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

Contents

Foreword

In today's era of hyper-connectivity, our devices act for us and digital services blend seamlessly into our daily lives. This brings us huge benefits and has changed many aspects of the way we live, but we still have one foot in the past. Identifying oneself is still rooted in the physical world and, for the five billion people online, digital authentication is burdensome and somewhat unreliable. Furthermore, being part of the digital ecosystem can come at a price, with people handing over too much private data in exchange for the promise of enhanced digital services and technology.

We can imagine a world where a person's identity and the devices operating on their behalf can be verified immediately, safely and securely, across multiple touchpoints and in both the digital and the physical world. Where access is gained without passwords and no identifying data is given away or put at risk. Where the capability to identify ourselves can work across borders and platforms. This is the future with digital identity.

With this in mind, we are delighted to initiate this open foresight program exploring the 'Future of Digital Identity' in partnership with Future Agenda. This report provides us with a set of insights, gathered from an array of leading experts and interested parties from around the world, that can help us collectively seize the positive opportunities that digital identity provides, whilst ensuring that we mitigate many of the potential risks. In short, this report aims to help us all make more informed decisions on the best route forward and work together to make a viable and trusted digital identity a reality.

We would like to thank all those who contributed to and participated in the program and look forward to collaborating with them and many others to realise the full potential of digital identity.

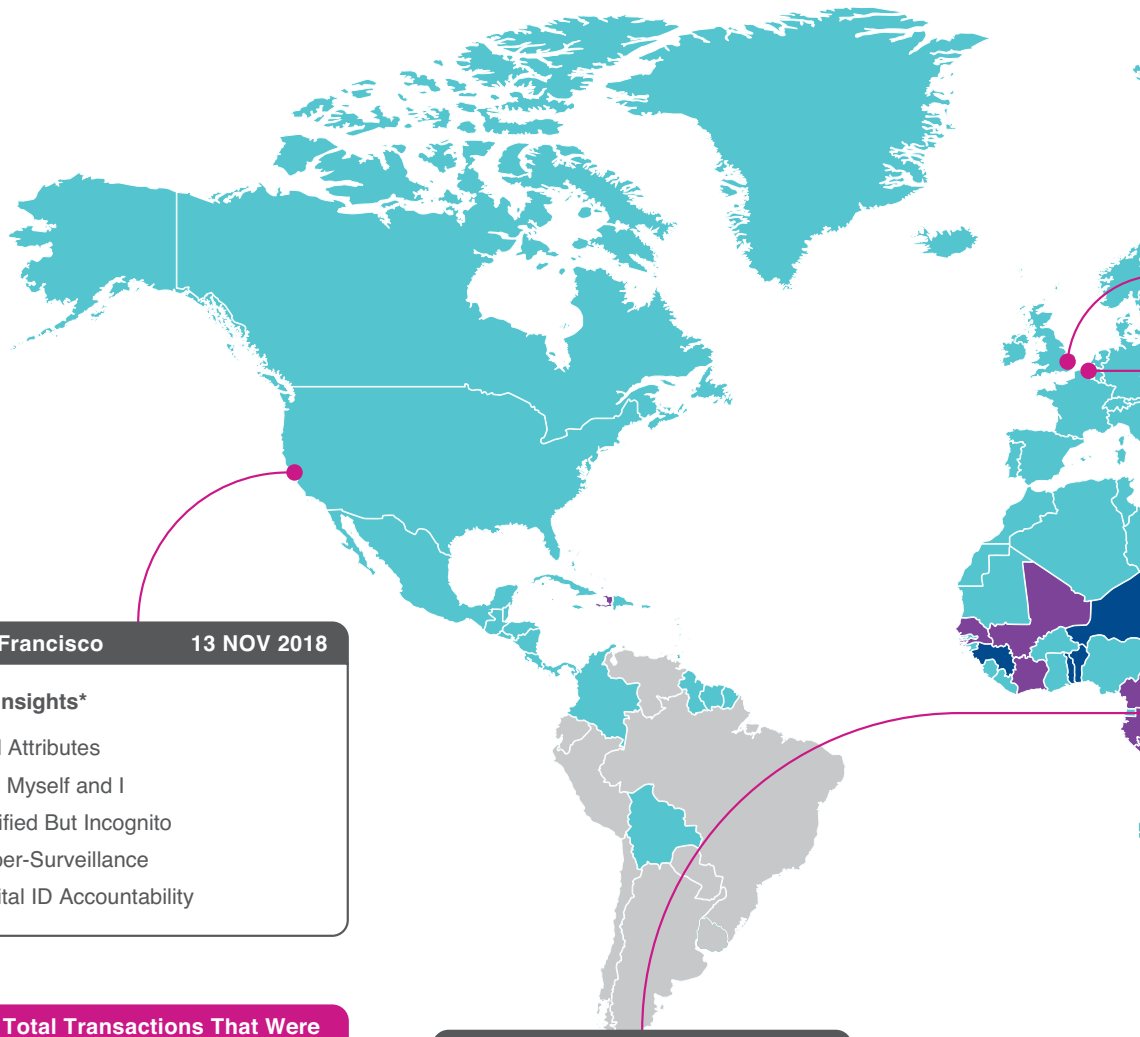
Ajay Bhalla, President,
Cyber & Intelligence Solutions
Mastercard

Acknowledgements

The Future of Digital Identity programme was thoughtfully and generously initiated by Mastercard. We would like to acknowledge and thank them for their collaboration and support in developing this open foresight programme.

In addition, we would like to thank the generosity of the 120+ informed experts who contributed their time and foresight into the programme. The enthusiasm of all those attending our events in 5 cities and 4 continents (Singapore, Sydney, London, San Francisco and Brussels) demonstrates an appetite to share experience, explore ideas, consider options and identify how to build more positive future directions. We thank them, most sincerely for their support, contribution and encouragement.

Future of Digital Identity (2018/19)
Locations and Key Insights



San Francisco — **13 NOV 2018**

Top Insights*

- Null Attributes
- Me, Myself and I
- Verified But Incognito
- Super-Surveillance
- Digital ID Accountability

% of Total Transactions That Were Recognised As Identity Spoofing

REGION	TOTAL
Africa	16.5%
Asia	12.8%
Europe	7.6%
Australia	6.8%
South America	6.3%
North America	5.6%

Source: Threat Matrix Cybercrime Report - Q2 2018

Singapore — **30 OCT 2018**

Top Insights*

- Setting the Standards
- Enhanced Cyber-Security
- Robust Authentication Equals Trust
- Convenience Rules
- The Case for Digital Inclusion

FUTURE AGENDA
Open Foresight

Brussels **27 NOV 2018**

Top Insights*

- Social Scoring
- Ethics By Design
- Influence of Scale
- Personalised Controlled Exchanges
- The Case for Digital Inclusion

London **15 OCT 2018**

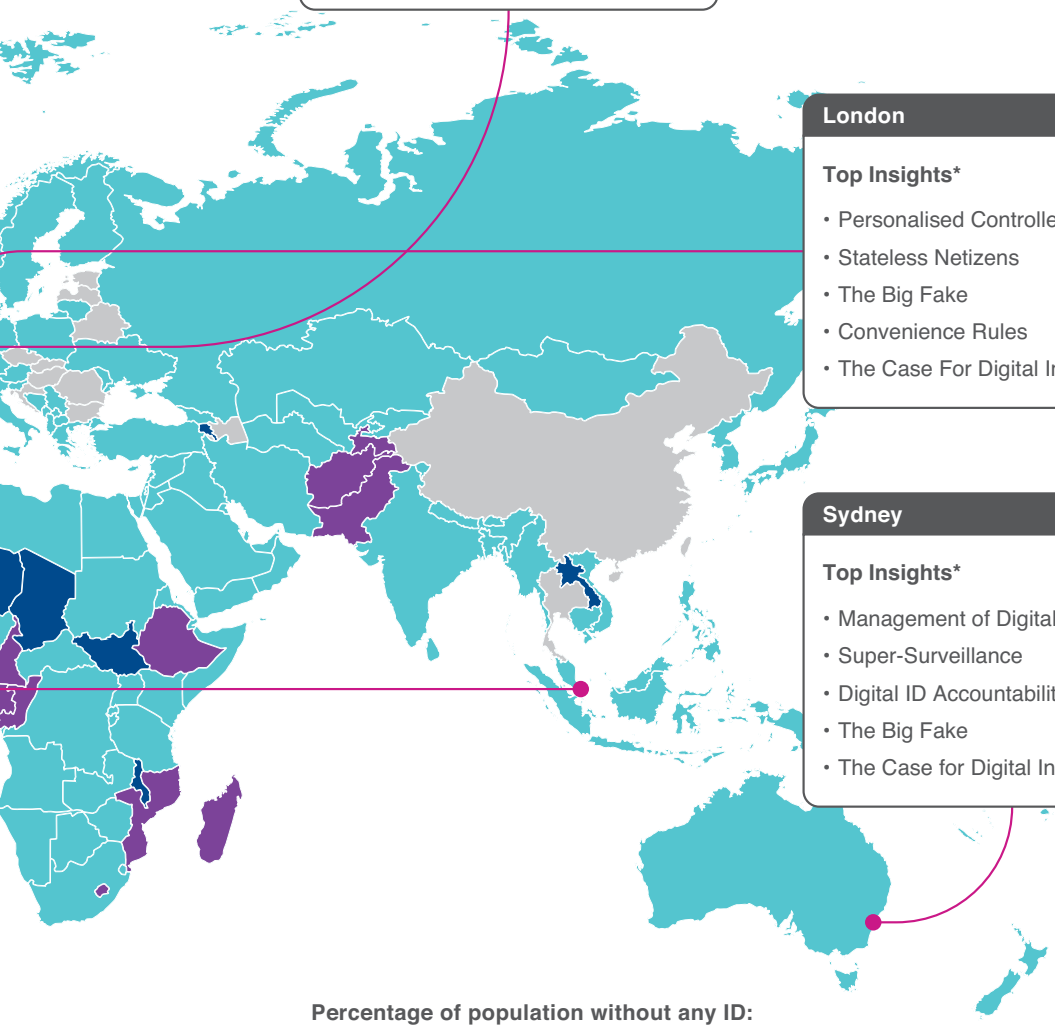
Top Insights*

- Personalised Controlled Exchanges
- Stateless Netizens
- The Big Fake
- Convenience Rules
- The Case For Digital Inclusion

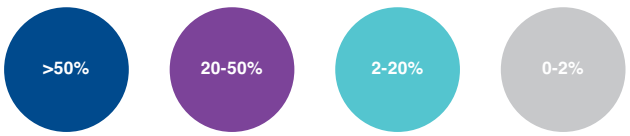
Sydney **02 NOV 2018**

Top Insights*

- Management of Digital ID Rights
- Super-Surveillance
- Digital ID Accountability
- The Big Fake
- The Case for Digital Inclusion



Percentage of population without any ID:



Source: World Bank 2018 http://id4d.worldbank.org;

The report and data presents economy-level aggregates on the share and number of the population without a foundational/national ID, based on surveys covering over 100,000 people in 99 economies—representing 74 percent of the world's population.

