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

# Defining digital identity: scoping the challenge

In 2012, Boston Consulting Group (BCG) produced a report titled “The Value of Our Digital Identity”[4]. The report suggested that the value of “digital identity applications” could reach $1 trillion, by 2020, in Europe alone. It was an iconic figure, but there is devil in the detail. The report defined ‘digital identity’ as: ‘the sum of all digitally available data about an individual, irrespective of its degree of validity, its form or its accessibility’[5]. In a sense, the economic evaluations the report goes on to make then, are really about the value of economic activities that leverage any personal data, of any kind, and in any way.

Whilst it is true that in some ways our digital selves are comprised of all the data we have ever created or has been created about us, this is not a definition that many who work in the field of digital identity would recognise. There is a key ingredient missing: the link or relationship between personal data and a real person[6]. Although difficult to define, it is the nature of that relationship that provides the essence of digital identity. Without it, what the BCG report describes as digital identity, is really just ‘data’.

The BCG definition also suggests that personal data is part of our digital identity *“irrespective of its […] validity”*. This is interesting. A lot of data we share about ourselves in, for example, a social media account, may not be correct. It could be out of date, mistaken, or even deliberately falsified, and yet still be associated with us and therefore still in some ways useable or made use of (as the BCG report suggests). Again however, for many who work in the field of digital identity, the truthfulness or verifiability of data is actually at the heart of the matter.

The key question for those who work in digital identity is often: *‘how can we prove that we are who we say we are?’*, during digital transactions, and most of the burgeoning number of technologies, products and services that come under the banner are solutions to this question. They are not necessarily concerned with the nebulous mass of personal data that we haphazardly spray across the digital landscape, but rather the data that is relevant at those specific moments when we seek to gain access to services specifically based on who we are, and/or what we claim about ourselves.

Verifying that we are who we claim to be might involve reference to a large body of data about us (as is the case when a payments provider analyses our online behaviours or payments histories to ensure that our authentication behaviours are not ‘unusual’), or it might not (where the only requirement for access to a digital service is that we know a username and password combination verifying that we are the same person logging in as the last person to use that same combination[7]).

This latter case, where little more is required by a digital service than a verification that we are a returning account holder, offers perhaps the other extreme in a spectrum of definitions of digital identity. At one end the ‘set of all data that pertains to me’ (*the ‘set of me*’) as outlined in the BCG report, at the other, a simple username and password combination that may say nothing about me at all, other than that I know the username and password.

Between these two extremes lies a Pandora’s box of subtly different definitions and identity applications, many of which present surprisingly challenging technical and conceptual puzzles.

The key question for those who work in digital identity is often: ‘how can we prove that we are who we say we are?’

# Digital selves and Digital ID

During our programme of expert interviews and workshops, we came across several different working definitions of 'digital identity', or rather, several different digital concepts that were being referred to as 'digital identity'. Below we have wrapped these different uses of the term in to five different definitions. We are fully aware that not all participants in the programme will recognise the equal validity (or even use) of all of these definitions. Nonetheless, in order to fully discuss all of the ideas and contributions collected, it is necessary to lay them all out.

To be clear, ***all*** of the following definitions come under the umbrella term 'digital identity', ***and*** each was, on its own, referred to as 'digital identity'. The words in bold are our own, and denote the terms we use in this report to refer to the various different perspectives. We confine the use of the term **'digital identity'** to those occasions in which we are referring to the topic more generally or when more than one of the following is being evoked.

1) The **'set of me'**: The notional digital identity defined by the putative set of *all* data pertaining to a person. This is a nebulous definition of digital identity that sees any and all data that we create (or is created about us) as contributing, in some way, to our digital self.

2) **'Digital personae'**: Digital social identities deliberately created by a user (or collection of users) for use in one or other digital space. Examples of different digital personae might include characters created by players in video games, profiles on digital dating services, the collection of attributes inside accounts on social media profiles etc. A single individual may create multiple digital personae within just one digital context, or across multiple contexts, and these identities may be similar to each other, or differ wildly. They *may* bear some relation to the individual's offline (real world) identity, or none at all. It is about how an individual chooses (or individuals choose) to represent themselves in digital spaces.

3) A **'Digital ID'**: A digitally stored set of *verified* personal data 'attributes' (such as name, age, gender, citizenship etc.) that can be used to identify that people (or machines), within a digital system, exchange or transaction, are who or what they say they are, and/or have the attributes they say they have. The digital equivalent of a passport or ID card.

4) **'Digital entities'**: This use of the term 'digital identity' is perhaps the longest standing. It refers to the ways in which *'entities'* are tracked, stored, authenticated, monitored and given permissions within a digital system. Entities might be human users, with username and password credentials and even personal data attributes, or they might be devices, such as mobile phones, printers or indeed any other object joining the burgeoning Internet of Things (IOT). Often, entities are given unique 'numbers' when they first join a system that allows administrators (or processes) to distinguish between them. In this way each unique entity within a system has a 'digital identity' (of sorts), which may *or may not* have a relevance beyond the confines of that system.

5) **Authentication tools:** The tools used to verify account holders, owners of data or attribute sets, or digital entities (such as username and password combinations, single sign-ons, biometric authenticators, unique digital signatures etc.) are an important aspect of digital identity and are sometimes (perhaps unhelpfully) conflated with it.

