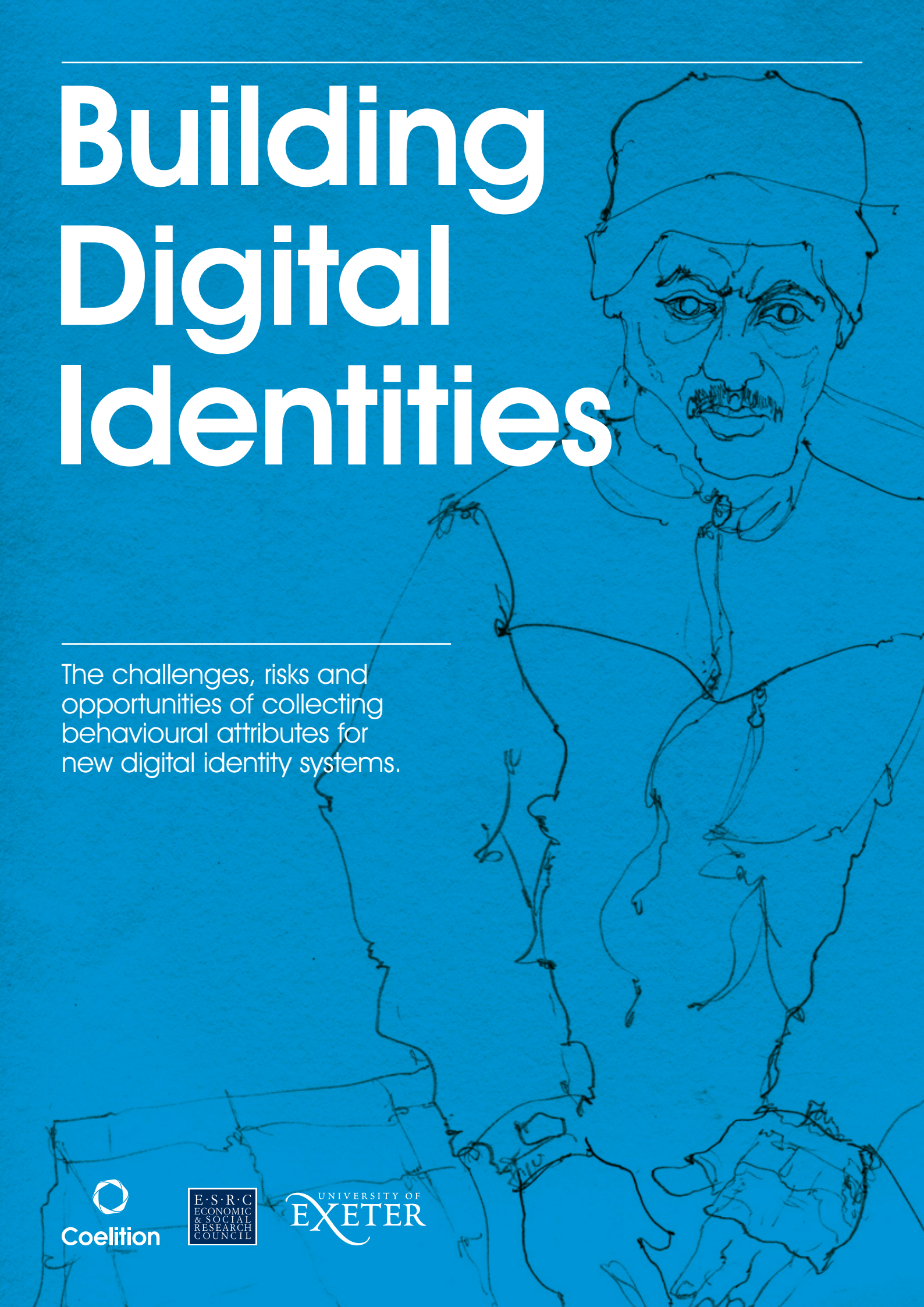
# Building Digital Identities



The challenges, risks and opportunities of collecting behavioural attributes for new digital identity systems.

Coelition

E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL

UNIVERSITY OF EXETER

# Executive Summary

**Ana Beduschi**
(University of Exeter)

**Jonathan Cinnamon**
(University of Exeter)

**Joss Langford**
(Coelition)

**Chunbo Luo**
(University of Exeter)

**David Owen**
(Gurukula Ltd.)

© University of Exeter & Coelition 2017. All rights reserved.

# Executive Summary

The provision of legal identity for all is increasingly viewed as a key mechanism for driving development goals. Behavioural attributes produced through digital interactions may have significant potential for enabling access to a legal identity for all, however the social, legal, and technical affordances and implications remain under-explored.

In the developing world investment in identity systems is growing exponentially, however successfully implemented systems may still fail to address the needs of the most marginalised in society, and in some instances further marginalise vulnerable communities, destroying informal economies of exchange and support whilst simultaneously excluding them from the newly developed formal mechanisms based on more robust identity systems.

This report brings together leading researchers across the legal and social sciences, alongside technical and commercial specialists to explore the challenges and the opportunities for the digital collection of behavioural attributes for new and emerging digital identity systems. We provide a unique and wide view to the problem area, and unpack the role of behavioural attributes within the existing legal, social and technical landscape.

## Key Findings

- There is a clear role for behavioural identifiers to sit alongside existing identity systems and provide new lines of data that can be used for verification.
- Behavioural identifiers can help provide a more prominent focus on person centred engagement as part of an approach to developing digital identity systems based on societal norms and expectations.
- The 1.5 billion people without legal identity cannot be viewed as a homogeneous group. It is imperative to distinguish between the different groups that exist (i.e. refugees, migrants, rural communities) and design systems for and with them, ensuring there is a role for users within the governance of these systems.
- We need a clearer understanding of how key legal frameworks at international, regional may evolve in relation to new technologies. Furthermore, whilst we know that international standards, norms and agreements can play a crucial role within the digital identity landscape, we need to better understand their influence at a domestic level.
- Corporate organisations continue to play an important role in both driving and restraining innovation in this sector. We need to invest in effective partnership work and the development of interoperability standards. We need a better understanding of the role of effective regulation and how to harness innovation for identity systems.
- Finally, the technologies that support digital identity systems are evolving rapidly. Adoption of these technologies are fluid and complex. Both private and public actors require intelligence in order to anticipate how digital infrastructure might evolve in the next five to ten years. Failure to do so, may lead to ineffective of identity systems which may prove costly for both social and economic aims.

# About this report

On the 8 February 2017, University of Exeter and Coelition with funding from the UK Economic and Social Research Council (ESRC) convened a workshop entitled Building Digital Identities. The workshop aimed to bring together and mobilise leading researchers across the legal and social sciences, alongside technical and commercial specialists to explore the challenges and the opportunities for the digital collection of behavioural attributes for new digital identity systems. This cross-sector and cross-disciplinary approach has brought a unique and wide view to the problem area.

The report draws on the discussions and themes arising from the workshop, alongside existing research to scope and anticipate key priorities for research and action. After an introduction the report is structured around three key sections:

1. **Dynamics of legal identity:** What is legal identity? What legal frameworks exist both nationally and internationally to define identity? How might these enable or constrain the use of behavioural attributes for identity provision?

2. **Implementation environment:** What are the conditions required for successful implementation of identity systems? What are the different roles that public or private sectors can play? How might we learn from failure?

3. **Infrastructures, scientific and technological innovations:** How are behavioural attributes being used to verify identity? What are the key frameworks required to ensure privacy, dignity and trust? What are the key scientific innovations?

Based on findings from the workshop and supplementary review of the literature we propose five key areas for further research and action.

- Person-centred design
- Legal and regulatory frameworks
- Public, private and person partnerships
- Social and ethical considerations
- Technology and innovation

# Introduction

# Introduction

A universal aspect of every human being is that we each have a distinct and unique identity. Our internal experience of identity and the expression of this identity are both multifaceted.

**Identities change with context and life stage, resulting in a range of personas and profiles that we actively manage. This composite identity creates and defines our role in society. In our interactions with society we are often required to verify who we are, and this is done in three main ways:**

- Firstly, the most common mechanism is through verifying facts about who we are, such as date and place of birth, gender, where we live and work;
- Secondly through distinguishing biological features including how we look, such as eye colour, hair, face, fingerprints and other biometric data such as DNA; and
- Finally, through the social and economic context of how we live and who we live with, for example where we have been, significant life events and daily routines. These form the basis for identity in everyday life. These are often the records that are captured within digital environments and include for example: browsing the web, making and receiving phone calls, making and receiving payments, borrowing a book, using a gym, buying a product or service, paying a subscription, attending an event etc.

Identity is the basis for autonomy and self-determination (Mas and Porteous, 2015); the capacity to verify one's identity is therefore of vital importance for accessing rights, benefits and services be these financial, health related or educational (ID4D, 2016; Gelb and Clark, 2013). However whilst some people may own multiple passports, addresses and have various means to identify aspects of themselves, others may be undocumented, which may in turn entail being denied opportunities and possibilities to exercise civil and social rights.