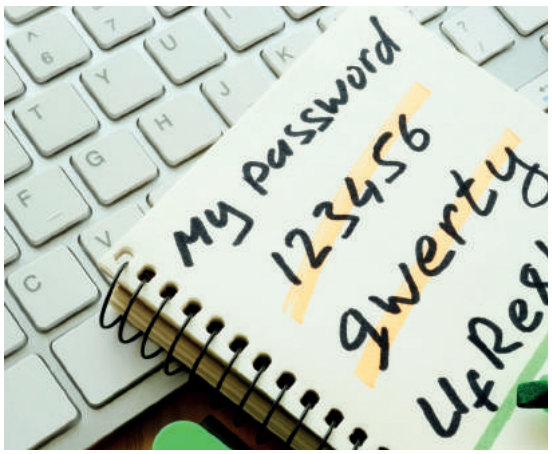
Executive summary

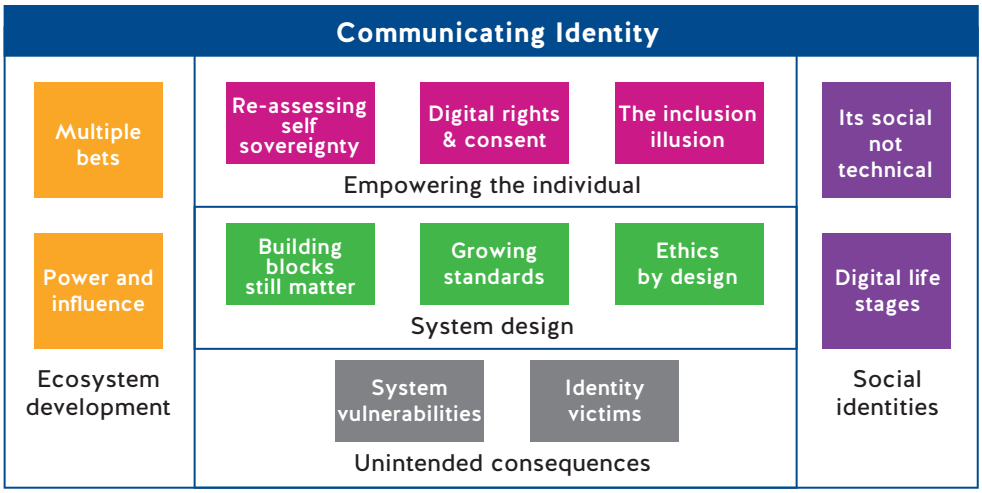
In an ever more digital and digitally connected world, how we resolve our digital identities will likely prove a fundamental underpinning, as well as an enabler, of human progress. This statement seems grandiose for a field that has largely been confined to a niche within the tech industries, but it is not an exaggeration. Quite simply, the knowledge of exactly who or what we are dealing with is a prerequisite of all communication and exchange. And yet, in digital contexts, it is all too often difficult, cumbersome or insecure to produce the traditional identity, credential and entitlement proofs that are so familiar and so important in the offline world (ID cards, passports, certificates etc.). The days of physical documentation as proofs of identity appear to be numbered.

Today, we live with a mess of ad-hoc attempts to solve the problem. We have wallets full of cards and bank security tokens, devices full of security applications, and notepads, documents and heads full of usernames and passwords. How we prove our identity in one digital context is almost never how we prove it in another. Our own clumsy attempts to make digital travels more seamless - using and re-using variations on easy-to-remember passwords, taking the reliability of people and digital personae at face value, and so on - has led to endemic cyber-insecurity. Reliable and secure Digital ID could change all of this.

Interoperable Digital ID is alluring in its promises of convenience and security alone. But digital identification and being able to digitally attach information to a proven identity is, as it turns out, potentially a much more fundamental game-changer. It could quite literally reshape the human digital future, helping to shift power back to individuals, re-asserting digital privacy, perhaps solving the knotty question of data-ownership. It might even be the means of addressing some of today's pressing humanitarian crises. More darkly, it could also be used as a means of mass surveillance or social control, or be the ground-zero of future cyber-attacks unless the correct controls are established from the start.

This report outlines the findings and insights of a Future Agenda Open Foresight Programme exploring "The Future of Digital Identity". It is built from the outputs of a multi-country programme of workshops and insight gathering that included over 120 leading experts, decision-makers and stakeholders in the field.





Report structure - Key findings

There is little doubt around the potential for interoperable Digital ID systems to bring great benefits to societies and economies. However, programme participants consistently highlighted the need to find clearer, more consumer-friendly (or citizen-friendly) approaches to communicating them. They highlighted a gap between the simple proposition of a 'digital passport', and today's reality in which current Digital ID products have limited scope for use across different contexts, differ in terms of their over-arching missions, objectives and promises, and in which coming to grips with the social and technical implications of different implementations is a daunting task. This is before even getting to the fact that the term 'identity' (digital or otherwise) already has an enormously rich set of societal baggage that is quite independent of the project of 'Digital ID'. Some suggested an end to the use of 'identity' altogether. We see this as perhaps an over-drastic response to the matter, but one which does at least highlight the urgency of the communication issue.

Better communication is likely to include more vivid and tangible illustration of both the long- and short-term opportunities and benefits for end users and stakeholder organisations alike. Such articulation however, may only arise from collaboration and consensus between different Digital ID stakeholders. Even larger players may have to come to a better understanding of the different motivations of potential partners in order to come to a shared understanding around language, goals and common measures of success.

During the programme, this issue of communication arose frequently. It was not just a matter of how to communicate a Digital ID proposition directly to potential users and customers, but also about digital literacy more broadly, and the need to find a shared language for making sense of some of the more difficult concepts that Digital ID raises. As such, we saw 'communicating identity' as an overarching theme, that sat across all of the other topics that were discussed.

Key Insight: Digital ID could re-empower the individual in a digital world

Digital ID could be a tool of empowerment, providing, for example, universal access to services, or rebalancing the current digital and data paradigm in favour of consumers and citizens.

- **Improved Agency -** A key potential benefit of Digital ID for individuals is the future promise of greater control over how their data is stored, accessed and shared.

- **Digital Rights -** Digital ID could provide the means for asserting an emerging set of digital and data rights. It will also likely become key in terms of managing how various non-digital entitlements and rights are issued, revoked, restored and redressed.

- **Digital Inclusion -** Digital ID implementations could provide a means for those who are most socially and economically disenfranchised, to gain access to much needed basic services.

Key Insight: Today's promise of interoperable Digital ID systems is poised for a key influencer or influencers to enter with scale, setting the path for future development.

- System Building Blocks - The basic model of 'claim, attestation, proof' is likely to remain the most robust (and simple) articulation of the process undertaken when applying Digital ID in a given exchange. Transparency regarding data access and onward usage, as well as the security of information transfers, will be the key shorter-term battlegrounds.

- Format Wars - given the fragmented nature of propositions emerging from a multitude of innovators and systems developers, we can expect to see 'format wars' in coming years.

- Early Winners - early winners will likely find themselves quickly burdened with the risks and responsibilities associated with maintaining a highly-sensitive and (eventually) mass-adopted system.

- Ethical Trade-offs - Designers of Digital ID systems will have to confront trade-offs between the ethics of privacy, security, accessibility and the need to meet urgent societal demands; whilst meeting the functional requirements that the market requirements.

- Ethics Opportunities - Digital ID stakeholders have an opportunity to consider ethics (and unintended outcomes) at the outset to provide an example to others of good data-driven technology development.

Key Insight: With clear benefits in view and a fragmented identity landscape that is clearly unfit for purpose, the next stage of Digital ID development will be defined by the 'bets' being placed, and successfully leveraged, by key stakeholders today.

The Digital ID landscape today is somewhat fractured with a variety of different stakeholders approaching the technology with different aims and different hopes. These varying perspectives on Digital ID are provided by (among others): National ID providers, the growing attempts to develop solutions based on international financial mechanisms and the organisations that underpin these, supra-national voices such as GSMA, The World Bank and the UN, and independent developers and funders such as, Yoti or the Omidyar Network. How these groups wield power and influence in coming months and years, and the successes they are able to attract, will have great bearing on the future direction and development of Digital ID systems.

- Regional and contextual alliance - Regional or contextual partnerships and alliances (trade blocs, supply chains or cross-sector and cross-industry partnerships, for example) could provide the biggest driver of early, truly interoperable, Digital ID systems.

- Distribution of Influence - with a value chain and eco-system still to emerge, influence and power are still to be distributed across the landscape of Digital ID providers, users, transaction service providers, data-storage providers etc.

- Emerging roles - New roles, such as services designed to help us navigate and best exploit the power of Digital-ID-enabled environments or Digital ID managers and assistants, could emerge to help users in a mature Digital ID eco-system.

Key Insight: Digital Identity is a social construct, not a technical battleground

As Digital ID becomes more embedded in our lives, some of the socio-cultural aspects of identity will likely influence our technological IDs. How we hope to be recognised, how others choose to see us and how we elect to represent ourselves in different ways for different situations or circumstances are as relevant in the digital world as the physical world. Digital IDs need not be as 'constrained' as paper ID documents, and as such are likely to accumulate for wider social significance, leading in turn, to inevitable, but as yet unknowable, user innovation.

- Social and Digital Identity – Digital ID development could empower individuals to see which kinds of data different service providers are seeking, for what purposes, and the outcomes of that sharing, allowing them, in turn, to selectively share and thereby influence and manipulate how they are seen and understood by service providers.

- Digital Life Stages – Should Digital IDs become a fundamental human right (as some suggest) then key questions will need to be addressed such as: Should Digital IDs be issued at birth? How will Digital IDs handle changes over the course of our lives? What happens to our Digital IDs after we die? And who will have the right to 'terminate' a Digital ID? Could the first immortal Digital ID already exist?

Key Insight: Digital Identity, like other mass technological innovations in our lives, will have unintended consequences. How they are made manifest is largely dependent on how the industry plots its own development, and by the decisions being made today.