In practical terms, the different uses/definitions of the term 'digital identity' are not mutually exclusive. They overlap, most notably perhaps, in terms of the kinds of data they contain or describe. This can make the language of digital identity confusing. We have done our best to hold to the terminology described above and apologise in advance for any inconsistencies that we may have missed.

**A digital persona** is more of a social or cultural idea of digital identity. It differs from the all-encompassing **'set of me'** definition, in that it is about how we choose to present ourselves digitally with specific data or attributes. It is about *our* 'presentations of self in digital life'[8], rather than the ways in which all or some of our personal data might be used, by others, to identify and define us in ways we may or may not wish. Crucially, nothing about a digital persona need reflect anything about the 'real world' person who created it.

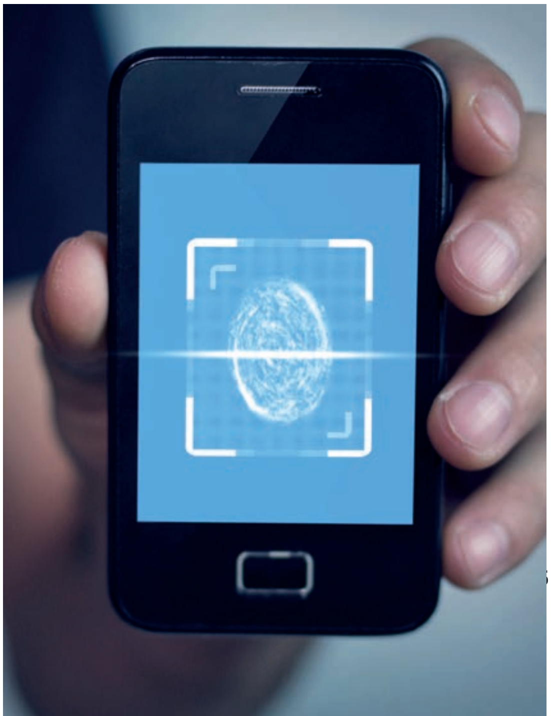
**Digital ID** is a more technical definition that has arisen from the digitisation of various financial, social and institutional interactions that require formal, accurate identification. A Digital ID ties a digital user to a real, physical person (when paying for goods and services, applying to use public services, accessing organisational IT systems etc.). It is the digital equivalent of an official ID card or document that can be 'shown' during digital transactions, in much the same way as we might produce a passport at an international border.

Just like identity documents, the primary purpose of this Digital ID would be to show that we have certain entitlements (such as the right to travel freely) and to provide the tools for verifying that we are the person to whom such entitlements belong. The immediate points of departure are simply that, 1) whereas physical identity documents tend to contain certain specific bits of information, a Digital ID can hold a potentially limitless number of data points and entitlements and 'attributes', from the right to travel internationally, to membership of a local library, and, 2) that the digital equivalent of the act of producing (or 'showing') your ID, as we shall see, can work in a slightly different way to pulling a document out of your bag. Assuming that a 'Digital ID system' existed however, there would then be no reason why a Digital ID could not be used anywhere that had access to that system, including during face-to-face interactions, such as gaining entry to a nightclub, buying alcohol, or hiring a car.

The critical difference between a Digital ID and the other kinds of digital identity outlined above, is the accuracy or verifiability of the attributes it contains. A Digital ID needs to contain at least some attributes that have been given, verified, or are verifiable, usually by an external government body or other organisation with sufficient authority to attest to their truth.

During our programme we chose to focus very specifically on the type of digital identity that we have called **'Digital ID'**, and our interviews and discussions centered on the lively debates and culture of innovation that currently surrounds this particular set of exciting technologies.

The critical difference between a Digital ID and the other kinds of digital identity outlined above, is the accuracy or verifiability of the attributes it contains.



# Authentication, Digital ID, and identity

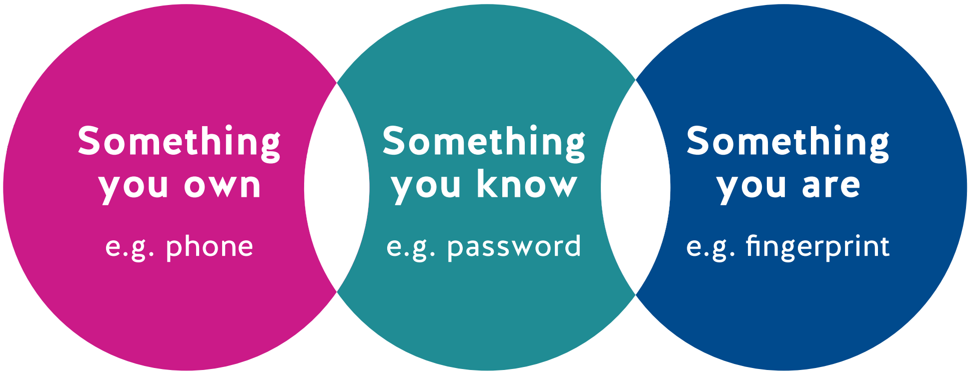
It is easy to conflate digital identity (and especially a Digital ID) with the tools associated with digital authentication processes, not least because these processes often involve the use of attributes that are also contained within an identity. A fingerprint, for example, can be both an attribute within an identity, and simultaneously a means of authenticating who it belongs to. The distinction is important however, because strong authentication is often taken to mean that there is something strong about the *identity.* This is a mistake.