For example, in Kenya as in many countries, identity cards are required to receive hospital care, to attend university, to vote, to marry, to obtain a passport and many other basic services (Oppenheim and Powell, 2015).

Identity provision is increasingly advocated for as a public good and linked to human rights and development agendas (Atick et al, 2016; World Bank Group/GSMA, 2016). The inclusion of legal identity for all by 2030 in the UN Sustainable Development Goal (SDG) 16.9, is one example of how this is being put into practice.

## UN Sustainable Development Goal 16

Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

Target 16.9: By 2030, provide legal identity for all, including birth registration

Indicator: Proportion of children under 5 years of age whose births have been registered with a civil authority, by age

**UN SDG 16.9**

# Introduction

The benefits of identity systems for national development have also been documented. Szreter (2006) argues that identity registration in 16th Century England was a factor in enabling that country to advance more rapidly than others through its ability to empower citizens and communities. Despite the benefits to individuals, communities, and states, there are currently an estimated 1.5 billion people living without the means to verify who they are (ID4D, 2016).

The discussions at the workshop and subsequent desk research uncovered very little intelligence (beyond case studies) about who these 1.5 billion people are, although localised detailed studies exist (Harbitz, 2009). It is evident from the case studies that this will not be a homogeneous group and that different cultural contexts, gender, histories, political and social contexts will influence not only behaviour, but also agency, dignity and vulnerability in relation to identity provision (Oppenheim and Powell, 2015, Caribou Digital, forthcoming). The World Bank Group suggests that children and women from poor rural areas in Africa and Asia make up the majority of this group (WBG/GSMA, 2016). A recent report by the newly established ID2020 agency goes further to provide illustrative examples including children and young people in Malawi, refugees who cannot receive or request authentication from their governments, people stripped of their identity documents as a result of human trafficking (ID2020, 2017). The examples work well to show not only the diversity of the people without identity, but also the range of contexts and implications.

Identity provision is also associated with risks and social harms, which need to be better understood. Research has shown that the benefits of legal identity are uneven; indeed some individuals and groups have been negatively affected by gaining a legal identity (Arora, 2016; Gelb and Clark, 2013; ID2020, 2017; Oppenheim and Powell, 2015; Caribou Digital, forthcoming).

For populations whose lawful status entitles them to financial, social and political participation it follows that verifiable identity will provide greater access to social and educational resources, however, many groups face discriminatory practices and exclusion based on their identity. The Rwandese Genocide in 1994 in which an estimated 800,000 were killed on the basis of their identity is one extreme example (Prevent Genocide International, 2015). However, other examples exist, in Malawi, it is estimated that 20-60% of individuals receiving free health services are not Malawian (ID2020, 2017).

Whilst a more effective identity system may help target health care provision for nationals and legal residents and lift the current strain on the system - the number of people needing health care will not decline. Undoubtedly some people will stand to benefit, others will lose. The provision of legal identity systems can also create new barriers and challenges to inclusion. For example, the use of fingerprinting in biometric identity systems may not be accessible to all excluding elderly, infants or labourers if suitable alternative routes are not in place (Gelb and Clark, 2013). For those that do get enrolled in biometric and other types of registration systems, the history of these technologies demonstrates that their use is associated with both benefits to individuals as well as an increased ability of the state to control populations and restrict autonomy and freedom (Breckenridge, 2014).

Finally, the use of identity systems may destroy informal economies, where individuals habitually resident in a country were generally assumed to be citizens, the introduction of identity cards meant that those without documentation were more frequently treated as, non-citizens (Brewer et al. 2015). How legal identity is defined is also crucial here. The current measure for SDG 16.9 is birth registration, yet studies have shown that in many countries this is not the core document needed to establish citizenship and access services (Oppenheim and Powell, 2015, ITU-T, 2016), whilst it has also been shown that the link between birth registration and outcomes associated with development and political participation varies widely across countries (Oppenheim and Powell, 2015).

# Introduction

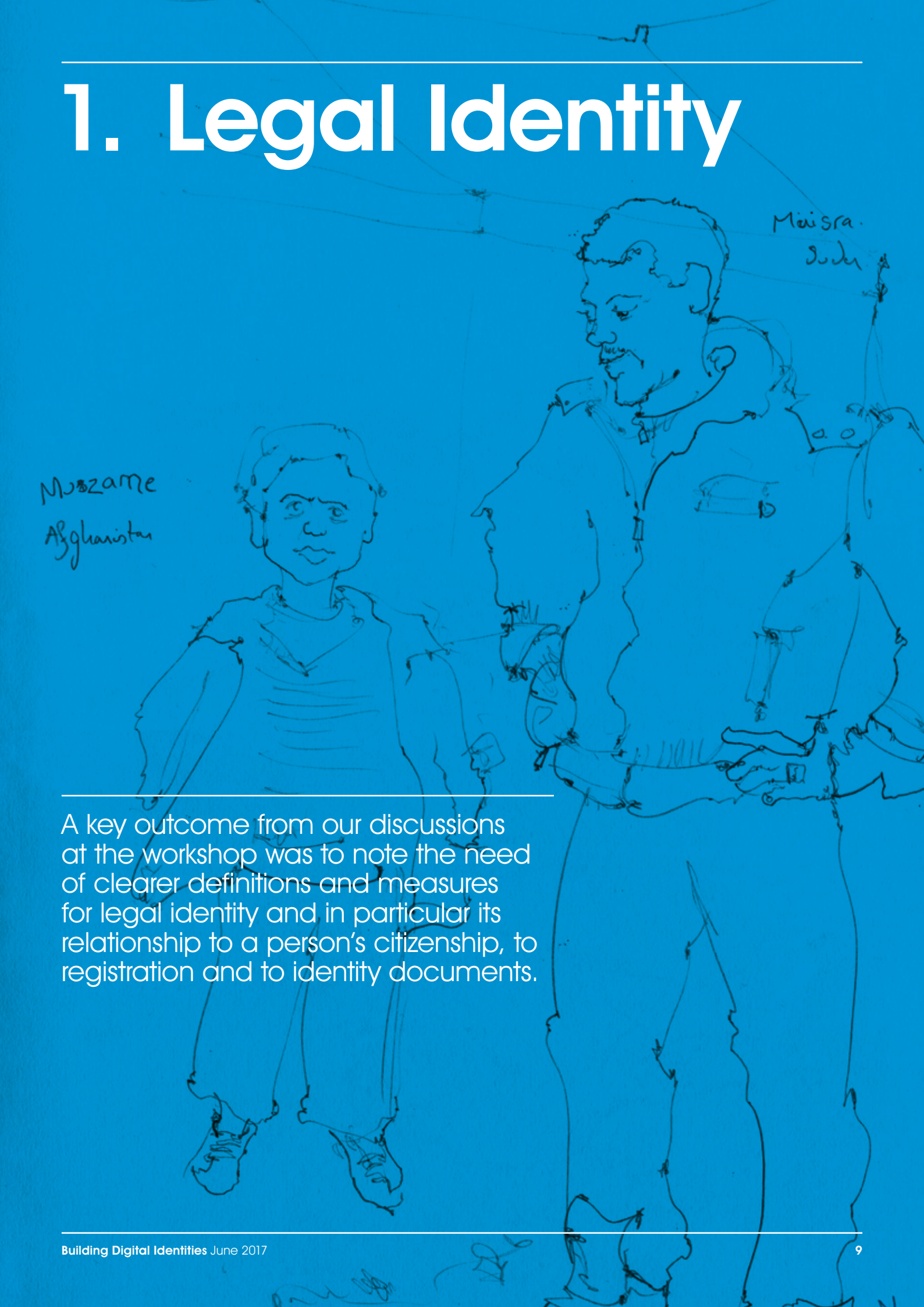
In the developing world, biometric technologies have become increasingly prevalent (Breckenridge, 2014) fuelled by an alliance of states, intergovernmental organisations and transnational corporations – what Lyon and Topak (2013, 28) referred to as the "oligopolies of the means of official identification". Gelb & Clark (2013) found that the industry grew at 34 percent annually between 2005 and 2010. These new innovations are rapidly opening new possibilities for governments to develop comprehensive systems that have the potential to reduce costs and human error as well as increase administrative efficiency (World Bank Group, 2016 ITU-T, 2016). However these approaches to identity registration, largely based on biometric and verifiable facts, are costly and require a level of infrastructural support not available in many settings.