Unintended consequences have come to characterise many of the technological innovations now embedded in our everyday lives. There are some steps that current and potential Digital ID ecosystem partners can take today to offset a range of unintended consequences. These include: greater collaboration, commitment to transparency, decentralisation by design, establishing lines of accountability, human-centred development and the establishment of frameworks of rights, responsibilities and ethics for both users and providers. Taking such steps early would require a marked change in mindset from that which characterises much of the tech industry today. Key unintended consequences that Digital ID solutions would want to avoid include:

- System Vulnerability - As Digital IDs become critical to the ways in which we access basic services, attacks and breaches of a Digital ID system could bring immediate and potentially life-threatening problems for those affected; possibly at the scale of entire populations (e.g. all citizens of a nation state).

- Identity Victims – Identity markers and identity data stores both have a long history of being used as the means to enact oppression, discrimination and social control. Stakeholders in the development of Digital ID systems need to take steps to ensure that, as far as is possible, Digital ID users are protected from the worst outcomes of identity mis-use. Future identity victims, after all, could include any one of us.

Digital identity is a complex idea, but that should not dissuade us from exploring its potential to transform our collective digital futures for the better. Even the most immediate promise that interoperable Digital ID systems could allow us fast, safe, secure and reliable passage through digital spaces and digital interactions and transactions is tantalising indeed.

We are still in the early days of the human digital transformation and almost certainly do not yet have a grasp of how truly fundamental an understanding of digital identities will be to the future human experience. Digital ID, today understood as how we can prove that we are who we say we are, will likely become the primary mechanism through which we construct our digital selves and engage with and inhabit tomorrow's digital spaces. It could be the key to unlocking the true value behind "Big Data", providing unstructured data-sets with meaning and context, as well as providing the means by which we can all benefit from that. Similarly, the technologies and protocols associated with the development of Digital ID systems could become the pivot points for paradigmatic shifts in our digital society, rebalancing control over the data stream in favour of the individual, or opening us up to new mechanisms of social control.

Today, there are many thoughtful, innovative and forward-thinking people and organisations working on the development of Digital ID. With encouragingly high levels of awareness around the potential pitfalls of poor implementation, they are likely to lead the way in realising the many social and economic benefits that Digital ID could bring.

We are still in the early days of the human digital transformation and almost certainly do not yet have a grasp of how truly fundamental an understanding of digital identities will be to the future human experience.

Introduction

We all have digital identities. In the moment that we first logged on to a computer or connected to the internet, our digital identities were born. Little did many of us understand the technical complexity that lay behind this digital birth. Even less did we understand the impacts of habits formed when we set up our first ‘user name and password’ and took baby steps into our digital future, leaving binary-coded footprints as we went.

In 2019, we still may not understand the complexities behind the technologies we use, but the impacts and consequences of our early digital behaviours are becoming clearer to us all. Aspects of our digital selves are leveraged to deliver miraculous new kinds of services for sure, but they are also stolen, mistaken, sold, targeted, abused, fed into mysterious algorithms with unknown (and perhaps unknowable) consequences, and used to drive creative and sometimes horrific crimes. At the time we write, there is a growing consensus that the unintended and negative consequences of the ways we interact in digital spaces are not always a price worth paying; that something needs to change. Trust in the digital age, is in decline.

Much of the public debate around our collective digital futures centres on concerns about the harvesting, storage and use of big data, with the EU's landmark GDPR (General Data Protection Regulation) legislation perhaps the most iconic early outcome. Through its radical approach to the use of, specifically, personal data, GDPR represents perhaps the first large-scale attempt to reformulate the rules governing digital interactions, and to hand some power and control back to ordinary citizens.[1] However, regulations such as those laid out in GDPR (other jurisdictions are sure to follow swiftly), still play out in a digital landscape and over a digital infrastructure that was not designed to easily fulfil them. In fact, much of the digital infrastructure we make the most use of today - social media, 'free' search services, cloud-hosted or enabled email and communications services, internet service provision etc. – was designed with precisely the opposite set of objectives in mind.

Some argue that, given the precedents we have already set, the infrastructure that exists, and the habits and heuristics that we have already formed, the personal data genie is out of the bottle and that expectations around privacy have or must change accordingly. GDPR notwithstanding, it is suggested, we should learn to embrace a world of data transparency. But it is also true that, albeit belatedly, popular and regulatory understanding of the issues of data privacy, and data rights more broadly, is rising. In turn, this is likely to lead to greater public awareness of concepts and technologies that could change current digital paradigms: encryption, decentralisation, distributed data networks, blockchain technologies, and so on.

In particular, we are also likely to see more and more focus on 'digital identity', an idea which can encompass all of these concepts, tying our digital selves to personal data and notions of trust and security, as well as to cutting edge technologies. The concept of digital identity has been around for as long as computers themselves, but thanks to new data processing techniques, leading companies looking to develop new technologies at greater scales, new business models, emboldened governments and regulators, and a clearer public understanding of what it means to live in a digital world, we seem to be at an inflection point. In the coming months and years, 'digital identity' is likely to be forced out of its industry niches and into the mainstream. As it emerges, it will bring to the public sphere a whole host of technical challenges, ethical questions, hopes and fears, promises, misunderstandings and ideological debate.

In the coming months and years, 'digital identity' is likely to be forced out of its industry niches and into the mainstream. As it emerges, it will bring to the public sphere a whole host of technical challenges, ethical questions, hopes and fears, promises, misunderstandings and ideological debate.

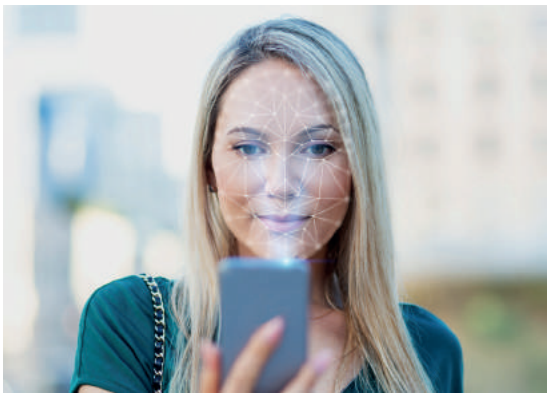
The promise of Digital ID

If the concept has been around for so long, why do we need to be talking about digital identity today? The answer lies in a recent surge of interest, innovation and investment around the idea of Digital ID[2], the means by which we can prove that 'we are who we say we are' in digital contexts and during digital transactions. Why is this important? Put simply, the knowledge of exactly who or what we are dealing with is a pre-requisite for all communication and exchange. And yet today, in a digital world, this fundamental aspect of human interaction is becoming increasingly difficult. It is all too often tricky, cumbersome or insecure to produce traditional identity, credential and entitlement proofs (ID cards, passports, certificates etc.) in a digital context. The days of physical documentation as proofs of identity appear to be numbered, but what are the alternatives?

Today, we live with a mess of ad-hoc attempts to solve the problem. We have wallets full of cards and bank security tokens, devices full of security applications, and heads, notepads and documents full of usernames, passwords and pin numbers. Each time we join a new service, or try to access a new digital service, or yet another offline service moves to digital delivery, we seem doomed to collect yet another set of credentials. How we prove our identity in one digital context is almost never how we prove it in another. Our own clumsy attempts to reduce this complexity and make our digital travels more convenient - using and re-using variations on easy-to-remember passwords, taking the reliability of people and digital personae at face value, and so on – have only led to endemic cyber-insecurity.

Imagine instead, a world in which we all had access to a single, digitised form of identification accessed, say, through a mobile device. A single tool that could be used to prove that we are who we say we are, and have the entitlements and rights that we claim to have, in any digitally connected context. A single tool that could be used to create and access online accounts or move data between different service providers in an instant; or cross international borders without waiting in line; or verify that we are the owners of a credit card or bank account; or assure others that we are over (or under) a certain age, or affirm our nationality, or our right to drive a car; or simply confirm that we have indeed had the fifth cup of coffee needed to collect a free donut. Furthermore, imagine that such a tool was designed such that it enhanced, rather than diminished, our personal privacy, and that re-using it made us more, rather than less, digitally secure. These are among the potential capabilities of a Digital ID within an interoperable ID system.

The initial promises then, are alluring enough, but in the longer-term Digital ID could bring even more profound benefits, as long as we can successfully avoid the potential pitfalls. In this report, the outcome of a global Open Foresight gathering process run by Future Agenda, we will also explore the future potential for Digital ID to radically reduce bureaucratic transaction costs globally, open doorways to new kinds of personal service innovation, rebalance the digital paradigm in favour of the individual, and even introduce new pathways to resolving intractable humanitarian crises. Assuming the advent of interoperable Digital ID is becoming inevitable, it is likely to play a major part in defining our digital futures.



Approach

The 2018/19 'Future of Digital Identity' programme followed Future Agenda's Open Foresight model to gather and develop emerging views on the topic. Broadly speaking, the model consists of three-steps: 1) An initial perspective provocation, 2) Facilitated workshops with experts around the globe, and 3) Synthesis of emerging views.

First, the outputs of a desk research exercise were combined with insights gained from a dozen stakeholder interviews, to produce an 'initial perspective' on the **'Future of Digital Identity'**. This document served as a point of departure for the programme and the basis for the following workshop discussions, as well as laying out the scope and ambitions of the programme for participants. Portions of that initial perspective remain valid and have been reproduced here, but it also provides a useful baseline for much of the more future-focused discussion laid out in the rest of this report. Some initial insights were also drawn from another Future Agenda global open foresight programme exploring the Future Value of Data, the output of which can be found **here.**

Workshops were then held in five different locations around the world: London, Singapore, Sydney, San Francisco and Brussels. As with all Future Agenda programmes, each event brought together a rich mix of stakeholders and experts in the field who could challenge existing assumptions, share new perspectives and build insightful and pragmatic views on how change is most likely to occur. Workshops took place under the 'Chatham House Rule[3]' to encourage open sharing of views.

Starting with insights drawn from the initial perspective, workshop discussions focussed on identifying the key issues, adding additional views and insights, and highlighting pivotal areas for future innovation and change, globally and locally. New insights and ideas generated within each workshop were carried through into following workshops, to ensure iteration, and scrutiny of each insight.