Take, as an example, a social media profile in which a collected set of attributes constitute a digital identity. The account which stores this profile may have a strong set of authentication protocols associated with it, such that the owner must use a variety of authentication methods (a fingerprint, a one-time-code, a password etc.) to gain access to it. Yet nothing about this strong set of authentication protocols means that the profile contains verified or 'true' information. In other words, strong authentication strongly verifies ownership of the account, but says nothing about the data it contains. Strong authentication is not sufficient, on its own, to make a particular digital identity useful as a Digital ID.

But strong authentication processes are critical to a Digital ID system, since rates of success and failure when validating the owner of an ID, will be a key factor in determining the reliability and security of that system, in the same way that the ability for border police to identify that a person presenting a passport is in fact the owner of that passport is critical to the success of border control[9].

The methods and tools that we use to authenticate ourselves digitally can today be categorised according to a simple taxonomy: something you own (like a phone, or credit card), something you know (like a password), something you *are* (a biometric attribute, such as your fingerprint). New technologies and techniques in authentication are likely to bring innovations in all of these areas, increasing security and reliability across different digital systems. For us, it is also interesting to note that some of these new technologies may even begin to feed back into identities themselves. For example, if we could be identified and authenticated by the way that we walk, or talk, or type, would it not be inevitable that we would start to think of our own uniqueness in ways that included these things? Advancements in authentication could lead us to entirely new ways of thinking about who we are, and how we choose to represent ourselves online and off.

## Authentication Taxonomy



Despite the arcane language, authentication protocols are something most of us are already familiar with, since they constitute the barriers and gateways we must go through in order to access everyday digital services. This means that even a technology lay person is already familiar with cutting-edge technologies such as the use of biometrics (facial recognition, fingerprint scanners etc.) to authenticate who they are. Perhaps less familiar would be those processes of identification that do not require us to actively authenticate ourselves. Examples of this might include the ways our online and browsing behaviours are used to help identify, with differing levels of confidence, that we are the person we say we are when we arrive at a login page of a website. In theory, our ever-bloating data footprints, and our indelible link to specific devices, say, could mean that, in the future, we can be identified within a digital process without the need to go through *any* complicated authentication processes. Systems will be able to recognise us as we walk up their digital driveways, so to speak.

## **CASE STUDY:** Single Sign On and Facebook Connect

facebook®

*The Single Sign On (SSO) approach is an early form of interoperable Digital ID. SSO is the ability to login to websites/accounts, using login information from another account or a ‘federated’ identity provider. As with the rest of the emergent digital identity ecosystem, there are a number of providers in this space, including Google accounts, Microsoft Account (formerly Passport) and Facebook Connect.*

In the case of Facebook Connect, users are asked a basic query when visiting another website such as: ‘Login using Facebook?’. If the user agrees then they can login to their facebook account and thereby gain access to the new site, which in turn relies on and uses the facebook ‘identity’. This process then also triggers a riotously complex set of data sharing agreements between the user, Facebook and the third party service. Competing federated identity services such as OpenID also provide a single sign-on service, but do not necessarily link anything other than login credentials between accounts.

For websites that apply Facebook Connect, they are able to provide a quick, easy and convenient way for users to sign up as well as ‘open a channel’ for the user to easily promote the site’s content back on Facebook. For Facebook, creating and delivering this service allows access to a richer data set of user behaviours. For the user there is greater convenience and a degree of extra security provided by no longer having to recall numerous login details and passwords.

# The future of Digital ID systems

Products, technologies and services specifically centred on Digital ID (although not new) are currently in a period of rapid development. At the same time, the increasing digitisation of government services, and growing political and private concerns about data-security, data-ownership and data-control are coming together to drive a market for more robust digital systems and services, many of which may come to hinge on Digital ID.

One clear, and immediate example of this, is the hope that future Digital ID technologies and interoperabilities will provide a robust and convenient solution to financial institutions around the requirements of "Know Your Customer" (KYC) guidelines[10]. In their "World Payments Report 2018" for example, Capgemini and BNP Paribas spend much of their discussion of "New Horizons and Payments in Transaction Banking" talking about the development of new Digital ID technologies and protocols[11]. That report seemed to borrow significantly from the World Economics Forum's landmark digital identity report, "A Blueprint for Digital Identity"[12], produced in 2016 and driven by similar motivations. The number of digital financial transactions is expected to reach 800bn/year by the end of 2020, with the security, accuracy and accountability of those transactions playing a key role in domestic and international stability. The importance of emergent Digital ID systems that could reduce bureaucratic burdens around KYC requirements, especially during digital transactions themselves, whilst simultaneously making them faster, more secure and more convenient for individuals and organisations alike, should be clear.

The number of digital financial transactions is expected to reach 800bn/year by the end of 2020.

Those involved in digital financial systems aren't the only ones pinning hopes on the future of Digital ID however. The UN sees a different set of possibilities in relation to its Sustainable Development Goals (SDGs)[13], and in particular the immediate potential for Digital ID systems to address the needs of 1.5 billion people around the world lacking a legal identity[14].