As of yet the potential of using digital behavioural attributes, (i.e. how we live and who we live with, daily routines) for verifying legal identity is not currently realised. Across the world, digital technologies are becoming increasingly integrated into our daily lives. Through many of our basic interactions, such as using a phone to talk or send SMS messages we are interacting with a connected infrastructure. We now frequently talk to and share news with peers and professionals through social networks, we access financial and social services, we purchase and consume a wide variety of media and products, and we measure and record aspects of our lives for example through health related apps. This use of digital technologies and associated infrastructures is producing personal data on an unprecedented scale; whilst this data has traditionally been conceptualized as a by-product of system functions – e.g. 'digital exhaust' – it is becoming an increasingly significant aspect of value generation in digital platforms, and therefore a core motivation for their development (Zuboff, 2016). Our interactions in the digital world, alongside an increasingly sophisticated set of tools to analyse personal behavioural data, are beginning to tell a story about us, about who we are, what we do, what we believe and value. They effectively work towards building a stratified layer or history of identity evidence that can be used for verification.

In countries with a comprehensive digital infrastructure, these attributes tend to sit alongside existing identifiers (e.g. home address, phone number, date of birth) to improve security and convenience. However, in developing countries, traditional identifiers may not be as widely available: births are not all registered, the location of home may be transient or unofficial and access to communications technology might be on a community rather than on an individual basis. In this context, behavioural attributes captured with digital technologies may play a profound role. They have the potential to provide new lines of data that may enable individuals to assert their identity in new ways. While some parts of the world remain digitally excluded, access to and use of digital technology is starting to increase in many less-developed countries. The rapid, recent expansion of mobile networks around the world is linking rural, remote, and low-resource settings with more urban and developed parts of the world. As usage rates grow in these settings and across the social spectrum, mobile phones in particular may be a particularly valuable platform for producing personal behavioural data for use in digital identity systems.

However, significant gaps remain in our knowledge about the potential of behavioural data for identity systems. Care must also be taken to minimize the negative impacts to individuals and wider society that identity systems can sometimes engender. Moreover, serious social harms are increasingly being documented in behavioural data mining and personal data analytics more broadly (Barocas and Selbst, 2016; Boyd and Crawford, 2012; Pasquale, 2015; Zuboff, 2015). Notably, the concentration of power in the hands of the corporate digital platforms in which behavioural data are produced and controlled – e.g. Google and Facebook – and their connections to governmental surveillance, security, and intelligence operations (Lyon 2014; Ball & Snider, 2013; Murakami Wood, 2013) should be of concern to any efforts designed to leverage personal data to demonstrate identity. This report thus approaches the issue cautiously, towards a more detailed understanding of the opportunities and risks of building digital identities based on behavioural attributes.

# 1. Legal Identity




A key outcome from our discussions at the workshop was to note the need of clearer definitions and measures for legal identity and in particular its relationship to a person's citizenship, to registration and to identity documents.

# 1. Legal Identity

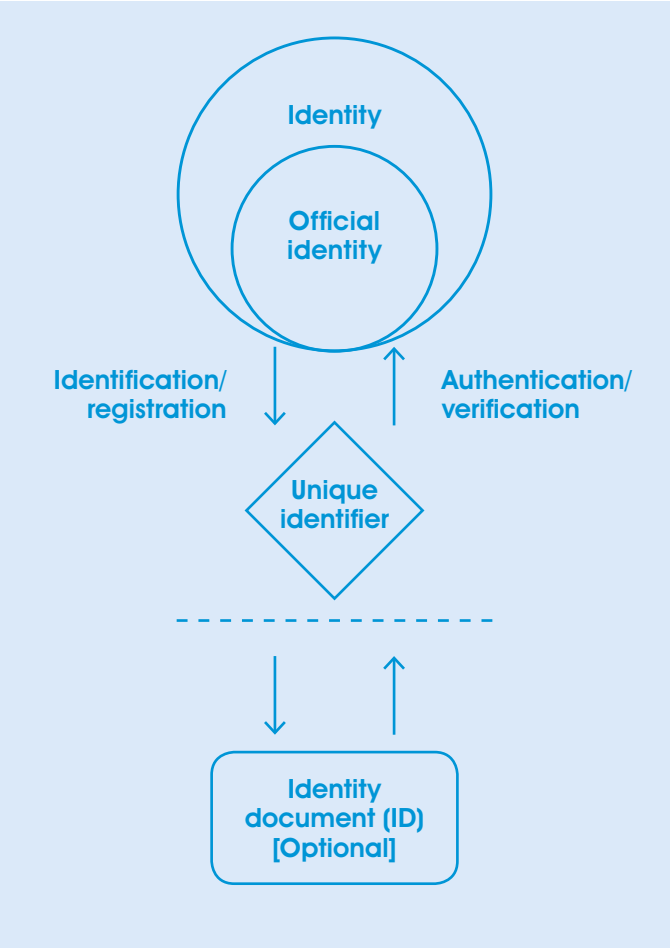
One definition for legal identity put forward by UNHCR, UNICEF, UNDP and Plan International was 'the recognition of a person's existence before the law, facilitating the realisation of specific rights and corresponding duties' (Lopez et al., 2014). This interpretation places legal identity firmly within human rights law where it is conceived as a status, that of being human. In human rights law, everyone has the right to be recognised as a person before the law (article 6, Universal Declaration of Human Rights -UDHR; article 16, International Covenant on Civil and Political Rights -ICCPR) and with this comes the right to be equality treated before the law (article 7 UDHR; article 26, ICCPR) and the principle of dignity. Perhaps the most widely used and referenced international instrument is the Universal Declaration of Human Rights, which states that all human beings are born free and equal in dignity and rights (article 1, UDHR) without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status (article 2, UDHR). It goes on to say that 'no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs' (article 2, UDHR).

Human rights law seeks to identify the humanity that we each have. Marshall (2014) argues that human dignity is a central characteristic of our identity in human rights law, as when a human being acts in a way that harms human dignity it is said to be inhuman. She points to our unique capacity as human beings to reflect on our existence and the existence of others, to perceive injustice, to pursue cooperation and to act in ways that are responsible and give expression to ethical principles (Marshall, 2014). Although there is no common judicial interpretation of human dignity, McCrudden (2008) identifies three elements, which are helpful for our framing. The first is that human beings possess an intrinsic worth, merely by being human; the second is that this intrinsic worth should be recognised and respected by others and the third concerns the relationship between the individual and the state, in that the state exists to serve the intrinsic value of the individual and not the other way around (Marshall, 2014).

Whereas human rights law is concerned largely with the relationship between the state and individuals, the past fifty years of development has seen the emergence of supra-national bodies, the European Union being amongst the most well-known examples, whereby elements of state sovereignty in ceded to the larger body. Examples in the identity space include the recent EU framework for identity management (Milieu Limited, 2016). Furthermore, there is a growing role for non-state actors including International organisations (i.e. United Nations) and large commercial corporations (i.e. Google, Apple, Amazon, Facebook). Whilst these actors do not have the authority to produce hard laws, they have the capacities to play a role in producing norms, and wield a significant amount of influence in generating, navigating and upholding guiding principles with regards to identity verification and provision. For example, in one ongoing case the Pakistani government has requested Facebook's assistance in implementing the state's law with regards to blasphemy. The details of the request are not clear; however, it has been widely reported that it may include help from Facebook in identifying individuals who post content, alongside censorship (BBC, 2017; Hashim, 2017).

# 1. Legal Identity

Increasingly and certainly with the provision of identity cards, recognition of our humanity is obtained through acts of registration and verification by the state. Rights are granted, distributed or withheld depending on credentials and ability to prove them. This perspective is adopted within the definitions used by the Inter-American Development Bank and other agencies, where legal identity is a 'legal civil status obtained through birth registration and civil identification that recognises the individual as a subject of law and protection of the state" (Harbitz and Molina, 2010). Costas Douzinas (2007, p.54) observes the challenge in human rights is the 'ongoing and always failing struggle to close the gap between the abstract man and the concrete citizen'; closing this gap involves adding 'flesh, blood and sex to the pale outline of the human' (Marshall, 2014). The aim of SDG 16.9 could be construed to help close this gap, to ease the barriers through which all citizens can access the benefits of full legal personhood as defined by the ability to have one's existence verified and proven by the state through the registration, documentation and verification of name, personal data, date of birth and a unique identifier. It is important therefore to acknowledge that SDG 16.9 is seeking the universal provision of verifiable legal identity. The key indicator for this goal is the registration of birth. This model of identification is laid out below. However as we will explore further in this report, this model is designed for 'hard identity' where any interaction or relationship begins with a strong identification event (i.e. the provision of birth certificate). Increasingly, identity interactions use the softer models where assurance is build using a combination of factors alongside an assertion of sameness over time.