In all, more than 120 experts, decision-makers and interested stakeholders took part in interviews or workshops. Participants in the workshops alone represented the following different industries and sectors:

Academia	4	4%
Banking	7	6%
Wider business stakeholders	17	15%
Cybersecurity	2	2%
Tech Entrepreneurs	4	4%
FinTech	5	4%
Foundations	1	1%
Government	12	11%
Identity providers	17	15%
Industry Bodies	3	3%
Insurance	1	1%
Legal	2	2%
Merchant services	19	17%
Mobile providers	6	5%
Professional networks	5	4%
Digital platform providers	4	4%
Social Innovation	2	2%
Social Media	2	2%

It is worth saying however, that the future of digital identity is unlikely, at least in the near or medium term, to be uniform. Different initiatives and innovations, from within different sectors, and differing patterns of user adoption and use, within and across geo-political borders, mean that we are likely to see myriad future pathways followed around the world and in digital spaces. The locations of our workshops were chosen in part to gain access to different regional views, but we recognise that, given more resources, the programme could easily have been extended to other locations and that key questions and insights might have been modified or re-prioritised as a result.

Furthermore, and perhaps due to the immediacy of the technical challenges involved in bringing a truly interoperable system of digital identity to life, participants in our workshops often spent a fair amount of time talking about 'today's problems'. As far as was possible however, we encouraged them to think further out, to a five- or ten-year horizon. In this report then, we highlight the areas of greatest consensus as to which parts of the Digital ID landscape were most likely to see the greatest shifts, or provide the most significant drivers of change, over the next 10 years. We do not intend the chapters to cover every aspect of Digital ID, or every argument and counter-argument made in relation to the points we raise.

It is worth saying however, that the future of digital identity is unlikely, at least in the near or medium term, to be uniform.

The insights we collected fell into seven broad areas:

- Defining and scoping the challenge
- Communicating digital identity
- Empowering the individual
- System design
- Eco-system development
- Social identities
- Unintended consequences

When reading these chapters, it is worth bearing in mind that it can become very difficult to keep any conversation about digital identity confined to one specific space or application. The reason for this is that the different definitions and types of digital identity are not discrete. They overlap in multiple different ways. Decisions or principles developed in relation to one aspect of digital identity, have implications for others, and definitions and terminology have subtly different interpretations depending on perspective. We hope that we have managed to provide some measure of clarity in relation to these issues, but recognise that in doing so we may have over-simplified on occasion. We see this report as a catalyst for further discussion, and would welcome further input from interested parties.

Different definitions and types of digital identity are not discrete. They overlap in multiple different ways.

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

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 Attributes that are intrinsic to an entity and are not defined by relationships to external entities.	• Age • Height • Date of birth • Fingerprints	• Industry • Business status	• Nature of the asset • Asset issuer
Accumulated attributes Attributes that are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's lifespan.	• Health records • Preferences and behaviours (e.g. telephone metadata)	• Business record • Legal record	• Ownership history • Transaction history
Assigned attributes 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 • Telephone number • Email address	• Identifying numbers • Legal jurisdiction directors	• Identifying numbers • 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, 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.

Empowering the individual

After a first encounter with the idea of Digital ID as a digitised passport or ID card, it is easy to miss the ways in which it could fundamentally transform the human digital experience, and our future in a data-driven society. But it could, and likely will. In this section we explore the emerging view that Digital ID could be a tool of empowerment, providing, for example, universal access to services, or by rebalancing the current digital and data paradigm in favour of consumers and citizens.

Re-assessing self-sovereignty

The idea of 'self-sovereignty' has taken on something of a life of its own in relation to Digital IDs. The introduction of an idea as lofty as 'sovereignty' can be both a help and a hindrance in understanding such a complex subject. On the one hand, it helps to introduce the importance and centrality of both agency and control. On the other, it brings yet another contentious concept to an already crowded field. Perhaps the desire to talk about sovereignty stems from two things: 1) the loss of control that many feel in the current development of digital societies, and 2) that if we are to have sovereignty over anything in a digital world, it should surely be 'who we are'.

Without wishing to get lost in the arguments and counter-arguments over whether a truly 'self-sovereign' ID can really exist (can we really self-certify?), there are two practical aspects of the debate that might be useful to borrow from. The first is in relation to the control and management of an ID itself i.e. where it is physically located, and where attributes are stored. The second is to do with how much control we might have when sharing those attributes.[27]

such as storing data on individual devices and/or various models of distributed and decentralised networks and ledgers, encryption tools, blockchain implementations and so on. Each presents challenges in terms of implementation and each has flaws when considered either against an idea of absolute sovereignty, or the need to recognise the fundamentally social aspect of ID (namely, that our claims to being who we are don't mean much if no one else agrees with us)[28]. However, they are bound together by the ambition to decentralise the Digital ID eco-system, keeping individual ID data packages out of centralised databases controlled by large organisations (corporate or governmental). The most important aspects of all of these proposals then, is that they each aim to enable the second aspect of Digital ID sovereignty: giving individuals a measure of control over how data is accessed and shared.

Agency and control will not just be about allowing individuals to store or move their data however, it will also be about how Digital ID applications are designed and built. For example, attributes within Digital IDs could be constructed so as to protect certain fundamental aspects of our identity, and yet still give the necessary confidence to others that we are who we say we are or have the rights and attributes we claim to have. Our dates of birth could be translated into the 'entitlement to buy alcohol' or the 'right to a child's fare'; our names could be obscured by unique identifiers, and so on.

Further, the interfaces of Digital ID applications could help to provide individuals with a far greater level of transparency when taking part in personal-data transactions than is currently the case. For example, Digital ID transactions could be designed such that they must involve ID holders being told exactly which attributes they are being asked to share, when, with whom, and for what purposes. Individuals could then also be given granular control over whether to share some, all or none of the attributes, as they wish.

These kinds of mechanisms would vastly increase an individual's control over the amount of personal data and information that flows from them, to others[1], and building on this principle, we can imagine significant changes to what is currently considered normal during digital interactions. Digital ID driven digital journeys could involve for example, regular and secure access to digitally-delivered services without disclosure of who we are, the ability to navigate social or commercial digital spaces 'incognito', and/or regular alerts to notify individuals when their data is being requested, used or gathered[2].

The importance, as one advocate of self-sovereignty in our Australian workshop argued, is not to consider sovereignty in its strictest sense, but to distinguish between the ways personal data is currently allowed to flow unhindered in the data-economy, and the ways that Digital IDs could change this: "Digital ID data will (need to) be removed from the data stream, in order to protect it from the 'open' ways in which the digital economy is developing." The way to achieve this is to allow individuals to be the gatekeepers of their personal data. At its simplest, this is an expression of the idea that the proofs of who we are, should not reside in the hands of those who can exploit, process (to their own ends), share and even lose them.

One other potential aspect of future Digital IDs that could see individuals empowered is the ability, during a digital transaction, not just to have control over the requests made by others, but also to make requests of our own. Just as others may want to verify that we are who we say we are, we may equally wish to verify that the other side of a transaction are who they say they are. There are huge benefits to this in terms of cybersecurity, with many standard phishing attacks, for example, being potentially rendered obsolete by such requests. Most criminals would likely be unable to prove that their nefarious digital properties (emails, websites etc.) actually are what they pretend to be, for instance.

At an everyday level too, there could be very practical benefits to this two-way exchange of identity. Imagine, for example, finding health advice online and being able to verify that an advice-giver really does have the associated medical training, as proven by their Digital ID; or confirming that a local plumber has the right certifications for the job in hand; or that someone you are speaking with is a person and not a robot. The list is potentially endless. Even in our relationships with bigger organisations and corporations, the ability to demand proofs could foment a wider cultural change. We may begin to demand and expect more transparency; first in terms of credentials perhaps, but later in terms of the longer-term uses of our behavioural data, and whether or not so much of our data is needed in order to deliver the service we are seeking.

Perhaps, the most important aspect of all the excitement around the concept of 'self-sovereignty', is not in whether or not a given implementation is practical or possible or 'true', but in its ability to provide a benchmark for Digital ID propositions. 'Sovereignty' could be seen as an idealised standard around individual agency and control against which new Digital ID innovations and technologies can be measured, alongside existing measures such as privacy, security and trust.

Digital rights and consent management

Up to now, we have largely discussed the role of Digital ID in terms of its ability to provide digital assurances during digital transactions, but there are other powerful things that a Digital ID in an interoperable system could do. Building on two ideas that we have already introduced - 1) that trusted systems of digital attribute sharing could mean that we need give far less information than is currently the case, and 2) that Digital IDs might be able to attach 'provenance notes' along with data or attributes - it is possible to imagine a future for Digital ID as a kind of digital rights manager and monitor. The easiest way to illustrate how this might change things is to compare against the way things often work today.

When we choose to access digital services today, we are often asked to create accounts. In fact, each account we create actually gives rise to a new digital identity. Accounts give us certain benefits, such as being able to store photos, or allow communications and connections with the service provider or other account holders, store transaction histories etc. Accounts are also of great benefit to service providers. They provide the ability to track individual user behaviours, and deliver more personalised services, or more targeted advertising.

In the case of the tech giants, this assigned identity (like the digital entities described in the opening chapter) means they can monitor our use of a whole eco-system of different services, triangulating data to create an ever deeper and richer picture of who we are. These deep and rich data sets in turn give those companies the power to explore new kinds of products and services, or even enter into and disrupt other industries. The more accurately we can be identified within digital spaces, and the more accurate the personal information associated with us is, the more valuable all of the vast amounts of associated data collection becomes. The question is whether the value exchange is truly transparent, whether we can weigh the future consequences of immediate decisions around sharing data and creating a digital identity and whether we have as much ongoing control over these new identities as we might want.

Often, if we want to access digital services, we have little choice but to agree to the terms and conditions that allow this invasion of our privacy and the creation of a digital identity on our behalf. And if the sign-up process also demands that we give certain stronger identifiers such as our phone number, we have little choice but to comply. Furthermore, having done these things, the conditions for a 'lock-in' situation in which we have invested so much into one service that it becomes more difficult to move out, or to another, are also created.

Digital ID has the potential to change this paradigm. In one simple scenario, we can imagine being given an option, during sign-up, to use our Digital ID instead of creating a user name and password (or whatever is being asked for). The service provider could then send an instruction to our Digital ID asking for certain identity attributes from within it in order to set up an account. At this point the Digital ID presents us with a series of options for using the service. Would we like to do so anonymously, without sharing any personally identifiable attributes, or only some? Or do we want to be clearly identified (perhaps in order to access or make best use of certain aspects of the services on offer)? Do we want the service to monitor, store and process our usage data or not? Do we want our data to be made available to other parts of the company's eco-system, or external partners? Would we like to move our data wholesale from this service to another? And so on, depending on the particular service being offered. It is worth remembering that even if we opted to remain relatively anonymous, the service provider would still be getting the advantages of confidence that they can strongly identify us as returning entities, due to the use of a Digital ID as a way of signing in.

