coming years, providing a solid bedrock, or common ground, for a wide range of stakeholders.



# Growing standards

*"Oh, there is an ever-growing list of universal standards; the problem is that they are not universal standards."*

This comment came from one of our programme participants who was pointing out that in one sense, even today, there is no shortage of universal Digital ID standards and protocols. Multiple organisations, large and small, are currently involved in an effort to create them. The problem is that they are all different and are not being universally developed or adopted. Nonetheless, whether universal, regional or local, for Digital ID to have any measure of interoperability, such that users can deploy their ID in more than just one or two environments, we must see either the development and adoption of standards, or some kind of technological solution that allows mapping between different standards regimes. Again, there are others more qualified than us to discuss the potential benefits and drawbacks of different attempts to build universal Digital ID standards, so we won't go into great detail here[43].

The relevant point for us is that for all the best intentions of innovators in the Digital ID space, the most likely outcome is that early movers will enter into a kind of 'format war', similar to the music and video storage format wars of the late 20th century or even the battle between AC and DC delivery of electricity. History tells us that the end of these format wars is not necessarily that the 'best' format wins. Rather they end up being a story of what comes first in a gauntlet race involving marketing campaigns, consumer attitudes, politics and government or institutional interventions.

It is also worth remembering that early winners in such a complex and risky technical environment will perhaps find themselves quickly burdened with the risks and responsibilities associated with maintaining a highly-sensitive and mass-adopted system. As was pointed out in several of our workshops, but particularly those in Europe, the regulatory environment around Digital ID is likely to be faster moving than we have previously seen when it comes to new data technologies. Digital ID accountability could emerge as an idea in wider public and policy discourses quite quickly after initial adoption. Increasingly (as we saw not just in our Digital ID programme but also across workshops held as part of our **Future Value of Data** programme), the idea of good data stewardship[44] is moving from being about data-management within organisations to becoming part of high-level discussions among policy makers, digital activist groups and regulators. In relation to Digital ID, future accountability mechanisms could well involve harsher punishments for data misuse and abuse, or poor security and lax approaches to privacy and data-protection, than precedent suggests.

As with all fast-moving technological developments, regulators will be 'building the aeroplane whilst flying it'; trying to tackle emerging issues in real time. This was seen as a 'motherhood and apple pie' statement by most of our workshop participants. The point to grasp perhaps, is that in relation to Digital ID, government involvement is almost a given, and regulators are unlikely to be as unaware of the rapid pace of change and the serious consequences of inaction as they have been in relation to the first wave of digital transformation[45].

# Ethics by design

During the programme many participants observed that, although the idea of Digital ID has been around for a long time, and much thinking and work has already been done, it is still *'early enough for ethics'*. In contrast to the 'build it and see what happens' approach that has characterised much of the development of big social technologies over recent decades, Digital ID stakeholders and developers have the time and space afforded by the complexities of the Digital ID project, to pause, and think about ethics from the ground up.

Being 'early to ethics' won't make ethical questions any easier to answer of course. Designers of Digital ID systems will have to confront sometimes difficult trade-offs between an emerging ethics of privacy, digital security, accessibility and the need to meet urgent societal need; alongside the responsibility of building systems that are both useable and meet the functional requirements and demands of the market. These immediate dilemmas will also be shadowed by a newly urgent set of ethical considerations around the need to address and mitigate the possibility of negative unintended consequences. Societies are still only just beginning to come to terms with the scale and speed at which the unintended consequences of data-driven technologies can spiral out of control. Of course not all consequences can be foreseen. Some of the thorniest issues may emerge only once a system has been built and tested.

Does this imply that Digital ID systems need to be built with an overabundance of caution, at the expense of ambition? Perhaps, though this need not be seen as a negative thing. Instead, Digital ID stakeholders could see themselves as leading the way in creating fundamental blueprints for good data-driven technology development. A blueprint that seeks, from the outset, to minimise the risks and maximise the benefits for the long term good of digital societies and economies.

One potential model for Digital ID ethicists to follow is that set by the world of bio-ethics, a course that has been put forward by some for the development and adoption of AI[46]. Whilst there is still debate and controversy around new bio-technologies and the ethical questions they raise, there is also a framework of robust national and international ethical oversight; an established eco-system of committees, recognised experts, and respected programmes of education and research (some of which already have precedents for the ethical issues around personal

| AI4People - Suggested Ethical Framework for a Good AI Society | |
|---|---|
| **Beneficence** | Promoting Well-Being, Preserving Dignity, and Sustaining the Planet |
| **Non-maleficence** | Privacy, Security and "Capability Caution" |
| **Autonomy** | The Power to Decide (Whether to Decide) |
| **Justice** | Promoting Prosperity and Preserving Solidarity |
| **Explicability** | Enabling the Other Principles Through Intelligibility and Accountability |

The first four components hail from Bio-Ethics, the fifth, Explicability, was added by the AI4P authors as a result of their exploration.

data[47]). The strength of this eco-system has recently been in evidence with the swift and co-ordinated response to perceived irresponsibility in the use of CRISPR (gene-editing) technologies[48].