(Gelb and Clark, 2013)

# 1. Legal Identity

World Bank Group/GSMA (2016) identify four components of the assurance process. What a person is (i.e. age, gender, finger prints etc.), what a person knows (i.e. passwords, pin etc.), what a person has (i.e. smart card, mobile phone, identity documents etc.) and what a person does (i.e. handwriting, keystrokes, application use). These broader models bring into play one further area of law, that is the right to a personal identity and personality, which can evolve over time. In law these largely emanate from rights to privacy or respect for one's private life found in human rights law (Marshall, 2014, article 8, ECHR, 1950). Hamilton (2008) argues that the persona and person are 'mutually constitutive and reinforcing aspects of identity' and Marshall (2014) notes that the persona is a 'socially active, culturally produced trace of the person; a copy of the person'. According to the European Court of Human Rights, the right to identity is largely derived from the right to a private life (see notably Pretty v UK, 25 April 2002).

A key principle provided within the right to respect of one's private life, which is especially pertinent for our discussion, is the commitment to facilitate and maintain conditions for individuation and the realisation of the self over time. David Feldman (1994) argues that these privacy rights, have evolved in response to the nature of social life. They give us control over the boundaries of our existence and relations with others. They provide a sense of recognition of the interlocking social spheres in which we have different responsibilities and relationships with varying degrees of intimacy. As we explore later in this report, the right to a private life (including personal and social aspects) at home, with family or in correspondence, alongside the ability for an individual to have control over what they share about their identity is fundamental to their well-being and to protecting the core dignity of being human.

Whilst provision of legal identity most commonly comes into contact with international human rights law, there are other national and regional laws which may need considering depending on the context. For example, in the case of the UK Identity project other laws of relevance include Disability Discrimination Act, Race Relations Act and Data Protection Act (Davies, S et al 2005) and at the time EU Law (Milieu Limited, 2016). In more advanced economies we will often find more intricate and established frameworks at both national and regional levels. However, in emergent economies these frameworks may be less well established, particularly at a regional level, but potentially also at national levels.

We have set out above a brief outline of some of the key legal frameworks, predominantly enshrined within international human rights law. In the discussion, we highlighted a distinction between identity (as an inalienable human right), identity verification (as a mechanism to enable the distribution or denial of those rights), and personal autonomy (as the capacity to exercise control over what you share of your identity). These distinctions and the need for clear definitions around them were a prominent feature of the discussions at the workshop. Whilst our outline here is predominantly located within international law, it is evident that a detailed understanding is required at country level, in relation to the intersection between international human rights law, regional and national law, including the legal frameworks on data protection and privacy laws.

Strong identity practices and identity definitions based on historical documents present a self-evident contrast to the everyday identity of an individual living within a community. Technology is increasingly creating new sources of information, many of them behavioural that may start to bridge this gap. Commercial organisations have shown that they can successfully deliver services on a global basis using these behavioural attributes with an acceptable level of identity assurance. The use and adoption of behavioural data for the provision of legal identity adds both opportunity and further complexity to the landscape identified above.

# 2. Implementation Environment

In recent years, there have been many failed identity projects struggling with escalating costs, integration and user adoption being just some of the common challenges. Whilst behavioural attributes have the potential to provide new lines of data for identity systems, lessons around implementation of biometric systems must be learnt.

# 2. Implementation Environment

Developing countries have shown increasing activity in creating national identity systems. Many of the National Identity systems reviewed are utilising biometric data (ITU-T, 2016) a rapidly growing industry within the developing world. Gelb & Clark (2013) found that the biometrics industry grew at 28 percent annually between 2005 and 2010 and that the rate was even higher in developing regions, at 34 percent.

The drivers for implementing such systems include meeting development agendas, a need for greater efficiency in administration, and compliance regulation for example, Know your Customer (Makin, 2017). Such programmes are often lauded for their capacity to promote inclusion and equality. The World Bank (2017) points to four case studies in Thailand, Peru, Pakistan and India claiming that 'strong identification systems can lead countries to become more economically prosperous and secure, operate more effectively and efficiently, protect human rights, and deliver benefits to people'. However, frequently, where there is evidence of positive impacts of identity systems such as in the case of Aadhaar, we know that these systems are not a panacea. One study conducted in 2003 on e-government schemes, suggests that failure rates in implementation are high and costly. It estimated that 35% of schemes were a total failure, and a further 50% a partial failure (Heeks, 2003). However, other studies provide higher success rates. Of the 48 systems which were reviewed by ITU-T (2016) found that 35 were operational and in use, and only 3 systems had stalled. Where implementation has taken place, studies have shown that identity systems may be increasingly restrictive for marginalized communities, making it more difficult for individuals to gain access to legal documentations (Oppenheim and Powell, 2015). In other cases, states may make access to key services contingent on documentation, destroying existing informal networks of support (Caribou Digital, forthcoming; Brewer et al, 2015).

The potential of behavioural attributes to enable individuals to assert and verify their identity is largely unexplored within the developing world, however there is much to learn from the successes and failures of the national identity systems which are emerging world-wide (CESG, 2014). In this workshop, we received two contributions reflecting on national identity systems in the UK (UK Identity Cards Bill and Gov.uk) and in India (Aadhaar and other systems). These contributions led to discussions which we have broadly come to understand to be concerned with the implementation of identity systems and the conditions needed for successful implementation. Two wide-ranging themes emerged from discussions, explored further below.

# 2. Implementation Environment

## 2.1 Person centred design, governance and implementation

The benefits of digital identity systems are frequently framed around six key areas: (i) financial inclusion, (ii) gender equality, (iii) access to health and education services, (iv) social protection and safety, (v) improved governance and (vi) greater efficiency (ID4D, 2016; World Bank Group and Centre for Global Development, 2017; Atick et al, 2016). Within these broad areas, it is easy to lose sight of the actual experiences of people using these systems. How on a micro scale do these technologies both enable and constrain behaviour? How do they impact vulnerability, resilience, agency and dignity? And how might this differ for different contexts, different identities and different relational dynamics? These are all questions that emerged throughout the workshop. We highlighted that there is not a single heterogeneous group of people without access to a formal identity and that human beings belong to multiple social groups. Similarly, we emphasised that dimensions such as vulnerability, resilience, and agency are not fixed. Instead, they are highly relational and dynamic, changing according to situations and contexts and to the interplay between key identity elements such as gender, ethnicity, disability etc. in any given moment. Accordingly, the concept of 'composite vulnerability' can define for example, these multiple layers of situational vulnerability (Beduschi, forthcoming). In developing identity systems there is clearly a role for cross-discipline, cross-organisational collaboration in order to work within robust ethical frameworks. In particular scientists and engineers who develop technologies should work more closely with researchers who are specialists in law and the social consequences of technologies (Dijstelbloem, 2017).

Studies have shown that the provision of legal identity through identity systems may have significant negative consequences for already marginalised communities. Examples cited in the literature include how the transition to more formal identity systems may destabilise existing informal ecologies of social support. For example, Barrios (2015) notes that prior to implementation of identity cards, individuals habitually resident in a country were generally assumed to be citizens, even in the absence of official documentation. However, the introduction of these cards alongside the requirements to present them to obtain services, has shifted these assumptions. Individuals without documentation of identity are now often treated as, if not assumed to be, non-citizens (Barrios, 2015). Other studies are showing that they may affect people's ability to exercise privacy over who they are, for example, one study has highlighted how women who had previously been saving secretly were forced into opening bank accounts in India and were therefore at greater risk of exposing their savings to spouses and family members who had power over them (Caribou Digital, forthcoming). Identity systems have also been shown to lead to increases in discriminatory treatment in the documentation process (Oppenheim and Powell, 2015; Brewer et al, 2015). Furthermore, the challenges that some groups face is that of a temporary loss of identification, for example in the case of refugees or migrants, many may have lost their identity documents in transit or had it stolen (ID2020, 2017). As discussed in the introduction behavioural data mining and personal data analytics are leading to new forms of social harm. These include for example the increasing technological powers of governments to track individuals, alongside a reduction in the ability of people to lie about who they are, or hide their identity – a crucial capacity in order to protect against prevalent systemic abuse (Barocas and Selbst, 2016; Boyd and Crawford, 2012; Pasquale, 2015; Zuboff, 2015). We are also seeing political manipulation and collusion on an unprecedented scale via large corporate platforms such as Google and Facebook, who play a role in both governmental surveillance and security alongside intelligence gathering and crowd manipulation (Lyon 2014; Ball & Snider, 2013; Murakami Wood, 2013).

# 2. Implementation Environment

The recent publication from the World Bank Group and Centre for Global Development makes it clear that individuals 'are at the centre of identification systems and have the right to know and exercise appropriate control over how their data is collected, used, stored, and shared' (World Bank Group and Centre for Global Development, 2017). The document spotlights inclusion as one of the ten key principles of identification, it states that:

> "Legal, procedural, and social barriers to enrol in and use identification systems should be identified and mitigated, with special attention to poor people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women, children, rural populations, ethnic minorities, linguistic and religious groups, migrants, the forcibly displaced, and stateless persons). Furthermore, identification systems and identity data should not be used as a tool for discrimination or infringe on individual or collective rights".
>
> **World Bank Group and Centre for Global Development, 2017**

One clear way to achieve these aims is through active user engagement with design, implementation and governance of systems (a person-centric approach). Its notable that whilst the benefits of user engagement are well documented across a wide range of fields we know surprisingly very little about effective user involvement within the digital identity space. Though there is much to learn from other initiatives and development agendas, specific knowledge about the techniques that are required to help improve accountability and transparency, develop trust, increase the relevance of systems and enable responsiveness towards differing contexts in the digital identity space is needed. The key policy instruments driving the agenda, in particular the Ten Principles on Identification for Sustainable Development (World Bank Group and Centre for Global Development, 2017) are advocating for user engagement, however we argued that it should be cited as central pillar of the principles of inclusion, design and governance within this publication.