At a more mundane level, our interconnected digital world has also started to make a mockery of traditional forms of identification. Being asked to produce '*two forms of ID*; at least one from each of the *two following lists*' already seems hopelessly anachronistic in a world of automated password-managers, paperless statements, RFID-driven payments systems, and biometric authenticators on our mobile phones. The idea of having a single Digital ID that can replace the need for the shoe-box full of identity documents and wallets full of cards, is not only one whose time has come, it is one that is all but presumed to exist already. Although it doesn't quite, yet. At least not in the sense we imagine it.

The idea of having a single Digital ID that can replace the need for the shoe-box full of identity documents and wallets full of cards, is not only one whose time has come, it is one that is all but presumed to exist already.

# Communicating digital identity

There are an ever-growing number of digital identity evangelists who believe, with some justification, that the advent of interoperable identity systems could fundamentally change current digital paradigms. The problem is that there are many different evangelists, sometimes thinking of different definitions or aspects of digital identity, making sometimes mutually exclusive claims. Even within the slightly narrower focus of Digital ID (which we have defined as referring to those tools and systems by which people can provide proofs of claims they make about themselves in digital environments), different stakeholders offer different promises based on different ideologies, technologies and models of implementation.

That said, it is not hard to make a broad public case for the development of interoperable Digital ID systems allowing us to identify ourselves in multiple (or 'any') digital context. Some version of the following list of benefits is usually pointed to:

**Convenience:** Job applications, airline bookings, opening a bank account, applications for parking permits or state benefits, and even mobile phone contracts can all still involve cumbersome exercises in repetitive form filling, document scanning, face-to-face presentations and so on. Strong and reliable Digital ID could make many of these processes as easy as making a purchase from an online retailer.

**Enhanced security:** The development of strong and secure systems of digital identification would greatly enhance cyber security for individuals, organisations and states. Cases of identity theft, cyber-fraud and cyber-attack are a growing problem (measured either in terms of number or severity[15]) and are often driven by the large-scale theft and distribution of databases full of identity attributes[16]. High profiles incidents, such as the hacking of Democratic Party emails in the USA in 2016, or the attack on Ukraine's energy infrastructure at the end of the same year, are often popularly portrayed as highly technological. In fact, most start with the very same kinds of identity and/or credential theft that drive the fraud of ordinary people.

**The expansion of digital service provision:** As governments in particular, move increasingly toward online service delivery and access, so too do the number of 'official' digital identification and authentication procedures associated with them. National Digital ID systems such as Aadhaar in India, vary in form and scope, but in many cases they are paving the way for a broader Digital ID eco-system that would allow for national IDs to be used in multiple contexts and even across borders. Perhaps more importantly, national Digital IDs are helping to embed a set of citizen/consumer behaviours around the use of stronger Digital ID.

**Broadening choice and access:** Where once accessing services requiring identity verification might have been localised, people now have the opportunity to access services across national borders, geographical expanses and through an array of digital channels. Strong Digital IDs have the potential to make such transactions simpler and more secure, especially where they are recognised across different jurisdictions (digital or otherwise).

**Transaction cost reduction:** Simply put, the costs involved in trying to deliver services that require formal identification, in a world without Digital ID, are extremely burdensome and an active barrier to innovation. Consider the UK's drive for 'open banking' for example. The initiative has the potential to transform the relationship between individuals, their money, and financial service providers. The need for secure identity and authentication procedures however, still often requires cumbersome paper-based documentation and identification protocols and/or face-to-face visits[17].

**Combining and separating identity attributes:** Traditional forms of ID (passports, driving licenses etc.), often contain very specific pieces of information (names, dates of birth, addresses etc.). Digital IDs need not be so restricted. A single Digital ID could contain all of the attributes that are currently distributed across different paper documents, ID cards and so on. Furthermore, these attributes can then be disaggregated from each other such that only one attribute need be shared where only one attribute is required, rather than inadvertently sharing all of the attributes that happen to come bundled with them in existing forms of ID.

**Global interoperability:** The easiest way of thinking about Digital ID interoperability perhaps, is to consider how an individual, with a Digital ID, would experience an interoperable Digital ID system. In such a system, someone with a Digital ID would be able to present their ID (or specific attributes from within a Digital ID) in the way they want to, in any context in which they needed to prove their identity or a specific attribute from within their identity[18].

**Personalised services:** Services are becoming increasingly personalised and tailored to individual citizens, service-users and consumers based on the increasingly sophisticated collection and analysis of personal data. Digital ID could play a significant role in this developing feature of a digital world. Digital ID could greatly enhance the accuracy with which service providers can determine who they are providing services to, for example, but Digital IDs could also provide means for individuals to securely store, and have control over, vast amounts of personal data of many different kinds, and selectively share it with (or temporarily grant access to) service providers, in *exchange* for personalised services.

**Greater privacy:** A case is often made that digital ID can enhance privacy in a data-driven world, by giving citizens and consumers the ability to have more fine-grained control over the types of data and information they share, in different contexts and with different institutions and service providers. This is certainly possible, though the claim does need some unpacking. The promise of greater privacy depends entirely on the ways in which digital identity systems are implemented and controlled.

**Digital inclusion:** The UN estimates that more than a billion people around the world lack identification documents, either due to forced migration, restrictive legal environments or simply due to a lack of proper access to bureaucratic structures, or a fixed address[19]. Lack of identification documents can lead to exclusions from, or restricted access to, all manner of critical services, from banking and housing, to work and even a mobile phone. Digital ID systems could go some way towards addressing this since Digital IDs can theoretically be issued to, and used by, anyone with even intermittent access to a mobile phone or the internet.