At first blush this scenario seems unlikely. Why would service providers allow us to remain anonymous and have privacy options so clearly demarcated? What's in it for them? And, given what we know about current digital behaviours, wouldn't consumers simply opt for the most convenient options that give them access to the greatest number of services, foregoing, as ever, the option of greater privacy?

True, if we think about the larger data-driven service providers like Google and Facebook, there is little incentive for them to create such a scenario; but for competitors, smaller providers and start-ups, giving users the ability to transparently exercise data rights might be a very positive point of differentiation. Furthermore, even if larger service providers didn't want to allow user anonymity, they might still want to allow users to create accounts using their Digital IDs[31]. This would, at the very least, trigger a transparent process around the attributes being requested, requiring users to actively engage with, and give permissions around, their usage, rather than blindly clicking an 'I agree' button. In a world of interoperable Digital ID, in which we all carry familiar tools that enable us to make fast and convenient choices around the ways our data is collected, stored and used, the idea of hiding privacy erosions behind long pages of terms and conditions will likely become less and less acceptable. Ultimately, thanks to a Digital ID eco-system, choosing privacy, and/or providing truly informed consent, could become just as convenient as not doing so.

If the above scenario applies to the passive collection of our data, then along similar lines, we can also imagine scenarios for active personal data sharing. By using a Digital ID as the interlocuter in a process of sharing personal health data with insurance companies or healthcare providers, for example, it could become possible to attach not just provenance notes along with chunks of our data (as we discussed previously) but also a set of instructions or permissions determining how the data can be used, by whom, and for how long. In an even more complicated scenario (that some Digital ID providers are already working on) Digital IDs could even act as a gatekeeper to user-controlled and maintained personal data stores. Data processors could be allowed to access the data-store, or send algorithms inside them to carry out data-processing, but only under strict and explicit conditions, such as 'no removal of raw data', 'no use of personally identifiable information (PII)' or 'only time limited use of data', etc.

An early analogue of how this might all work can be found in the more detailed cookie-consent tools that have sprung up on websites since the arrival

CASE STUDY: Personal data stores and Digi.me / Solid

Putative ownership is a helpful tool for managing personal data even if an organisation you share with goes bust, or the relationship is suspended. The control that ownership gives you is helpful for managing misuse and fraud (i.e. it is in your hands, not in the hands of multiple others).

In the case of Digi.me for example, individuals receive a copy of their data after which they can then selectively grant data access to apps that they choose from the Digi.me ecosystem. Businesses and individuals within the Digi.me environment gain access to volumes of normalised data with the possibility of creating apps – such as consolidated management of all social media history in a single location, or access to, and processing of, personal health records.

Solid, a de-centralised web movement backed by Tim Berners-Lee is part of a growing effort to reinvent the web such that it can realise the goals imagined at its inception. One of the critical components of this reinvention is identity. Solid, includes a component whereby users are given the option to login with their Solid 'Pod', instead of a myriad of web logins, with various websites/organisations. Individuals are said to truly own the data in this pod and are provided with the tools to give permissions to entities and apps to read or write to subsets of it.

of GDPR, which allow granular and transparent permissions to be set regarding the placement of cookies on web browsers. These tools are cumbersome today of course, and likewise early implementations of digital rights and consent management within Digital IDs would also exhibit signs of over-complication. But it would be wrong to dismiss these wider potential roles of Digital ID as being pie in the sky. For one thing, already today the principle of using Digital ID to manage and exercise digital and data rights (at varying scales) is being adopted by a significant number of Digital ID stakeholders, with rallying calls especially focussed on the promise of providing greater privacy. Ever more sophisticated, and user-focused consent management tools are also already being developed in both the private and public sectors. In the longer-term we could see the development of new technologies (automated AI-driven, consent managers, for example), that make even exercising complicated data rights, a matter of convenience.

The immediate future is not likely to be a sudden change in the data economy paradigms of today, but about recognising the critical role of Digital ID in giving power back to individuals in an ever-evolving data infrastructure. Of course, this will require today's fast-moving inventors and entrepreneurs to think carefully about the tools they are creating. Ensuring that they will deliver on the promise. AI-driven Digital ID assistants or consent-managers for example, should not further erode individual agency

CASE STUDY: Digital consent management and Hu-manity.co

Digital consent management is the ability for entities to grant permissions with regard to use of their data. This issue has received greater awareness in recent times by the arrival of legislation like GDPR in Europe. A typical exchange when a first-time visitor visits a website for example, involves a pop-up window asking about use of their data with, say, advertising partners.

In some cases, users are given a 'pick list' where they can choose options on what data is shared with which partners. But outside of this system, vast volumes of inherent user data – driver and vehicle history, consumer spending habits, medical history, etc. - is gathered, bought and sold by various parties on a regular basis, without much in the way of meaningfully informed consent or transparency.

Consent management could be an important aspect of digital identity. Of particular interest to some is the ability to alter consent details over time and critically, to be able to 'walk away' and not be tied sharing data endlessly.

Hu-manity.co have built a mobile app, #My31, that gives users enhanced ability to control their data and to have a say in how it is used by others. They see users having ever greater awareness of how their data is being used and aim to meet a growing demand to be able to manage this. They see this as the '31st Human Right'. The core of the mission of Hu-manity.co is to ensure that individuals can claim, via #My31, that their data is respected as their legal property.

The result for users is that they can grant explicit consent to organisations on specific use of data, and enjoy a greater level of informed consent or privacy. Once a critical mass of users join the movement, Hu-manity.co claims that it will fight on behalf of users for reward /compensation opportunities with key industries, such as healthcare and insurance.

by allowing an all too *convenient* outsourcing of decision-making. But with due consideration (and there are many voices or parallels from other sectors[32] to help guide in this regard) Digital IDs and suites of Digital ID tools could change our digital futures for the better.

There is one final and different sense in which future Digital IDs are likely to act as rights managers. Most of the documents that we currently use to prove our identity today are actually primarily the means by which we can demonstrate various entitlements: a library card entitles us to access libraries and borrow books; a passport entitles us to travel freely across borders; and national ID (digital or otherwise) confers the rights associated with citizenship etc. The other attributes they contain are used to establish our identity; that we are indeed the holders of those entitlements. In the future, a single Digital ID might be able to do the job of identification for a number of different institutions, organisations in a number of different contexts, allowing us to combine the proofs of many different entitlements in a single place (or into a single tool).

In this way, much the same as a lack of access to legal identity documents today can hinder people's ability to access services, so too a lack of access to Digital ID in the future could become detrimental to a person's ability to get on in life. Ironically perhaps, whilst many of the access rights and entitlements that a Digital ID accumulates may never be considered fundamental rights on their own, the right of access to a Digital ID itself, could well become so[33]. Digital ID systems could come to be seen as being part of a society's critical infrastructure, with wide-ranging implications for the ways in which public, private and third sector Digital ID stakeholders are managed and regulated.

This normalisation and centralisation of Digital ID to society would have an impact on the day-to-day realities for Digital ID stakeholders. With an ever-growing user-base, inflating lists of attributes, and an emergent set of Digital ID rights, the future might not be one of constant user amazement at miraculous instant access to digitally delivered services, but rather the more mundane management of a growing set of issues around how access rights and entitlements are issued, revoked, restored and redressed in a Digital ID eco-system. Even today it is possible to see how messy some of these day-to-day issues are likely to become.

Theoretically a Digital ID could contain attributes gleaned from multiple sources, and even some which are extrapolations of other attributes. If so, where would responsibility lie for ensuring that each one is properly maintained? As one participant in our London workshop pointed out, with reference to a real-life case-study, such issues could become very tricky indeed. If someone, for example, demonstrates a repeated pattern of behaviour which involves abuse of their Digital ID and the attributes it contains, should they have their right of access to a Digital ID permanently revoked, or only parts of it? And what is the relationship between any actions taken in regard to their specific Digital ID, and other forms of ID (digital or otherwise)? Should records of whatever action is taken against them be kept in the ID itself, or removed elsewhere? And should such records be permanent or temporary? Would there be duties of disclosure and how could they be enforced? All of these issues will need to be thought about carefully in the rush to create new Digital ID products, in order to avoid the need for radical re-engineering down the line.

As a final addendum to the idea of digital rights and identities, we perhaps should also consider the right to be 'un-digital'? The arrival of Digital ID as a channel for individuals to express their desires to opt in or out of various digital exchanges and transactions, is likely to raise the idea of being allowed to opt-out completely. How this might be effected in a world of spreading sensors, mass data collection and biometric recognition is not clear today, but the need to serve those who wish to do so may come with a moral imperative if not yet a practical solution. Could Digital IDs become a mechanism for monitoring the erasure someone's wider digital identity?

The inclusion illusion

During our workshops there were varied and contradictory responses to the idea that the clearest need, and perhaps even earliest true Digital ID implementations, would be found in non-traditional markets for new technologies; namely, those who are most socially and economically disenfranchised. Roughly speaking, there were three types of responses to the case for 'digital inclusion':

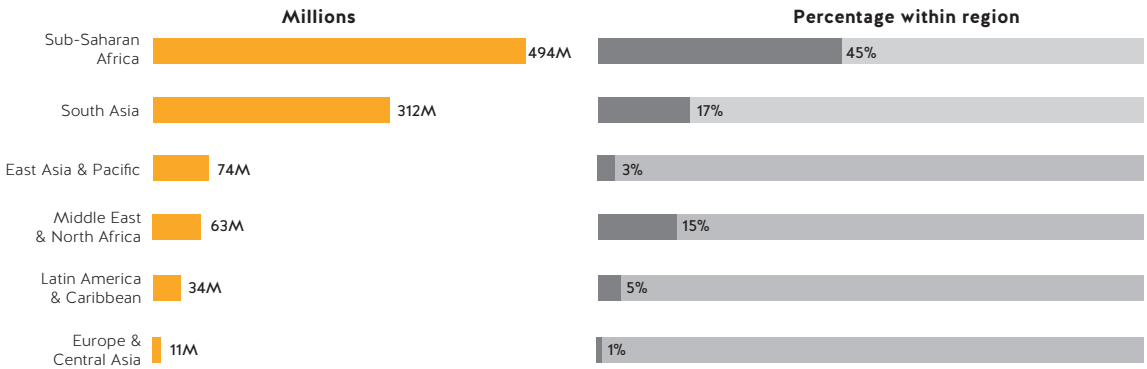
1. We should follow the UN's development goals in recognising that the vast movements and forced displacements of populations all around the world is creating a crisis in terms of legal identity. Those developing the future of Digital ID should make addressing the issue a high priority, since it is the most obvious area of consumer (or rather 'citizen') need.