## 2.2 Implementation

Demand led or top down?

Whilst the majority of developing countries now have some form of digital identity system, the contexts for implementation and the way in which projects have been implemented vary significantly across regions (ITU-T, 2016, Gelb and Clark, 2013). Gelb and Clark (2013) describe two main evolution pathways, 'demand led' and 'top-down'. Demand-led services, such as was the case with Ghana's E-zwich system, evolve from meeting a demand for a specific function (in this case transferring payments) and then expand to a much wider range of services including identity documentation for those on public payroll (Gelb and Clark, 2013). Several of the examples, begin with innovations in the electoral system, for example DRC biometric registration for the 2005 elections is now the country's primary identity system. The demand-led approach can be attractive for lower-income countries particularly, given the cost, resource and infrastructure considerations. They enable innovations to start small and scale up incrementally, often building on the needs of users (Gelb and Clark, 2013). However, the demand-led approach can suffer from an inability to achieve economies of scale. There can be issues with the quality of data, security and privacy laws, likewise there is also higher-risk of building a patch-work system consisting of incompatible modules (Gelb and Clark, 2013). In contrast 'top down' approaches begin with the development of national identity systems which can then be used as a foundation for more specific applications and services. Examples abound in Latin America, but also exist in Malaysia and Pakistan and Europe (Gelb and Clark, 2013). The linkage between identity and service is often a staged process and the challenges of such approach include higher initial costs, slower development returns and possibly less active take up, more coordination and a requirement for long-term political support (Gelb and Clark, 2013).

# 2. Implementation Environment

Commercial innovation

Private companies play a crucial role in the identity provision space, through innovation, development or supply. Providers may develop and supply both hardware and software, or identity services such as enrolment and authentication. Commercial service providers also act as identity providers. For example, subscriber identity module (SIM) cards and bank cards are both a form of identity documentation, and are often linked to identifiers provided by the state. Private firms are reliant on digital identity systems in order to provide services and enable transactions, including for example through banking, online commerce, mobile network operations (World Bank Group and Centre for Global Development, 2017; World Bank Group/GMSA (2016). Some of the largest corporate organisations (Google, Facebook, Apple, Amazon etc.) are basing their business models on the capacity to know an individual customer and to predict their attitudes, needs and wants. However, this capacity remains largely untapped for the provision of social good. In a recent study of innovation in emerging markets, Caribou Digital (2016) found that relatively few firms were building identity management solutions, though there have been considerable developments in components of these solutions (i.e. biometrics, algorithmic analyses, and distributed ledgers).

They note that the innovation is largely concentrated in the US and UK with very little innovation in emerging markets, citing unproven business, significantly lower levels of digital inclusion and disposable income as key barriers (Caribou Digital, 2016). A key underlying issue behind this disjunction is the lack of investment in creating interoperable frameworks under which private companies can operate. Due to the rapid growth of these large digital industries such as Facebook we have seen the emergence of new norms, with these organisations developing standards in accordance to their own frameworks and priorities.

While the role of private business in the development of technology is easily recognised, other commercial organisations are now using this technology with existing brands to develop personalised services. These services can build a relationship with a consumer with digital interactions that allow identity to evolve in more natural fashion. This 'soft' identity approach allows individuals to control privacy with multiple profiles until a transaction (e.g. digital payment) requires a 'harder' identity to be used. In these systems, the history of behavioural data (defined by an assertion of sameness) forms the basis of both the identity assurance / verification and the valuable personalisation of the underlying service. This type of approach has benefits of data richness for the organisation and convenience for the individual, however the downstream impacts on privacy need to be monitored carefully.

# 2. Implementation Environment

There is clear common-ground for collaboration between governments and private companies in order to increase the capacity of both private and public sectors to provide efficient services to individuals, be they potential consumers or citizens. However, the roles that are played will depend on the implementation environment. Countries with more developed identity systems can enable private companies to utilise a minimum set of attributes which can be can be used for identification, authentication, and authorisation. Where this data is not available private companies may play a role in supporting the government in the provision of legal identity. For example, in Uganda mobile technology is used to enable birth registration in remote villages (World Bank Group/GMSA, 2016).

Whilst regulatory change can play a key role in fostering innovation, it can often do so without a clear sense of the purpose of the innovation from a user perspective (Caribou Digital, 2016). Identity solutions need a clear rationale and purpose underpinning how and why they might be adopted. To some extent state-led identity systems can make adoption a legal requirement (potentially leading to marginalisation and exclusion), successful private-sector systems are frequently more person-orientated.

However, Caribou Digital (2016) identified that at present a lack of scalable identity systems in the private-sector, with many of the innovations growing out of highly localised niche conditions. Building on work by Caribou Digital (2016) we identified the following groups of industry players:

- **Enterprise identity solutions providers**
  (e.g. Gemalto, Vasco, Morpho, Safran)
- **Identity providers**
  (e.g. Facebook, Google, Apple, Twitter, Mydex, Yoti, ShoCard)
- **Identity verification providers**
  (e.g. Experian, Group, Equifax, Call Credit)
- **Decentralized identity framework**
  (e.g. Blockstack Labs, Open Mustard Seed)
- **Data aggregators**
  (e.g. Acxiom)
- **Transactional providers**
  (e.g. PayPal, mobile operators, transport providers)

# 2. Implementation Environment

Fostering conditions for implementation

The place and fit of behavioural identity systems within the existing identity environment is important. There are two overlapping approaches worth considering. The first is the use of behavioural attributes alongside existing systems be they demand-led or top-down, the second is the use in contexts where neither traditional nor biometric identity systems have been successful in reaching the 1.5 billion people who do not currently have legal identity (such as women, children, rural populations, ethnic minorities, linguistic and religious groups, migrants, the forcibly displaced, and stateless persons). We explore the possibilities further in the following section.

Designing and implementing identity programmes on project by project basis, limits the potential of these systems to meet social goals, and can severely hamper progress (Gelb and Clark, 2013). ID4D (2016) identify four key enablers for successful implementation:

- Good governance and institutional capacity;
- Legal and regulatory frameworks;
- Technology standards and interoperability frameworks;
- Public-Private partnerships.

These broad areas provide a helpful basis, although it is recognised that more research is needed into the failures of identity systems, whether these be partial or complete failures. Our discussions identified a set of considerations for successful implementation, which have been further developed following the workshop to align with the ITU-T review of 160 schemes where biometric identification has been used:

(i) Existing geo-political conditions, such as the case of Afghanistan where the ongoing conflict and compressed timeframes have played a key role in hampering progress (ITU-T 2016).

(ii) Existing technology infrastructure, for example in Bolivia and Somaliland where connectivity problems have meant that biometric technology had all but a cosmetic impact on existing identity systems; or Yemen where inadequate technology, (alongside) poor procurement and data management processes have hampered progress (ITU-T 2016).

(iii) Fragmentation, for example in some instances such as Malawi where projects have been too small for savings to cover the cost of programmes, or different identity systems have been used for individual programmes thus failing to provide services in a client centred way. In one case, Nigeria there were 12 ongoing identity card projects of which 8 called for biometrics (ITU-T 2016).

(iv) Inclusive practices, for example, in the case of Aadhaar where the decoupling of formal identification from citizenship, may have helped with inclusion, but it may simply have shifted the documentation burden to later processes (ITU-T 2016). The provision of alternative pathways through a system, such as when individuals cannot supply information (i.e. fingerprints), alongside clear performance standards is crucial to inclusive systems.

# 2. Implementation Environment

(v) Privacy, although conceptions of privacy differ from culture to culture, countries require a stable framework for data protection that covers the storage, linkage and use of data.

Many developing countries do not have such a framework, and existing regulations in more developed settings are often inadequate to safeguard privacy rights in the rapidly evolving digital sphere. In the shorter-run, agreed protections on personal data within a project provide a short-term solution (ITU-T 2016).

(vi) Costs, whilst costs are falling biometric identification is still seen as too costly. Often high-cost, proprietary packages are chosen instead of cheaper low-tech substitutes. However, costs must be considered holistically, for example in the absence of a functioning identification system, biometric or behavioural systems may be no costlier than paper-based alternatives, and may save greatly in the long run due to more automation and reduced fraud (ITU-T 2016). One further consideration would be to identity existing digital platforms that already collect personal behavioural data, which might then lower costs compared to developing standalone systems.