Pointing to these benefits however somewhat masks the technical challenges that lie behind creating the truly interoperable Digital ID system that would deliver them. Digital ID products and services today are neither as intuitive nor as interoperable as this list of promises suggests. Consumers or businesses wanting to dip their toe in the Digital ID waters today are confronted with a bewildering array of options, each with different risks, rewards, principles, promises and user-experiences[20]. Furthermore, since the infrastructure for interoperable Digital IDs is still under construction and still being fought over, Digital ID users today are likely to find that the number of uses they can make of their particular Digital ID is limited, reducing the compulsion to invest in and adopt the technology. For many Digital ID stakeholders, at least in the commercial sector, the ‘killer app’ or use-case that will drive mass adoption and usage is still missing, either due to the lack of perceived need on the part of consumers, or due to the technical hurdles that still need to be jumped to bring the most compelling use-cases to life.

Putting aside the technical difficulties however, perhaps the biggest challenge facing the community of Digital ID stakeholders is the question of how to communicate the idea in the first place. As one of our workshop participants put it: *“I’ve concluded after some time in this arena that ‘identity’ has rather failed as a concept, or rallying call, or technical objective. Identity is perhaps too vague to translate properly from the analogue to the digital, at least not at this time, when we’re still in the early days of the digital transformation. So I say, calmly and seriously, we should forget about ‘identity’…”.*

## **CASE STUDY:** Digital inclusion and Omidyar Network

OMIDYAR NETWORK

*Omidyar Network is a philanthropic investment firm aimed at catalysing economic and social change through market-based activities. It sees Digital Identity as one of six core building blocks for enabling prosperous, open and stable societies. From its point of view, Digital Identity, if built responsibly, is a way to help people participate more fully in the economy and in digital society, not least because of the volume of activities, including provision of government services, that take place online.*

Omidyar see an appropriate Digital Identity as one that is "private, secure, and controlled by the individual – enabling individuals to access resources they are entitled to, such as government services, financial services, education, e-commerce, and communications". An increase in participation is hoped to be a catalyst for innovation in other areas such as property rights, financial inclusion, civic engagement, and education.

In 2016, Omidyar created the Good ID movement (now in partnership with The World Bank, GSMA and others) which promotes inclusive dialogue, and aims to ensure all forms of identification are good for people, as well as for business and governments.

This comment would no doubt shock many, both in our workshops and across the Digital ID industry, but it does point to a paradox at the heart of communicating Digital ID in 2019: Whilst the idea of a Digital ID - a digital replacement for a passport or ID card that could live on our phones and be used wherever and whenever we need to prove who we were - is very easy to grasp in theory; the technical and social complexities behind it make it very difficult to realise in practise. And communicating those complexities is hard. To a lay person, the very idea that having a digital version of their passport on their phone is somehow more complicated than having to rifle through their luggage and produce their passport at a border, seems to be a contradiction in terms. And yet, at least for now, that is the case.

There are countless other ways in which Digital ID is difficult to communicate, and the fact that various Digital ID providers are producing implementations that have vastly different capabilities and propositions, with sometimes even contradictory implications for privacy, security, interoperability, individual sovereignty, data-ownership and so on, doesn't help. The problem also infects the writing of this report. As we have demonstrated, even the simple task of defining 'digital identity' is difficult, let alone dealing with the dilemmas involved in keeping things simple and broad enough for all stakeholders and participants to see where their own expertise plays a vital part, whilst simultaneously recognising the deeper complexities involved[21].

We see this urgent set of conversations around the best way of 'communicating digital identity' as an overarching theme of this report. It was a theme that was repeated throughout our series of workshop discussions, and was frequently identified by participants as being an immediate problem whose solutions will have longer-term consequences for the field.

# Attributes, not ID

During all of our workshops there was some measure of open frustration with regard to pinning down the term digital identity, and with trying to fix the boundaries around Digital ID. This does not mean that shared language was completely absent however. The idea of 'identity attributes', for example, was far less contentious. Attributes lie at the heart of any thinking about Digital ID systems. In simple terms, they are the single data points that make up any kind of digital identity. In traditional forms of ID attributes are easy to spot (name, address, date of birth etc.), but attributes could also include height, weight, preferences around email notifications, the number of visits to a particular website, club memberships, sexual orientation[22], anything. One useful, and commonly accepted way of thinking about this is through the following framework of *inherent, accumulated* and *assigned* identity attributes (as outlined in the World Economics Forum's paper "A Blueprint for Digital Identity" 2016 and reproduced in the table here).

During our workshops it was suggested by some that the future of Digital ID might be better thought of as the future of 'attribute exchange', and that in time we may dispense with the notion of Digital ID altogether. Notwithstanding the amount of time and effort already spent socialising the idea of 'digital identity' and 'Digital ID', it was suggested, the idea of exchanging attributes is not only easier to understand, but more accurately reflects both what is going on in most Digital ID systems, and the ways in which users are likely to use future iterations of Digital IDs. This argument is best illustrated, albeit simplistically, by looking at the difference between the use of traditional identity documents and a Digital ID.