2. Providing legal identity to the millions of people who currently lack access to legal identity services is important, but their needs are not enough to lead them to being among the first wave of Digital ID users.

3. Digital ID is a red herring in the issue of societal inclusion (or vice versa). Digital ID has long been touted as a solution to the identity access problem, without leading to any clear solutions. Access to Digital ID will ultimately follow on from conditions of greater social inclusion and equality of access, and the maturity of a Digital ID system to the point of being able to facilitate this, rather than the other way round.

There is validity to all of these positions. It is ultimately a question of emphasis. Is the future of Digital ID inclusion going to be most influenced by the technical and social difficulties of implementing robust enough Digital ID solutions for marginalised populations? Or is the future of Digital ID inclusion going to be primarily driven by the need to address an urgent societal problem[35]?

There are an estimated 1 billion people without an official proof of identity worldwide. Close to half of them live in Sub-Saharan Africa, where almost one in two people lack a form of ID



Source: ID4D-Findex Survey Data 2018[a]

[a] The report and data presents economy-level aggregates on the share and number of the population without a foundational/national ID, based on surveys covering over 100,000 people in 99 economies—representing 74 percent of the world's population.

There is perhaps another red herring hiding in this whole question however; in the language used to describe the socially disenfranchised. By referring to the idea of 'inclusion' or to the 'marginalised', or 'disenfranchised', we set up a false dichotomy between an idealised 'consumer' or 'citizen' on the one hand, and 'people in need of help to access' on the other. When it comes to Digital ID this is misleading in a number of ways. First, there is no a hard relationship between people's ability to access services and their need for them. In any society people have greater and lesser access to, and need for, different services, and are more and less engaged with existing digital services. Second, if we consider the populations of (even undocumented) migrants living outside of their home states, then in many cases we are talking about people who may have once had far more privileges than they do now. In fact, they may at one time, have enjoyed far more access to various opportunities and services than do parts of the population in the states they now find themselves in. This means that they should not necessarily be sharply distinguished from those more naturally considered the most natural markets for Digital ID. Third, if markets are at least in part about demand, then what matters might not be who is 'different' or which market segment is 'difficult to address' or who needs to be 'included', but rather where that market demand lies.

Whilst it is easy to think of situations in which a Digital ID would be useful, or more convenient, for many of us, it is harder to think of single use-cases that are 'vital', or that might require us to produce our Digital IDs frequently. Indeed, the more ambitious Digital ID stakeholders are seeking to circumvent this problem by solving for many use-cases at once. The situation and demand profile might be look different however, among those who rely on, say, government services to meet basic needs. We need not look to populations of undocumented migrants or displaced populations

CASE STUDY: Welfare delivery and UK Universal Credit

The UK's Universal Credit (UC) programme is one example of Digital ID assisting with welfare delivery. At its core UC aims to combine six welfare payments into one and in theory represents efficiencies in service delivery for both government departments as well as recipients.

The programme has however suffered from delays. Some of that rollout delay has been due to the attempted incorporation of a Digital ID. Issues – understandably perhaps - include users not always having access to key information or documents - such as a passport or driving licence or other photo identification - which can hamper their success when signing up to the digital system.

At the outset, Universal Credit used Verify, the UK Government's digital identity service, as an alternative for face-to-face identification, but only 1/3 of welfare applicants were successful in using that system. The Department for Work and Pensions (DWP) responded by creating an in-house verification system – "Prove your Identity". However even this only brought the digital user sign-up success rate to c. 50%.

alone to find those who *are* frequently asked to produce identity documents to unlock access to services today. They live everywhere. The illusion lies in the idea that 'inclusion' is only about those at the extremes.

In fact, it is this level of need amongst those who frequently use public services that is perhaps driving the development of government ID solutions around the world. The best example, for all its faults[36], is perhaps the "Aadhaar" ID system in India. The driving purposes and goals behind the development of Aadhaar were as diverse as described in the opening sections of this report, but the potential for the system to give efficient access to government services and enhance the delivery of welfare provisions by the state, were front and centre. Aadhaar may not present an ideal form of a Digital ID eco-system to many Digital ID technologists and stakeholders, but what it is, is a Digital ID system that has seen mass-adoption and usage[37]. Following Aadhaar's lead, it is perhaps no surprise that today, one of the first places to look for functioning Digital ID systems (if not interoperable systems) in any country, would be in their processes of welfare delivery.

Arguments over the need to focus on 'digital inclusion' aside, the longer-term impacts of Digital ID for disenfranchised populations are worth considering. If access to large-scale Digital ID eco-systems remained off the table for stateless, itinerant or marginalised people, then could smaller-scale initiatives temporarily fill that gap? Rudimentary Digital IDs that allowed people to verify themselves as 'returning customers' through the use of digital tokens, or Digital IDs with very few attributes that could be used to provide access to basic humanitarian services, for example, could see wide-spread adoption. This might in turn lead to increasing participation by larger ID providers, growing the legitimacy of such systems over time. This raises an intriguing prospect, particularly for stateless people, that the 'pseudo-citizenship of nowhere' that a Digital ID may itself provide, could come to be seen as the focal point for a new form of social identity, belonging and even organisation: formally ascribed 'stateless netizens' for instance (?).

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.

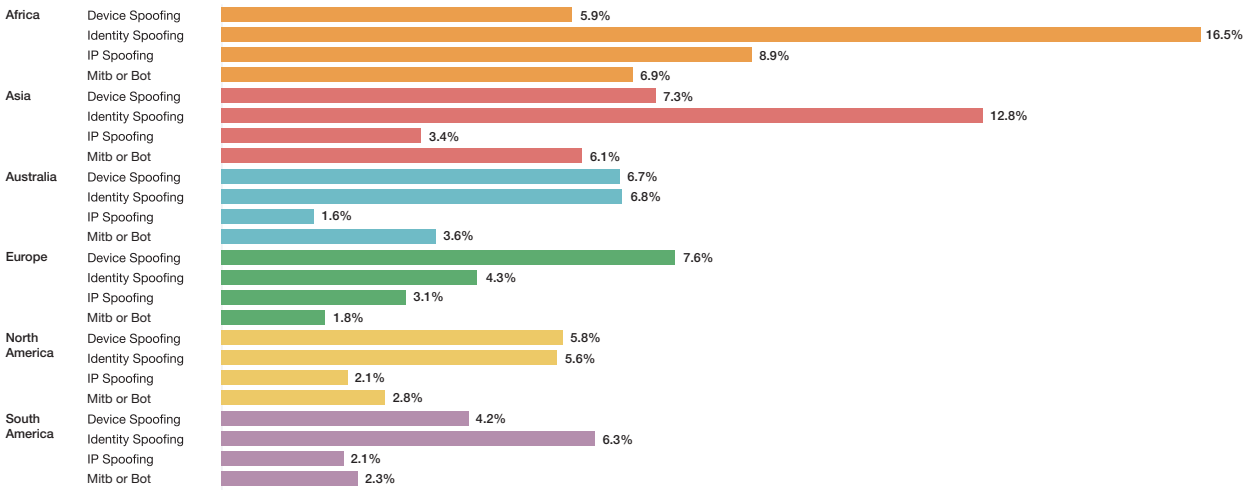
Encryption is a given, but there is more than one way to implement encrypted exchanges of information, and key decisions will need to be made over what is (and is not) kept 'secret', the precise moments within a process that encryption and decryption occur, which parties can and can't encrypt and decrypt, 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.

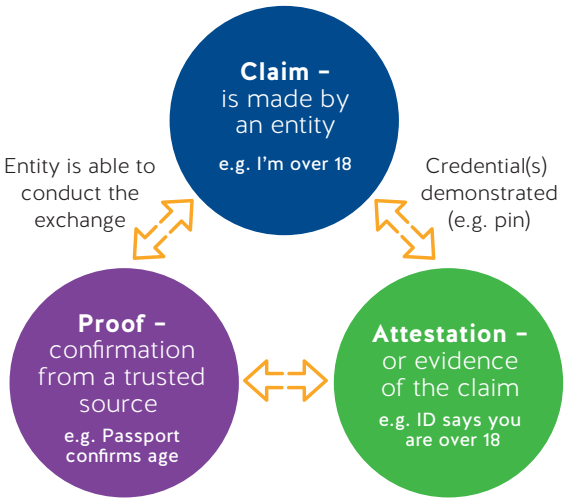
Conversely, more centralised Digital ID systems will aid the development of an interoperable and widely accepted eco-system (Aadhaar and even organisational identity systems provide cases in point). But they will require us to ask the question, assuming we have the choice, of which (few) institutions 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.

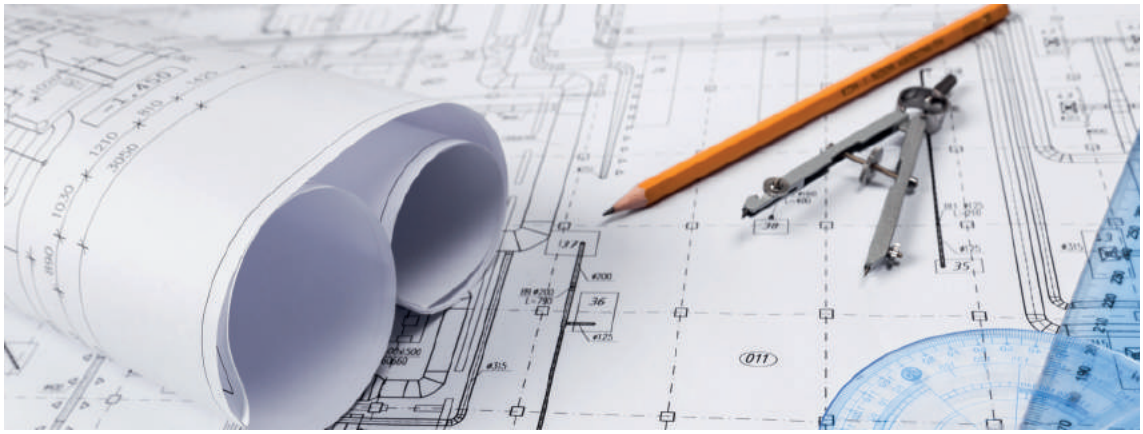
Or perhaps this is far too simplistic. Either way, there was one point of universal agreement around which the notion of privacy erosion was deemed to have gone too far, and the role of digital identity and Digital ID in it, was all too apparent: social scoring.

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.