(vii) Public opinion and trust, the formation of public opinion and trust on new technologies is not historically, culturally or geographically isolated, but linked to prior debate and experiences. Policy makers and relevant agencies need to lay the ground work for effective public support, failure to do so, could lead to non-compliance and boycott.

(viii) Policy making, the technologies associated with tracking behavioural attributes are rapidly advancing and it is therefore crucial to foster the conditions whereby policy makers can make informed decisions, and feel able to manage the risks and uncertainties.

### 2.3 Summary

It has emerged from the workshop and subsequent research that the contexts in which digital identity systems are developed are highly complex and that there is no 'off the shelf' single solution.

The studies show that good governance and institutional capacity, legal and regulatory frameworks, public and private partnerships all play a significant role, alongside clear user engagement and test cases. At present the largest digital platforms (Google, Facebook, Apple, Amazon etc.) are basing their business models on the capacity to know an individual customer and to predict their attitudes, needs and wants. This capacity is an untapped potential for social goods and particularly the provision of legal identity. Whilst some argue that the business models are unproven, the next phase of the identity landscape will need harness the capacity that is already out there in the private space as well as finding ways to incentivise innovation for development purposes. Identity defined and verified through behavioural attributes are inherently inclusive, low cost and emergent from existing technology infrastructure. Our challenge is to explore how they can be included in policy based on public opinion and new privacy practices.

# 3. Infrastructure, Science and Technology

As technologies evolve and become ubiquitous, they offer new opportunities in the developing world.

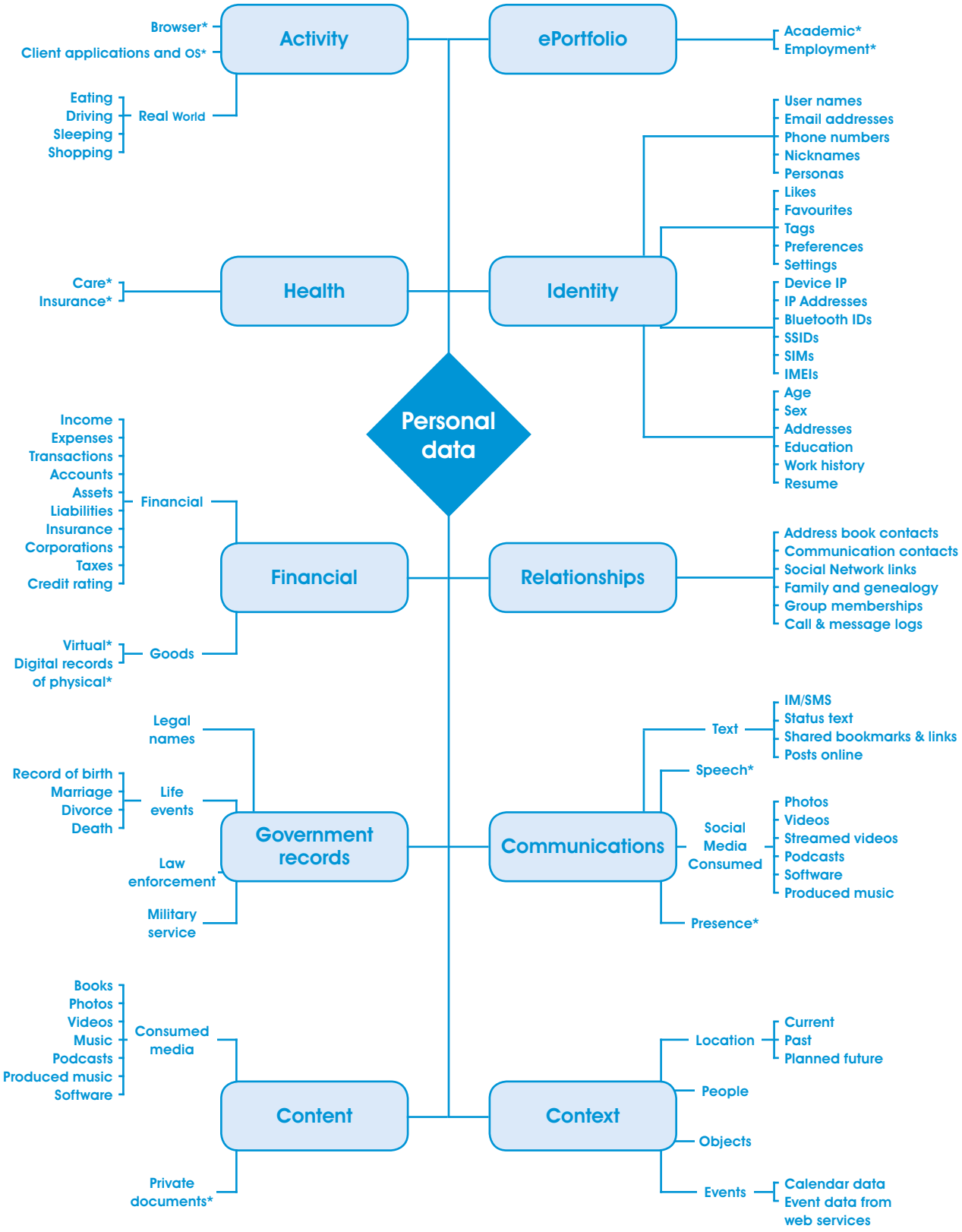
# 3. Infrastructure, Science and Technology

Participation in digital activities has traditionally been exclusionary due to the high cost of hardware and usage fees, or simply by the total absence of the necessary infrastructure in some settings. Developments in digital technology however, including inexpensive mobile devices, wireless networks, and cloud-based applications, are enabling an increasingly accessible digital sphere. We are seeing an unprecedented rise in the absolute numbers of people joining the global digital economy, enabling access to a broad range of financial, educational and social services. Mobile phones in particular present an opportunity for producing behavioural attributes for use in digital identity systems in many countries. These changes are not without negative consequences for those who cannot access the devices of digital infrastructure, as these communities are becoming increasingly marginalised.

Digital interactions point to who and where we are, whereas traditional forms (i.e. certificate of birth) and biometrics (i.e. fingerprints) work well to provide single strong identity authentication events, behavioural identifiers provide long term contextual evidence. These attributes are increasingly being explored as an additional component to identity resolution, particularly within the developed world where privacy is a primary concern, but will clearly play a role in developing world in the near future.

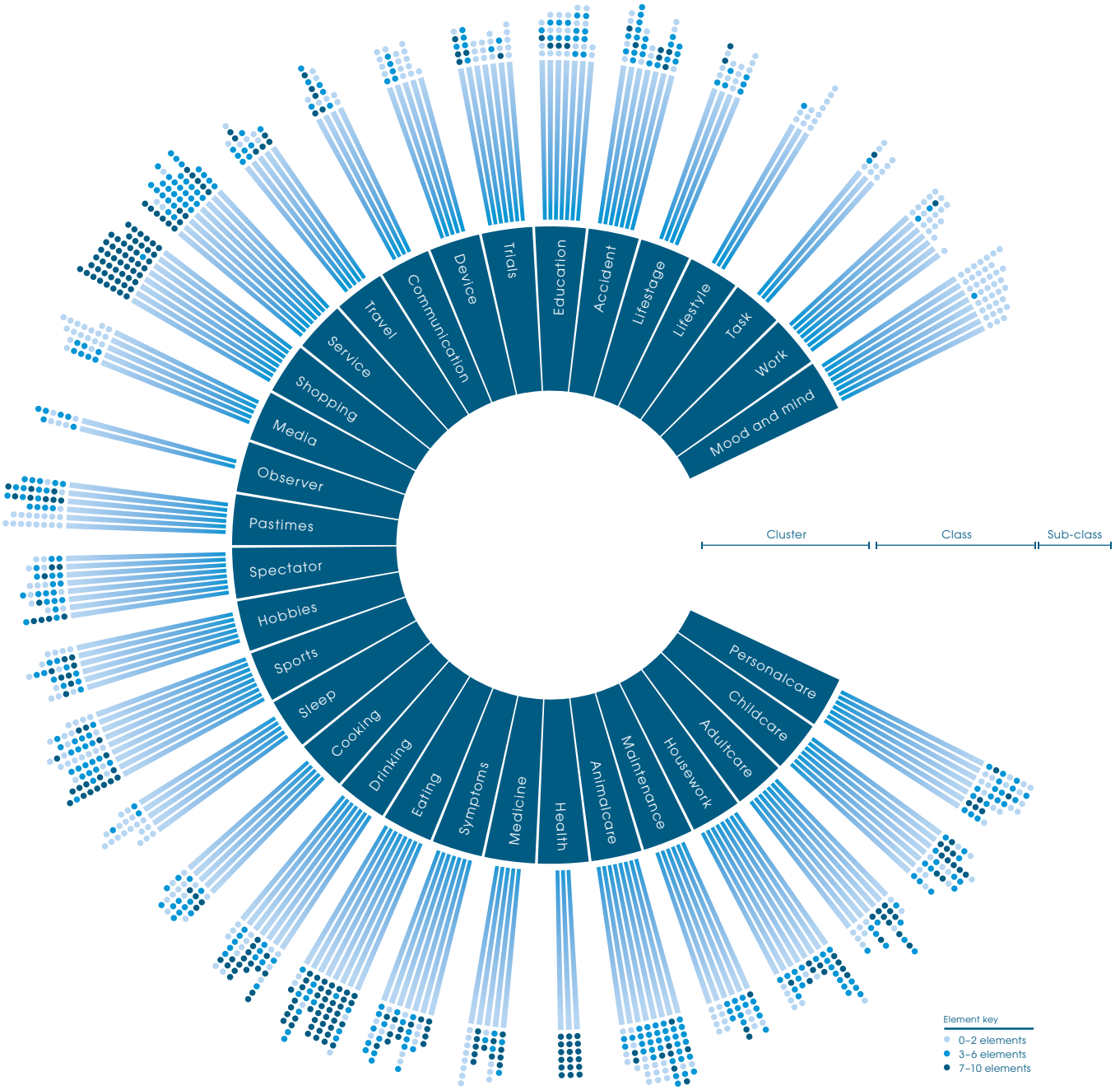
The construction of identity systems based on behaviour requires novel and systematic technical solutions that exploit and challenge currently available techniques. The assurance and validation of identity based solely on behavioural attributes or in conjunction with these attributes requires a nuanced approach to the assessment of risk. It also requires the development of statistical tools capable of assessing large amounts of low-certainty data points over long time spans to build a high-certainty outcome. Creating such a system necessitates cross sector inter-disciplinary efforts from social science, data science, networking, encryption, and computing expertise. Reflecting on our discussions at the workshop we have identified four key technical components: (i) data collection events, (ii) digital infrastructure, (iii) novel algorithms and (iv) security mechanisms. Each are explored further below.