## Identity is a collection of pieces of information that describe an individual or entity

| | For individuals | For legal entities | For assets |
|---|---|---|---|
| **Inherent attributes**<br>Attributes that are intrinsic to an entity and are not defined by relationships to external entities. | • Age<br>• Height<br>• Date of birth<br>• Fingerprints | • Industry<br>• Business status | • Nature of the asset<br>• Asset issuer |
| **Accumulated attributes**<br>Attributes that are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's lifespan. | • Health records<br>• Preferences and behaviours (e.g. telephone metadata) | • Business record<br>• Legal record | • Ownership history<br>• Transaction history |
| **Assigned attributes**<br>Attributes that are attached to the entity, but are not related to its intrinsic nature. These attributes can change and generally are reflective of relationships that the entity holds with other bodies. | • National identifier number<br>• Telephone number<br>• Email address | • Identifying numbers<br>• Legal jurisdiction directors | • Identifying numbers<br>• Custodianship |

Adapted from: WEF - A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity, August 2016

Today, when we are asked to present documents or ID cards in offline situations, we often present something that actually contains far more information (or 'far more of our attributes') than is necessary to enable the transaction we are trying to complete. To use a well-worn example, when a young person is asked for ID at a bar or nightclub in order to prove they are old enough to buy alcohol or gain entry, they might present a document that reveals their name, their date of birth, the name of an organisation or institution that they belong to, and so on. All that is really needed by the barman or doorman however, is a single attribute that indicates 'is entitled to buy alcohol' or 'is entitled to enter nightclubs'. As long as the barman and doorman can trust the presentation of those single attributes, they don't even need to know the person's date of birth, let alone anything else. A bit of extrapolation shows that the same is true of a great many other transactions. As a San Francisco workshop participant pointed out, even most digital *financial* transactions would rarely actually *need* much in the way of personal data attributes to be shared. An answer to the question, 'Can this person, whoever they are, use this credit card number, to make this purchase: Yes or no?' is all that is required.

Assuming a future in which the technical challenges of building a Digital ID system where digital presentation of single attributes like this can be trusted, then a full 'Digital ID' may never actually play a part in such transactions; at least not from the perspective of those involved. The barman, to follow our example, simply gets a 'yes/no' answer to his question of whether to serve the customer, and a proof that he has asked the question and been given a reliable answer. No more, no less. What is clouding our mental image of this digitally transformed transaction perhaps, is that in an offline world we understand it in terms of the presentation of a collection of attributes, an ID. It seems difficult to let go of that culturally ingrained concept when imagining the same transaction taking place digitally.

Once we have a fully-fledged, interoperable digital system that allows the exchange of granular attributes, it is likely that users will come to understand digital transactions in terms of the management of specific pieces of information, rather than wholesale presentations of digital ID. The analogue to the offline world will disappear.

This argument may not work in every conceivable model and implementation of a Digital ID system. It may only apply in specific situations in which users have full choice and full control over the attributes they share during a digital transaction. However, given the difficulties involved in communicating Digital ID writ-large, the idea of granular attribute (or information) exchange may offer one potential way forward.

An answer to the question, 'Can this person, whoever they are, use this credit card number, to make this purchase: Yes or no?' is all that is required.

# The purpose and value of Digital ID

The previous discussion opens up a debate around what Digital ID systems might actually be i.e. is it really about identity, or about information exchange? In our Australian workshop, this was built on further, with a suggestion that another reason Digital ID is so hard to communicate, is that its *purpose* is ill-defined. A sub-group of participants within that workshop argued and discussed for several hours over how to determine a single over-arching purpose to Digital ID, and failed to conclude. They did not suggest that there were no uses for Digital ID, or that the purpose, or missions behind different stakeholders' approaches to the development of Digital ID could not be identified. Rather they were suggesting that there was such a cacophony of different uses and missions that it was impossible to draw a single articulable thread through them all. The voice of the ultimate end-user (the consumer or citizen), in particular, was often completely lost in the din.

It might be tempting to suggest that Digital ID does not need a single over-riding purpose, and that it's multiple uses and purposes can co-exist. There is some truth to this, and, given the inevitability of the emergence of more interoperable Digital ID systems over time, and their likely centrality to the ways in which we will conduct out digital lives, it is surely inevitable that digital identities *will* eventually have as many social *purposes* as our 'real world' identities do. The problem is that building a Digital ID eco-system for the future (on-boarding users, building interoperable digital infrastructures, developing attribute storage models etc.) requires some measure of co-operation and investment from different stakeholders, be it financial institutions and governments, consumers and corporations, or citizens and states. Without a unity or clarity of purpose, such co-operation is likely to be slow.

As one workshop participant in London pointed out, *"…the development of a truly interoperable Digital ID system suffers from a classic 'collective action problem'.*[23]" – whilst many organisations can see the benefits of a fully functioning Digital ID eco-system, co-operating to build it would require investments that, in the short term, benefit other organisations in the eco-system more than themselves. A simple example of this problem might be the perverse incentives around 'Know Your Customer' (KYC) guidelines and financial institutions.

In theory, a system of interoperable Digital ID could be built around the verified attributes of bank customers. Banks have already done much of the work required to verify that their customers are who they say they are, when they open accounts. If bank-verified attributes (name, age, citizenship, address etc.), which already constitute a digital identity, could be stored in a portable Digital ID, allowing customers to share the verified attributes whenever and wherever they open a new account or transact with a financial institution, the whole sector could avoid the costly inefficiency of replicating the same verification procedures over and over again. The problem is, of course, that building such a system requires collective action, to build universal standards. Why would a single bank invest in building such a system, only to give their customers Digital IDs that they can use to quickly and easily move to a competitor? Similarly, why would a government step in to build and maintain such a digital infrastructure, bearing the costs and the risks, when it is private banking institutions that have the most to gain from it? And so on.