Eco-system development

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



Development overview of digital identity

Microsoft Passport	Identity 1.0 – First stage Single Sign On (SSO) technology	c.1995
facebook	Identity 2.0 – Social identity used for logins	c.2010
PayPal	Identity 3.0 – Real identities mixed with virtual activity	c.2015
DIGIDENTITY	Identity 4.0 – Personal identity providers & ecosystems	c.2018

Multiple bets

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

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

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

*We intend absolutely no negative connotation to this term whatsoever

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Power and influence

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

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

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

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

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

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

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

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

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[66].

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[67], and have done since the days of the very first 'usenet[68]' forums; presenting different 'social selves' in different contexts, to achieve different aims[69]. 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[70]. 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[71]; 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

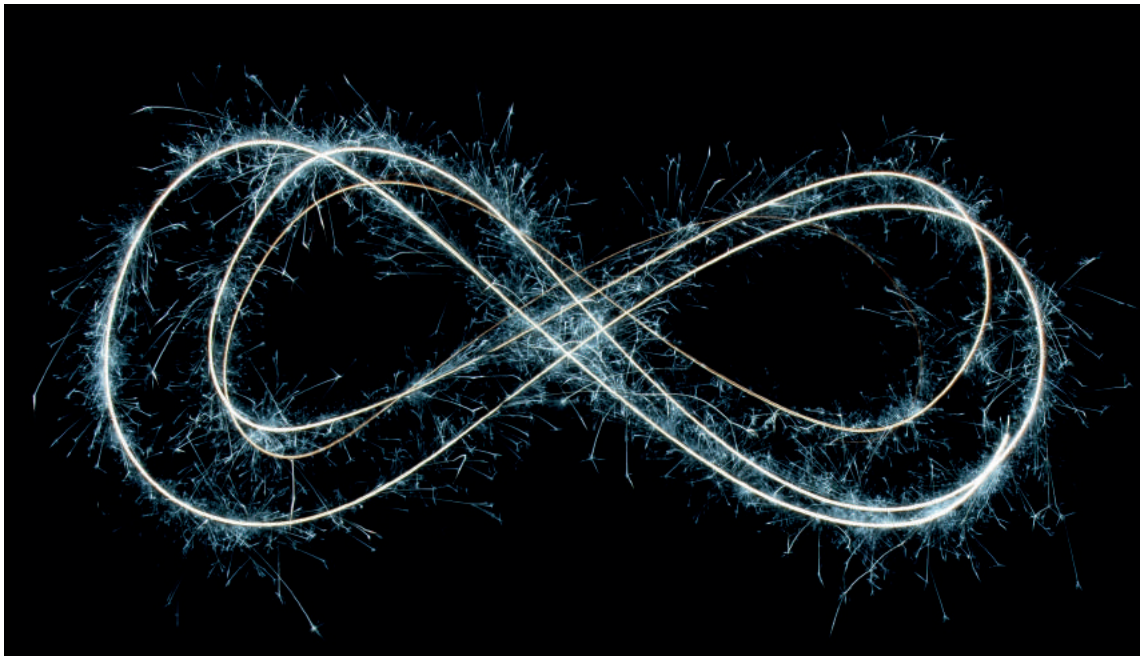
It is possible that the first immortal Digital ID already exists. This idea was suggested by a programme participant during one of our workshops. Although the comment was made with some incredulity, the thinking that led to it was sound. As Digital IDs become more and more comprehensive, becoming ever 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.

Unintended consequences

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

These included:

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

System vulnerabilities

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

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

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

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

Complete digital security should probably be seen as a permanent aspiration rather than a state that has ever been achieved, and, as we have already said, cyber-security is already in the DNA of most attempts to develop Digital ID systems. That said, the consequences of poor design of digital identity systems are already in evidence. Large-scale digital attribute stores, of exactly the kind that a centralised, interoperable Digital ID system might make use of, have been breached in recent years. Of those, some of the highest profile - such as the leaking of data from the Aadhaar system in India[75], the breach of the Comelec database in the Philippines[76], the hack of the Office of Personnel Management (OPM) in the US[77], the Equifax credit ratings agency data breach[78] and the personal data leaks and breaches at Facebook[79] and Google[80] - involve the very institutions that may be major stakeholders in future Digital ID systems. The long-term consequences of

even these breaches that have already taken place may never be fully quantifiable.

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

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

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

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

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

Identity victims

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

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

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

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

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

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

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

Conclusion

Digital identity is a complex idea, but that should not dissuade us from exploring its potential to transform our collective digital futures for the better. Even the immediate promise that interoperable Digital ID systems could allow us safe, secure and reliable passage through digital spaces and digital interactions and transactions is tantalising.

We are still in the early days of the human digital transformation and almost certainly do not yet have a grasp of how truly fundamental an understanding of digital identities will be to the future human experience. Digital ID, today understood as the slightly narrower aspect of digital identity related to the question of how we can prove that we *are who we say we are,* will likely become the primary mechanism through which we construct our digital selves and engage with and inhabit tomorrow's digital spaces. It could be the key to unlocking the true value behind "Big Data", providing unstructured data-sets with meaning and context, as well as providing the means by which we can all benefit from that. Similarly, the technologies and protocols associated with the development of Digital ID systems could become the pivot points for paradigmatic shifts in our digital society, rebalancing control over the data stream in favour of the individual, or opening us up to new mechanisms of social control.

We conclude with a summary of those areas of the Digital ID landscape and debate that are likely to provide the pivot-points for pathways toward the future. Given the number of different bets that are being placed, we cannot be sure if any (or even all) possible future realisations will come to pass, but we point to these crucial sites of decision as being the moments at which pathways will diverge. Digital ID stakeholders will make decisions related to them in different ways (including by omission), and for different reasons, but each will eventually have to confront the implications of them.

Collective purpose. For all the technical challenges behind the building of truly interoperable Digital ID systems, the challenge of defining their purpose will need to be met even earlier. The standards and protocols that emerge to allow the development of large-scale Digital ID eco-systems, will emerge thanks to their fitness to serve that purpose, so the need to tackle the question of exactly what it is, is urgent. Does Digital ID serve a mass-market consumer need around convenience? Is Digital ID necessary to unlock a wave of future digital innovation in financial and other services? Or is the primary purpose of Digital ID to rebalance the locus of power in a data-driven world? Is it the answer to societal exclusion? Or to the question of data ownership? Is it just a 'nice to have'? Can different stakeholders recognise a common purpose, or are they doomed to argue solely from within their niche?

Despite the fire and heat in much of today's current debates about implementation (centralised vs. decentralised, security and accountability vs. privacy, zero-knowledge principles and sovereignty etc.) the questions are most likely to be resolved by the resolutions made around this question of purpose. The loudest voices in the argument are likely to be consumers/users/citizens, commercial providers and governments. Their aims and goals today may not always coincide, and, in the case of end-users, may not yet be loud enough. Those stakeholders that are able to find a common thread between these competing interests, are likely to have the largest stake in defining and owning the future of Digital ID.

Agency and control. The precise mechanisms of agency and control that holders of Digital IDs come to have over their data, will matter. Small differences between different stakeholders' approaches to, for example, the collection of meta-data associated with Digital ID transactions, the implementations of consent management, the right to be forgotten, or to withdraw consent, the ability to travel in digital spaces incognito etc. may seem trivial today, but could have long-term consequences for the future of humanity. Different implementations have a number of different technical advantages and drawbacks today, but in the longer term, it is their effect on this aspect of Digital ID that is likely to matter most.

Flexibility and reversibility. Whether it be the need to incorporate a changing set of digital ethics and rights, the effects of unknown and unintended outcomes, the ways in which users adapt and innovate around the use of Digital IDs, or the impacts of devastating cyber-attacks; those Digital ID systems that are designed today to adapt to and accommodate change in the future, will likely prove the most resilient.

Collaboration. Truly interoperable Digital ID systems will require collaboration between different stakeholders from different sectors and cultural spheres. The strongest alliances and partnerships will be those that incorporate multiple different voices and in which the needs and achievements of one partner are recognised and understood by all.

The solutions we find to the difficult questions around Digital ID today could have far-reaching and long-term consequences that are difficult to envisage from where we stand now.

The Killer-App. Whilst the most obvious use-cases for Digital ID are easy to articulate ('a digital ID card'), a single 'killer app' that will drive investment into the development of a large-scale, interoperable Digital ID eco-system or mass user-adoption, is yet to be identified. Today there are still gaps perhaps in the understanding of how the various different capabilities of a Digital ID can meet genuine consumer, user and citizen need and demand. A single compelling use case may help to bridge this gap in a meaningful way, and could well provide a catalyst to collective action. It is worth remembering that Digital IDs can achieve multiple 'big' things all at once, from easing commercial transactions and enhancing digital security to providing transparency during data transactions; but the articulation of these benefits may need to be applied to more mundane and every day behaviours, or in small-scale, instantly recognisable user-rewards. As Digital ID moves ever closer to the boundary between being a technical challenge and a social one, the focus on the end user may need to be brought to the fore.

The solutions we find to the difficult questions around Digital ID today could have far-reaching and long-term consequences that are difficult to envisage from where we stand now; one foot still planted in an analogue world.

The key questions

Below we list some of the questions for society, regulators, stakeholders, and individuals in relation to the issues raised in this paper.

Some Key Questions for Digital ID Stakeholders:

Who are the other key digital identity stakeholders that can help enable our vision?

What role do we wish to play in the identity ecosystem?

How should we understand the purpose of Digital ID and how do we build to reflect that?

How does personal data mesh with machine data?

What is our ethical position regarding digital identity?

How can we contribute to the prevention of unintended and negative long-term consequences?

Some Key Questions for Individuals and Society:

How can my personal digital information facilitate my life?

How will I manage my digital attributes?

Who do I trust to help me do this?

Do I want my personal data to help society?

What are my digital rights and who protects them?

When do I want and need to be identified and when can I remain anonymous?

How can I better understand the role my data plays in a digital society and economy?

Some Key Questions for Industry:

In a world of Digital ID, will customers still want to share data with us?

How will we ensure that we are 'trustworthy'?

What data do we need to collect in the future?

How will we be able to comply when customers assert digital rights?

Can we develop new, privacy-preserving customer propositions?

What potential new products and services does widespread adoption of Digital ID unlock?

How can we benefit from increased cyber-security and better accountability in digital transactions?

Do we need to understand the impacts of Digital ID on our business models better?

Some Key Questions for Government and Regulators:

Would a government mandate around Digital ID help to accelerate the benefits of a secure and interoperable ID system?

How should we properly regulate Digital ID systems, and how can we ensure we create a dynamic and responsive regulatory environment for Digital ID going forward?

What kind of identity ecosystem do we wish to support?

What role will Government data about individuals play?

How can we ensure that digital identity benefits all of society?

How do we ensure that no citizen is excluded?