# 3. Infrastructure, Science and Technology




**Personal Data Ecosystem (Hamlin, 2011)**
An illustration of the diversity of personal digital interactions.

# 3. Infrastructure, Science and Technology




**Visualising Life (Coelition, 2017b)**
**A taxonomy of human behaviours.**

# 3. Infrastructure, Science and Technology

### 3.1 Data collection events

Data collection events concern any area of our life which can be recorded. These might typically include mobile phone use, engagement with social media, shopping, browsing, or accessing services. Hamlin (2011) provides one illustration of the range and diversity of digital interactions (see illustration).

However, as the boundaries between the digital and the real world become increasingly blurred we require ever more sophisticated taxonomies for understanding, coding and processing our behavioural data. An emerging challenge for identity systems is to harness this data in a manner that is scalable and can build technology-agnostic systems with privacy and human rights protection at their core. Coelition's work in this area has continued to show the importance of being able to separate the information about an individual's behaviour from the means that it was collected (Coelition, 2017). The OASIS COEL specification (OASIS, 2017) is one such framework supporting the collection and processing of behavioural data. Centered on a holistic, hierarchical taxonomy, it allows any type of event in our daily lives to be recorded and be uniquely coded to an individual (see illustration). Crucially, the specification pseudonymises personal data at source and maintains a separation between the different data types and clearly defined roles & responsibilities for all actors. All behavioural data are defined as event-based packets. Every packet is connected directly to an individual and can contain a summary of the consent they provided for the processing of the data (Coelition, 2017). This highlights the existence of mechanisms through which data portability can be enabled.

### 3.2 Digital infrastructure:

Digital infrastructure in the form of networks (i.e. fixed internet, GSM, 4G, Wi-Fi), storage and processing systems (i.e. distributed servers / cloud) are central to economic growth and development. However, this same infrastructure can significantly interfere with the privacy of the individuals who come to rely on it. As the digital economy grows new pressures are placed on the supporting infrastructure with key challenges varying depending on the contexts. In India, there has been a rapidly expanding growth in telecom technology (reportedly going from no connectivity to over 350 million mobile Internet users in less than two decades), challenges include spectrum availability and costs, broadband infrastructure and reaching rural areas (Samtani and Sarawgi, 2017). In Sub-Saharan African, where mobile phone proliferation is amongst the highest in the world (Zamfir, 2015) new business models are addressing some key infrastructure challenges. For example, only 24% of the population of Sub-Saharan Africa has access to electricity, but rather than hamper access to digital technology, a number of businesses are tapping into the opportunity and providing solar panels for powering lamps and recharging phones in exchange for small payments over the phone (Zamfir, 2015).

In our discussions, we noted both the challenges and importance of public private partnerships in not only promoting growth and innovation but in ensuring standards which generate trust, protect rights and promote equality. These standards should overlay the following two principles which underpin the development of digital infrastructure in order to create the conditions for new digital identity systems:

- Interoperable platforms: there is no single approach to improving identification systems. Each country, department, and business develops its systems in a way that are suited to its core aims. Having frameworks for interoperability across platforms can enable integration, scalability and cross border operation.
- Open standards: facilitate interoperability and data exchange among different products or services and are intended for widespread adoption. Also work to provide auditability, transparency and data portability.

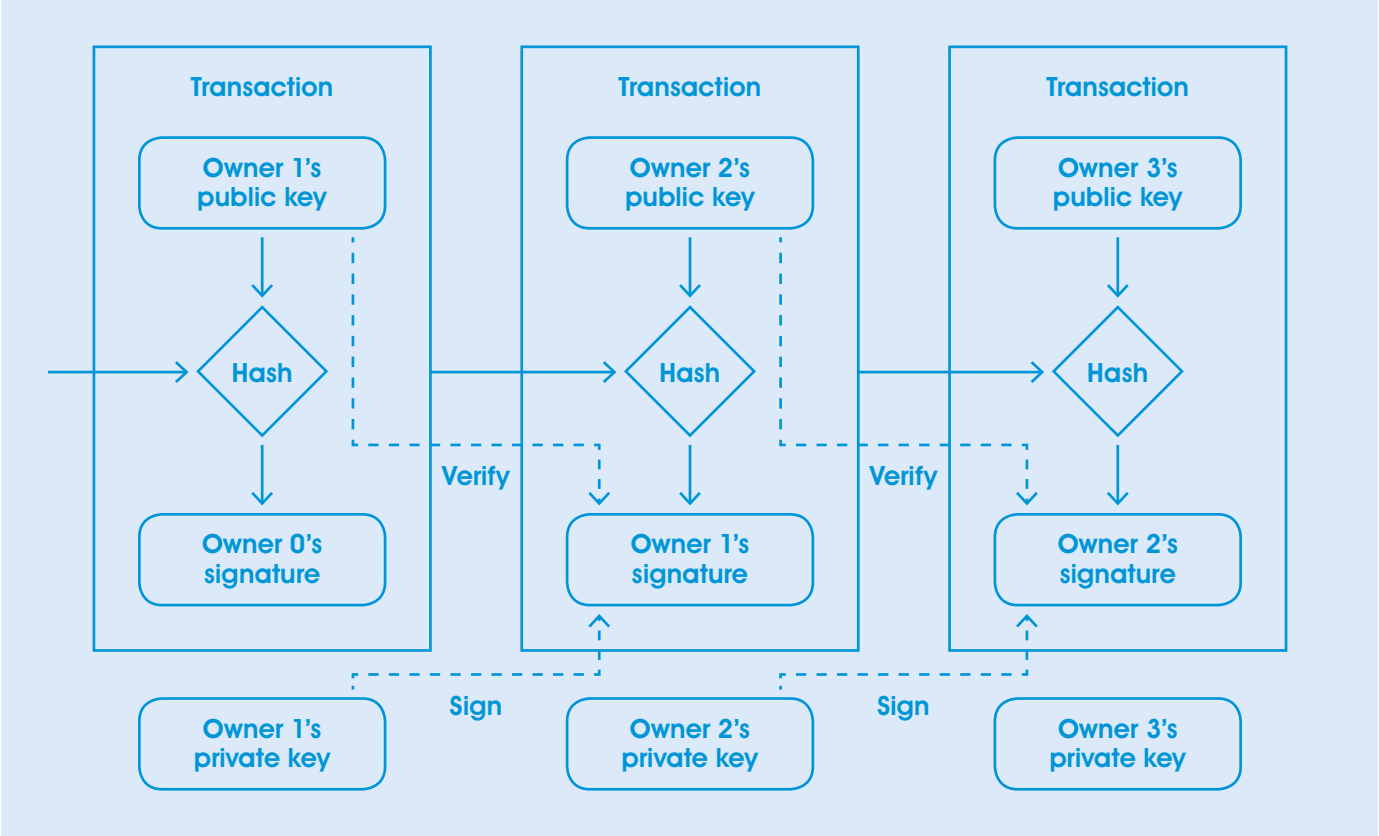
# 3. Infrastructure, Science and Technology

### 3.3 Novel algorithms

There is a growing body of research advancing digital identity provision and verification. These include novel algorithms which may help in cases of identity uncertainty, increasing privacy, data protection and shared signals. Examples include: probabilistic modelling which uses probability theory to express uncertainty and noise within a model; Bayesian inference, which permits reasoning about uncertain events and the incorporation of expert information, and machine learning. Machine learning for example is being used by Microsoft to help protect identity and produce intelligence on who might be trying to attack accounts (Androutsopolos et al., 2000, Microsoft, 2016).