The key point for us however, is that in the future, Digital ID might bring transparency to data provenance, changing the ways we think about and conceive of our role in a data-driven society and economy.

Such considerations bring us back to the question of purpose. If Digital ID is going to be seen as more than just a 'nice to have' for consumers in particular use-scenarios, then different stakeholders are likely going to have to learn to articulate the value of many different Digital ID propositions, not just the ones that directly benefit themselves. Those stakeholders that make the effort to do so may well be the eventual winners, able as they would be to recognise fully and early, the wider and longer-term implications of the advent of Digital ID, for us all.

There are also immediate benefits to understanding value from different perspectives. If, for example, a Digital ID system requires end-users to invest time and effort in creating, filling and learning to use a Digital ID, then the value to them needs to be clearly spelt out. If I, as a user, am going to trust a system with my biometrics and my most highly sensitive personal information, then I may want to know that there is some other value to me than reducing the transaction costs for financial institutions on the rare occasions when I change my bank account. This is a little flippant perhaps, there are potentially many other tangible user-benefits[24], but in a world in which consumers and citizens are becoming more and more aware of the value of their personal data, the Digital ID value exchange will likely need more clarity and transparency.

There is much more that could be said around the purpose of Digital ID that would require the luxury of a weightier tome than this to fully explore. However, as was pointed out during that Australian discussion, it is worth considering that however we imagine the purpose of Digital ID today, it may not reflect the purposes that evolve over time. The various values and benefits associated with it now could be become redundant, or be dwarfed by new Digital ID applications that come with future iterations. If the primary value now is to enhance aspects of an existing digital system (i.e. the choice, speed and security of digital transactions) are there future applications of Digital ID that actually remake these transactions altogether?

One such future application might come from the relationship between Digital ID and data-provenance. Leaving aside privacy considerations for a moment, there are many ways in which Digital ID can enhance data-provenance. If today Digital ID is described as the answer to the question 'how can you prove that you are who you say you are?', then it is not a stretch to see that it could be an equally good answer to the question 'how can I be sure where this data comes from?' or even, 'how can I be certain who this data belongs to?'. The impacts of this on the value of data (personal and non-personal) and where it accrues, could be profound.

Perhaps the clearest example was given to us by a participant in Singapore in relation to health data. Using wearable sensors, 'smart' devices and digital personal diaries, an individual may be able to collect a vast amount of personal health data. This individual could be asked to share, or could offer to share, that data with, say, a healthcare provider or health research body. At this point, a choice could be presented to them as to whether their data is used solely to build aggregated data sets and effectively anonymised or destroyed thereafter, or whether it is permanently attached to them, allowing for more data, including more contextual data, to be added in the future. By allowing the data to be attached to them, the individual would be greatly enhancing its value. Assuming that the data collector can be *sure* that the data does indeed come from the same person, and can also be sure that any future data from that person can be attached to it, they can learn a great deal more from it. For the individual too there is the possibility of being provided with a much more highly personalised and therefore effective healthcare service.

It is around the degree of confidence that the health researchers have in the provenance of the data that a Digital ID comes in. A Digital ID could be used at both ends of such a transaction, validating the consumer's identity during data collection by sensors, and then during the sending of the data to the data collector. Theoretically, a Digital ID could also be used to share other verified data (in the form of identity attributes) providing even greater context to the original health data, and again increasing its value to the researchers.

There are many other contexts where the same thinking applies. As a rule of thumb, data with provenance is of greater value – is more useful - than data without provenance (which of course is one reason that we are constantly asked to create accounts for digital services where there doesn't seem to be any need to do so). It should be remembered that a strong Digital ID can't always give certainty to the data within a data set, the reliability of the specific health data in our example lies elsewhere, but it *can* provide certainty around where the data comes from. In theory, a Digital ID product could also provide both the storage and distribution mechanism for *any* data a person creates (alongside verified attributes), always giving the option of providing strong provenance. There are already Digital ID start-ups whose long-term business models are based on precisely this fact.

Extending this a little further, if Digital ID can provide data with provenance, then could it also be used to tackle the knotty question of data ownership? Although the strict legal fiction of data ownership is a matter for legal and philosophical debate, future iterations of a Digital ID system could present a whole new context for that discussion. Without getting into the complexities, it is possible to imagine a future in which all of the data that we create is branded with a digital signature, verified or generated by a strong Digital ID. In theory then, chunks of our data could be traced through digital processes, like sheep with colourful farm brands wandering between fields. This could provide a mechanism for establishing the specific contribution our data has made (and is making) to processes such as machine learning, or the data-driven development of products and services. Such branded data need not even be confined to personal data. It could also apply to the data generated by things we *own;* phones, vehicles, or even smart fridges.