In contrast, when it comes to data-driven technologies, despite the fact that many have just as profound implications for the future of humanity, self-regulation remains patchy and untrusted. Today's Digital ID stakeholders have the opportunity to actually shape the future in this regard, by recognising the authority of independent experts, helping rather than hampering the development of strong regulatory frameworks, and so on. Designing ethics into Digital ID will not just be about designing-in privacy protocols, or even adopting internal, organisational ethical codes, but also about designing, building and participating in, a trusted and effective eco-system of robust and authoritative ethical oversight. The foundations for just such an eco-system are already emerging, with ethics and responsibility high on the agenda at many international Digital ID conferences, initiatives such as ID2020[49], Omidyar Network's "Good ID" initiative[50], and the ongoing work of organisations such as the Electronic Frontier Foundation (EFF)[51], Open Data Institute[52], the Internet Society[53], and others.

In the future, Digital ID might also have a role to play in making *other* digital spaces and technologies more ethical. We have already highlighted some of the potential benefits that stem from the ability of Digital ID to provide data with provenance. The ability to identify the real people behind digital personae could be similarly beneficial. For example, one extremely powerful and potentially positive benefit of Digital ID comes from its ability to provide a mechanism for digital accountability. If, say, politically motivated ads on social media platforms were required to come with an identifying signature from a Digital ID, then there might be a direct line of accountability to help tackle the burgeoning problem of 'fake news'. Such a use-case would certainly be compelling to some in today's political climate.

Similarly, by requesting identifying attributes from a Digital ID during login or sign-up processes, social platforms could make online abuse and bullying, and even certain types of cyber-crime, much more difficult to perpetrate. In theory, bad actors could not only be better monitored within systems, but could also be more appropriately and effectively targeted for sanction or censure, either by the service providers themselves or even by other service users. Within a growing number of public digital contexts, hiding behind anonymity to create social harm may no longer be tolerated, or even possible. Digital ID could pave the way for the ethical norms and conventions of civility in offline spaces to re-enter the public digital realm.

Further, Digital ID could also enable savvy netizens to leverage this power to make themselves identifiable or not. In being selective and discerning in terms of who they share personal identifiable information with, and under what set of terms and conditions, consumers may be able to take more active control of the value exchange in digital transactions. They might demand, for example, better prices, enhanced offers or higher service levels, in exchange for more identifying attributes and consent to receive hyper-accurate advertising. Arguably this 'levelling of the playing field' would provide a more ethical digital landscape in which power is more evenly distributed between citizens, consumers and service-providers.

In each of these examples we see potential benefits to stronger identification in digital spaces. Some argue that, to some extent, we already live in this world, and that this willingness to be identified is one side of the existing 'grand bargain' that we make when using so-called 'free' services provided by the tech giants[54]. But that is not quite true. First, many are in fact unaware that they are currently identifiable in digital spaces at all (let alone the means by which this is done) meaning that this so-called 'bargain' is inherently one-sided, and cannot be leveraged by all parties equally. Second, although consumers and internet users can indeed be followed, monitored

and targeted with some measure of accuracy today, there is still a lot of 'noise' in the system. People share devices and accounts, change settings, clear cookies, create multiple digital personas, and of course, deliberately mask themselves, meaning that attribution and therefore real digital accountability is often extremely difficult. Digital ID has the potential to help make the 'bargain' transparent to users, and also to help service providers create much 'cleaner' data sets, in which the degree of confidence that a particular data point can be associated with a particular individual, is much higher.

For some, this is precisely the future path that Digital ID will (and should) take us on; to a world in which we are always identifiable and, as such, our needs are better understood and accountability is transparent. The benefits - hyper-personalised service delivery, easy movement through and across digital spaces, smart and efficient public services, enhanced security and accountability – would more than compensate for a lack of privacy, they say. Others point to a different end-point to this scenario; a future in which political dissent becomes all but impossible, discriminative targeting becomes trivial and commonplace, and in which we become so 'readable' that we can be easily manipulated and controlled by various interests, perhaps even without our knowledge. Hyper-personalised services have as their inevitable corollary, hyper-surveillance.