What steps must we take to prevent unintended consequences?

How can we think about the ethics of digital identity early?

How can access to and delivery of public services be improved by widespread adoption of Digital ID?

References

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] We clarify the use of different terms related to digital identity, such as 'Digital ID, in the next chapter.

[3] https://www.chathamhouse.org/chatham-house-rule

[4] https://www.libertyglobal.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf

[5] Ibid., p36

[6] The BCG report does in fact recognise the importance of the relationship between personal data and a real person, but sees it as largely being about a trade-off between consumer privacy and the ability of service providers to personalise (and therefore further monetise) their services.

[7] Or, as pointed out by one of our workshop participants, that it is the same person who has agreed to a set of terms and conditions when they first made an 'account'.

[8] Cf. "The Presentation of Self in Everyday Life" (Goffman, 1956)

[9] This somewhat innocuous and amusing news story, shows how a failure in passport authentication led an airline to make a robust public defence of its entire approach to security and safety: https://www.independent.co.uk/travel/news-and-advice/klm-flight-airline-passport-friend-prague-amsterdam-newcastle-airport-security-a8789481.html Digital ID of course, should make situations like this a thing of the past.

[10] https://en.wikipedia.org/wiki/Know_your_customer

[11] https://worldpaymentsreport.com/

[12] http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[13] https://sustainabledevelopment.un.org/sdg16 Target 16.9 "By 2030, provide legal identity for all, including birth registration"

[14] http://www.undp.org/content/undp/en/home/blog/2017/6/1/Moving-towards-digital-technology-for-legal-identity.html

[15] https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf

[16] To give an idea of the scale of the problem, at the time of writing, cyber-security blogger Troy Hunt's https://haveibeenpwned.com/ project currently hosts details of at least 6,931,949,148 individual identity credential thefts. The number will be higher at the time of reading.

[17] For more detail see https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market investigation-full-final-report.pdf

[18] For a more detailed discussion of the concept of interoperability in relation to Digital ID, see https://cyber.harvard.edu interop/pdfs/interop-digital-id.pdf

[19] http://www.undp.org/content/undp/en/home/blog/2017/6/1/Moving-towards-digital-technology-for-legal-identity.html

[20] This report from Caribou Digital produced in partnership with the Omidyar Network illustrates the complexity of the Digital ID marketplace in 2016. The landscape has only become more complicated since: http://cariboudigital.net/new/wp-content/uploads/2016/08/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf "Private Sector Digital Identity In Emerging Markets" (Caribou Digital Publishing, 2016)

[21] We fully accept that many of the concepts we introduce deserve deeper consideration.

[22] We have deliberately included attributes that might be more or less socially contentious to illustrate that the term 'attribute' itself is neutral as to what they might consist of.

[23] The idea is expanded on here https://medium.com/mydex/unleashing-the-potential-of-verified-attributes-fe001e01b091 "While all individuals and almost all organisations would benefit greatly if a wide range of verified attributes were available for quick, easy, safe sharing and checking there is no immediate particular benefit to any single attribute provider to incur the costs of providing citizens/customers with these verified attributes about themselves."

[24] Specifically, we explore potential user benefits with regard to personal cyber-security, privacy and the ability to exercise more control over the flow of personal data, even the ability to exercise 'data rights', later in the report.

[25] http://cariboudigital.net/new/wp-content/uploads/2016/08/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf (2016)

[26] https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051

[27] For an example of the kinds of ambitions around identity and self-sovereignty see for example https://medium.com/lifeid/lifeid-self-sovereign-identity-bill-of-rights-d2acafa1de8b

[28] Here we are in danger of being too casual with philosophical, anthropological and social-psychological theories of 'self'. In the interests of brevity and readability we have made the decision to simply assert that the purpose of Digital ID and also the broader idea of 'identity' itself, are fundamentally social constructs and concepts. For further references it may be worth starting here https://en.wikipedia.org/wiki/Intersubjectivity

[29] For a fuller and more technical discussion of all that we have introduced here see https://bitsonblocks.net/2017/05/17 gentle-introduction-self-sovereign-identity/ and "The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them" (Lewis, 2018)

[30] In the next section, we take this a step further to explore how future Digital ID implementations could move on to become fully-fledged consent and privacy managers

[31] One point worth remembering here is that use of a Digital ID, thanks to the greater privacy afforded by the translation of personal attributes into anonymised entitlements, greatly reduces the number of sensitive personal data points that organisations need to store and maintain, reducing liabilities under laws and regulations such as those laid out in the EU's GDPR.

[32] Consider for example the efforts being made around the ethical development of AI at places like Oxford University https://www.cs.ox.ac.uk/efai/ or the Ada Lovelace institute https://www.adalovelaceinstitute.or/

[33] Arguments are already being made in this regard. For a clearer articulation of the arguments, see for example: "Digital Citizenship and the Right to Digital Identity Under International Law" (Sullivan, 2015) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2519806

[34] The report and data presents economy-level aggregates on the share and number of the population without a foundational/national ID, based on surveys covering over 100,000 people in 99 economies—representing 74 percent of the world's population.

[35] With the emergence perhaps, at least in the short term, of different kinds of Digital ID attribute collection and verification based on for example, the corroboration of peers, behavioural data and even self-assertion (up to a point).

[36] https://www.eff.org/deeplinks/2018/02/can-indias-aadhaar-biometric-identity-program-be-fixed

[37] See here for a longer version of this argument https://hbr.org/2017/11/how-india-is-moving-toward-a-digital-first economy

[38] See for example the argument over blinding being made here https://diacc.ca/wp-content/uploads/2017/02/Consumer-Digital-Identity-Companion-Paper.pdf or the kinds of claims and promises being made here https://spideroak.com/no-knowledge/

[39] We do recognise that there are also genuine attempts to develop the use of ZKPs in Digital ID protocols, see for example https://www.itu.int/dms_pub/itu-t/oth/06/04/T06040040040001PDFE.pdf and https://digify.com/a/#/view/55d40168f67c4676bed9e49ed99832fc

[40] ThreatMatrix, Q2 2018 Cybercrime Report and is based on actual cybercrime attacks from April – June 2018.

[41] We recognise that 'digital identities' and 'digital identity' technologies have always been on the front line of cyber security, criminality and attack, but here we are specifically referring to emergent forms of digital identity, i.e. 'Digital IDs', as becoming a new frontline.

[42] We refer to this example later in the report but it is worth mentioning here. As the cyber-security writer Bruce Schneier put it after the theft of biometrics in the OPM data breach: *"…many systems don't store the biometric data at all, only a mathematical function of the data that can be used for authentication but can't be used to reconstruct the actual biometric. Unfortunately, OPM stored copies of actual fingerprints."*

[43] For examples see https://en.wikipedia.org/wiki/EIDAS or https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY standards could also emerge from de facto commercially driven identity systems

[44] See for example https://www.dataversity.net/rwdg-slides-three-approaches-data-stewardship/

[45] See for example https://cordis.europa.eu/project/rcn/88243/reporting/en

[46] AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds and Machines (2018) 28:689–707; November 2018. In the paper, the authors cite the four bio-ethic principles of Beneficence, Non-maleficence, Autonomy and Justice as representative of a range of recommended AI ethics from other sources and then add the fifth principle of Explicability.

[47] http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

[48] https://en.unesco.org/news/unesco-panel-experts-calls-ban-editing-human-dna-avoid-unethical-tampering-hereditary traits

[48] https://id2020.org/

[50] https://www.omidyar.com/blog/launching-good-id-dialogues

[51] https://www.eff.org/

[52] https://theodi.org/article/exploring-good-common-principles-for-a-digital-identity-system/

[53] https://www.internetsociety.org/issues/identity/

[54] The old adage that 'if the service is free then you are the product'.

[55] https://en.wikipedia.org/wiki/Social_Credit_System

[56] See for example, https://securekey.com/wp-content/uploads/2017/07/SecureKey_Whitepaper_Telecom_FINAL Feb2018.pdf

[57] https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf

[58] https://www.gemalto.com/govt/identity/5-reasons-electronic-national-id-card

[59] https://id4d.worldbank.org/

[60] https://www.omidyar.com/our-work/digital-identity

[61] https://fidoalliance.org/

[62] https://ipfs.io/

[63] https://www.inrupt.com/

[64] There is some surprisingly early precedent for this in the form of European driving licenses https://europa.eu/youreurope/citizens/vehicles/driving-licence/driving-licence-recognition-validity/index_en.htm and the APEC business travel card https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Business-Mobility-Group/ABTC

[65] See for example https://factordaily.com/aadhaar-india-stack-export/

[66] As in non-digital spaces, this will only ever be a 'measure' of control. We would be unlikely to have full control of the ways in which we are understood in digital spaces, just as we do not have full control over others' perceptions of us in the offline world.

[67] For a journalistic account, see https://www.engadget.com/2016/03/04/multiple-online-identities/

[68] https://en.wikipedia.org/wiki/Usenet

[69] Interestingly, the idea of a digital or internet 'sockpuppet', a deliberately false identity used to manipulate discussions, were also among the earliest forms of digital identity https://en.wikipedia.org/wiki/Sockpuppet_(Internet)

[70] These need not be physically close communities such as neighbourhoods or villages. It could include 'communities of interest' that are 'local' in the sense of being self-contained.

[71] An analogy here might the way in which former employers provide personal references for job-seekers. Whilst general characteristics are always sought by prospective new employers, a reference from a similar employer, in an industry they know well, is likely to have more meaning. The 'further away' the industry supplying the reference is to the new employer's industry, the less meaningful and therefore 'trustworthy' as a verification of the job-seeker's skills it becomes.

[72] The World Economics Forum's "Global Risks Report 2019" outlines these scenarios in more detail and suggests that large-scale data crime and cyber-attack are among the more likely risk scenarios https://www.zurich com/_/media/dbe/corporate/knowledge/docs/the-global-risks-report-2019-executive-summarypdf?la=en&hash=6B7B 3A8BAC42C7DA05C33D7B914D46256D17B00

[73] "Dawn of the Code War" (Carlin, 2018)

[74] https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/

[75] https://www.hindustantimes.com/tech/aadhaar-breach-everything-you-need-to-know/story-VhCKHDIL8lziw6OcnhL4wO html

[76] https://en.wikipedia.org/wiki/Commission_on_Elections_data_breach

[77] https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

[78] https://en.wikipedia.org/wiki/Equifax

[79] https://newsroom.fb.com/news/2018/09/security-update/

[80] https://www.blog.google/technology/safety-security/project-strobe/

[81] https://www.schneier.com/essays/archives/2015/09/stealing_fingerprint.html

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