If we can trace the contribution of 'our' data in a value chain, then does this imply that there is a mechanism by which we can be fairly recompensed for our data contributions to a data-driven economy? In theory, as was argued by one data-provenance evangelist we spoke with during our programme, a portion of the economic value our data helps to create could be channelled back to us in the form of real monetary compensation. This idea was met with some challenge and incredulity (both technological and in relation to the current willingness among service users to provide data without monetary compensation). The key point for us however, is that in the future, Digital ID might bring transparency to data provenance, changing the ways we think about and conceive of our role in a data-driven society and economy. Even if the idea of tracing data contributions was initially realised in only very limited contexts, it could still have a profound effect on attitudes towards other interactions with data-driven services.

These are the disruptive ideas, but it is also quite possible that the driving factor that finally leads to the development of large-scale Digital ID systems may have little to do with direct user-benefits or value, at all. As the authors of a report commissioned by the Omidyar Network point out: *"For governments […] providing identity is a fundamental goal that underpins its ability to measure, manage, and control."*[25]

In other words, when considering the purpose of Digital ID, we may need to remember that different stakeholders have different purposes. Providers will need to be able to make clear to end users exactly whose purposes their particular model and system is serving. There may be consequences for not being transparent. Consider, for example, the fallout from the ways in which different groups within Facebook repurposed the collection of more verifiable identity attributes from its users to enhance targeting, even after telling users that they were being collected to enhance the security of their accounts[26].

# Convenience rules

Given much of what has gone before and the hifalutin talk of 'purpose', it is perhaps ironic that in most of our workshops there was a measure of agreement that the primary driving force behind the eventual emergence of Digital ID systems would most likely be the same driving force behind most tech development thus far: convenience. Digital ID may, eventually, prove to be a catalyst for changing the human digital experience, but in the short term, it is more likely to be the simple speeding up of transactions, and the promise of being able to use a single Digital ID in multiple different contexts (its interoperability) that consumers reach for.

As one workshop participant put it: *"We are likely to end up in a Betamax vs. VHS scenario, in which experts point to the 'better' option, while the market swarms down the path of least resistance."* With the big data companies (Facebook, Google, Amazon etc.) all beginning to consolidate their identity tools, it may be that the future faces of 'convenient Digital ID' are already sitting right in front of us. In the long term this may not be the best option for users, but as was pointed out in Singapore, the model for this path already exists in China. Tencent's 'everything app' WeChat is fast moving through the stages of being a *de facto* Digital ID due to the size of its user data sets, to providing verified attribute ID services, to being an officially approved vehicle for national ID.

# Proxy Digital IDs

One of the consequences of having a sector focussed on the idea of 'Digital ID', with its connotations of attributes stored in documents and wallets, is that it can set up an artificial wall that obscures different approaches to the problems it is trying to solve. If Digital ID is ultimately the answer to the question of how we prove who we are and the claims we make in digital environments, then we should consider the other ways of approaching this question. Digital ID is attractive as an option, because, in its ideal form, it is about connecting the most trusted institutions in society with those service providers who need to have a high degree of confidence that we are who we say we are, and allowing users to mediate that interaction. But there are other ways of 'verifying' attributes.

Some Digital ID providers are already exploring and testing the possibilities of using facial recognition, not just to identify that a person is who they say they are, but also to determine their age, without reference to any particular document or institutionally verified attribute. At the moment, the algorithms driving such 'age recognition' systems are confined to determining the likelihood that someone is above or below a certain age, but there is a wider implication. In the future, to what extent could the deployment of algorithms, able to access large portions of 'set of me' data, be used to make high-probability determinations of other identity attributes? Could they accurately determine our permanent residence, by cross referencing location data and fields in social media accounts, or our nationality, our GP, our income level etc. In other words, might algorithmic recognition negate the very need for Digital ID in most circumstances? Could service providers come to solely rely on other parts of the digital identity Venn diagram to verify whether we are who we say we are?

## **CASE STUDY:** Facial recognition and Yoti

YOTI

*Yoti, a UK-based Digital ID platform uses facial recognition technology in interesting ways. Age verification via the "Yoti Age Scan" (YAS) is useful, for example when purchasing age restricted items at self-checkouts. As they say themselves:*

"YAS is a secure age-checking service that can estimate a person's age by looking at their face. We consider it to have wide application in the provision of any age-restricted goods and services, both online and in person.

YAS is designed with user privacy and data minimisation in mind. It does not require users to register with us, nor to provide any documentary evidence of their identity. It neither retains any information about users, nor any images of them. The images are not stored, not re-shared, not re-used and not sold on. It simply estimates their age."

This is an example of Digital ID technology being used in the absence of an ID itself.

The barriers to this future may lie in questions around how such identity algorithms could be deployed at specific moments, the level of ‘noise’ in current personal data sets, and the extent to which such systems would be fallible or game-able. But in many ways the building blocks of such a future already exist in the form of huge personal data stores, centralised, and under the control of, precisely those organisations that might be able to deploy them. Early precedents already exist in the form of digital behaviour recognition, and the thinking behind proxy identification is already built in to the blueprints of many new Digital ID systems.

The idea of proxy identification seems to elide many of the different ways of thinking about digital identity that we outlined in our opening section, in perhaps uncomfortable ways. It suggests a digital future in which not only are we unable to escape identification, but also have little power over how we are being defined by those doing the identifying. In the next section we explore a different perspective on the future of Digital ID. One in which Digital IDs and ID systems could shift the balance of power in a digital world back towards the individual.

Proxy digital ID suggests a digital future in which we are unable to escape identification.

# 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