With careful thought, intelligent development, and a commitment to ethical design, it should be possible to enjoy at least some of the benefits associated with greater transparency whilst avoiding the most dangerous pitfalls, However, as was almost universally agreed across our programme, it will require more careful thought and more responsible development and implementation than has characterised much social and data-driven tech development thus far.

As a final thought on this topic, those developing Digital ID systems, products and services will need to be mindful of the implications of making certain promises themselves, and ensure that the realities of their technologies are transparent to users. For example, it has often been suggested that Digital ID will offer uses greater control over the data they share, and/or that the design of attribute-formats could reduce the need to share sensitive personal information with those requesting our credentials, thereby enhancing privacy. Promises are already being made in this regard in the language of Digital ID white papers and marketing materials. In reality of course, Digital ID providers also have options for data collection *themselves.* Whilst the contents of digital attribute exchanges in any Digital ID implementation are likely to be 'secret', for example, the facts of the transactions themselves i.e. who we are transacting with, when, where, and with which attributes, may not. Some Digital ID providers may opt to create systems that do not (or cannot) collect and store this meta-data. Others may seek to derive value from anonymous aggregations, and yet others may see the value of storing it all as being too great to ignore. The same is true of the personal data storage that will accompany Digital ID systems. Will Digital ID providers operate on a 'zero knowledge' principle, or retain the ability to access attributes? And would the answer that a provider gives in one context necessarily hold in all? Could Digital ID providers operating in China for example, make *any* clear privacy-preservation promises, and what implications might there be for interoperability if they cannot?

Whether Digital ID enhances or diminishes user privacy with regard to the organisations and digital spaces it connects us with, should be explained to users as being an entirely separate matter from the privacy implications of using Digital ID systems themselves, lest we recreate the very Faustian bargain that Digital ID is often purporting to disrupt.

During our workshop discussions, the privacy debate raged. Some argued that consumers and citizens had long since given up on privacy, and that the future of Digital ID was much more about convenience, security, trust, and accountability than about meeting a consumer or citizen demand for greater data privacy. Others argued that Digital ID was precisely the much-needed vehicle for changing the current digital paradigm and re-asserting privacy in a data-driven world. An argument was even made that the very introduction of Digital ID would be the catalyst to raising public consciousness, finally, of the amount of information they are being asked to share in digital contexts.

Views on the matter seemed to vary regionally. Though not universal by any means, we saw less concern with privacy in the US and Singapore than we did in Australian and European workshops. This is perhaps reflective of the different public discourses around technology in each of these environments: the influence of China and Chinese technologies in Singapore as well as the particular nature of the Singaporean social contract; the drive for innovation and data entrepreneurialism on the west coast of the US; the top-down regulatory and bureaucratic approach to social issues in Europe.

Or perhaps this is far too simplistic. Either way, there was one point of universal agreement around which the notion of privacy erosion was deemed to have gone too far, and the role of digital identity and Digital ID in it, was all too apparent: social scoring.

Twice during our programme, in completely different contexts, an idea was raised around one particular, seemingly benign, even ethically desirable, potential for Digital ID. The idea was that Digital IDs could help us to track our own personal carbon footprints. By connecting our Digital ID with various sensors, we could all monitor and control our impact on the environment and be encouraged to behave in more environmentally sustainable ways. In both instances initial enthusiasm for the idea was quickly replaced with a sense of dread that once such 'environmental impact scores' were collected, they would inevitably become a means (or even a mechanism) for social reward and punishment. In fact, the idea of 'scores' of any kind being associated with Digital IDs was quickly established as a slippery slope toward a model that nearly all agreed really was dystopian: China's social credit system[55].

The social credit system in China is, as yet, not transparent, and we don't know at the time of writing precisely what the Chinese government's plans for the system are or will be, or how it will be administered, or whether there will be processes of accountability and redress, or how the Chinese population will react to it in the long term. However, much has been written about it in commentary, with many seeing it as the very worst outcome of the surveillance possibilities of a data driven society: the first step towards immutable, totalitarian social control. In the last two chapters of this report we will deal more directly with the possible unintended consequences of Digital ID systems, and social scoring should be considered alongside them. Even with the most ethical of intentions, the nuts and bolts of a social scoring system could be unwittingly built into any Digital ID implementation due to the simple fact that identity attributes are never just a neutral set of facts. Identity is, and always has been a social and, critically, political phenomenon.

# 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