### 3.4 Secure data storage and communications

The focus of this research was not to select or invent technical solutions, however we found it useful to outline some of the technologies of potential to expose the wider issues. One such technology is the use of blockchain as a verifiable open ledger. It provides a potential mechanism to enable an individual with limited access to digital technology and infrastructure to verify who they are, in a way that is secure and protects the privacy of the individual. The technology is an example of the types of approach that might specifically support the population of 1.5 billion people who exist without the capacity to verify who they are.




Nakamoto, undated
An illustration of the blockchain technology.

# 3. Infrastructure, Science and Technology

The proposal follows three key principles. First of all, it is open, so that anyone can participate. Secondly, it is distributed therefore relying on multiple copies of the database being kept across distributed network. This model ensures that the system is less vulnerable to fraud, as the database both self-corrects and signals intrusion should someone seek to hack the system and infringe some records. The third and final principle is that each successive block in the chain is digitally signed by the owner of the previous block (see illustration).

An additional element of the overall system could be the use of SCRAM protocols (Salted Challenge Response Authentication Mechanism). It is commonly known for its use in secure chat systems (XMPP). It enables mutual authentication between server and client without plaintext password exchange or storage at any stage, and crucially free implementations exist. It thus provides a technological solution to allow secure upload of identity information to a blockchain. The system could hypothetically enable a blockchain of identity photos and ancillary information to be stored in an encrypted block, and could be verifiable from anywhere with internet access. The proposal raised a discussion about the ability of block chain technology to encode additional information overtime - crucial for use in capturing a history of behavioural evidence. We also noted that there was a role for 'trusted person', an individual based within the community who would provide additional verification that the original upload was genuine.

Distributed ledgers are not a universal solution. They are not particularly good databases for high volume data transactions and analytics. The technical approach to consensus is not fully standardised and changes in the underlying processes can lead to issues such as invalidation of existing data assets.

Other distributed technologies may also be useful (for example smart contracts or personal data stores) in the provision of data sharing, agreements, consent and permissions management. All these approaches will have their own benefits and challenges. The larger question will remain how can we use these technologies to drive digital inclusion in an interoperable and trustworthy manner?

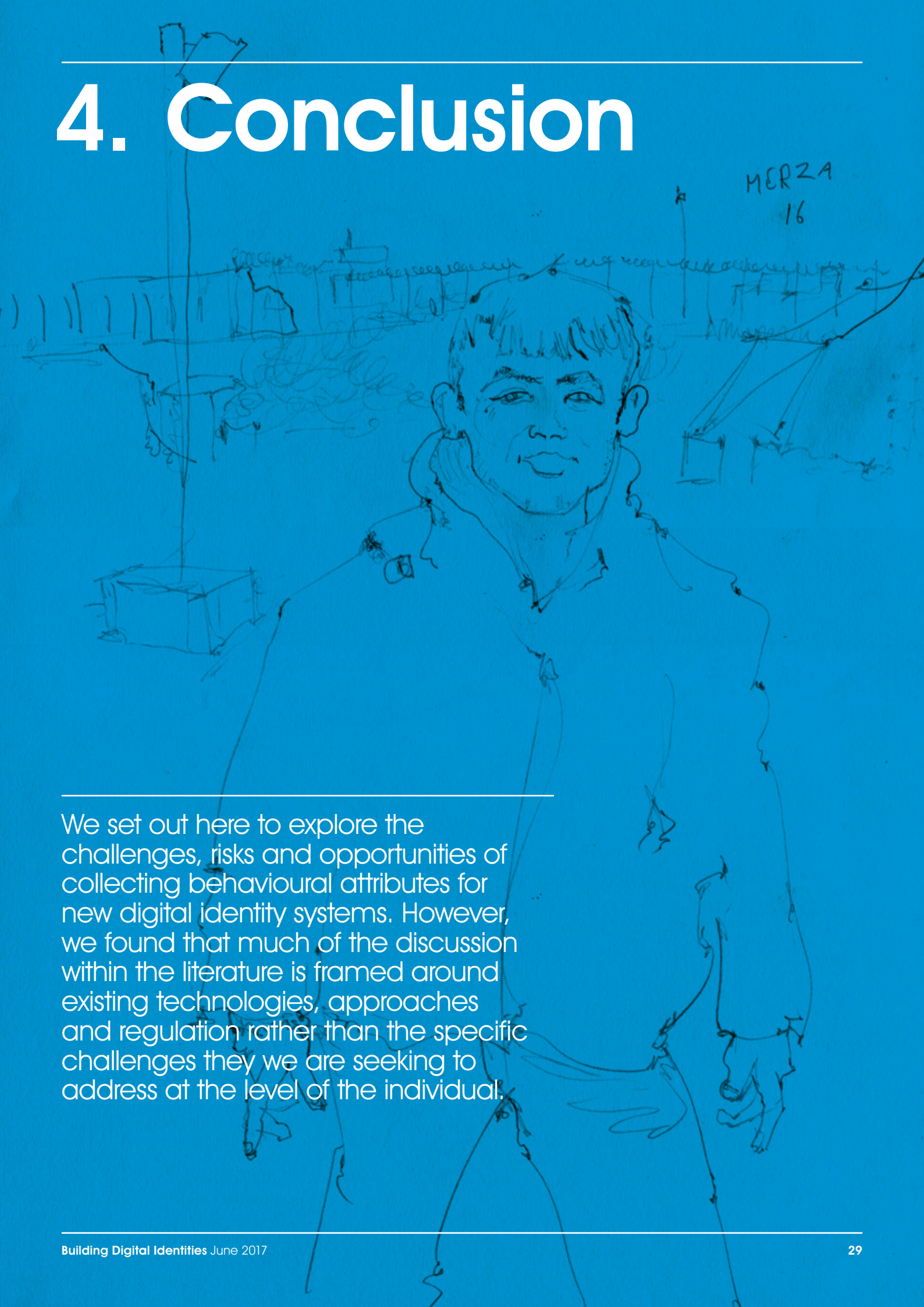
# 3. Infrastructure, Science and Technology

### *3.5* Summary

The importance of identities, particularly to the most vulnerable groups worldwide, should be a critical consideration for a digital identity system built on digital signatures (Mason, 2017) and life events, where state-of-the-art security measures should be thoroughly investigated in research and properly tested in real-world industrial systems, and thus requiring cross-sector multidisciplinary efforts. Specific concerns of security measures include database security, network security and physical security, which are pivoted by advanced encryption algorithms and network security protocols such as Advanced Encryption Standard (AES) and Transport Layer Security (TLS), whether they can provide the required stringent performance in a distributed and large-scale system would be an interesting topic worth further investigation.

Finally, it is important to note that although regulations are evolving away from traditional static verification, we are not close to a point whereby policymakers are confident enough to trust the performance of algorithmic models and codify them in regulation (Caribou Digital, 2016). Serious questions are being asked about how such algorithms are designed, what levels of accuracy are appropriate, and how to ensure transparency and accountability in automated decision-making (Caribou Digital, 2016; Ananny, 2016; Kitchin, 2016). There is a pressing need to provide ongoing intelligence to policy makers and the public about the potential and risks of new technologies and how they might help ameliorate or hinder our ability to address social problems.

# 4. Conclusion




We set out here to explore the challenges, risks and opportunities of collecting behavioural attributes for new digital identity systems. However, we found that much of the discussion within the literature is framed around existing technologies, approaches and regulation rather than the specific challenges they we are seeking to address at the level of the individual.

# 4. Conclusion

In exploring the role of behavioural attributes for the 1.5 billion people who lack legal identity, we have been able to ask questions about the nature of 'legal' identity that are currently under-explored in the literature with a focus on the ethical, social, and human rights based aspect of identity provision. We have sought to bring into the discussion a need to understand who these 1.5 billion people are, and the importance of considering the composite factors of vulnerability, agency, dignity and resilience. We feel there is a strong case for a more prominent focus on user engagement within the key policy instruments of the agenda including the ID4D programme, as part of an approach to developing digital identity systems based on societal norms and expectations.

Whilst we have found that it is inappropriate to look at the use of behavioural attributes as separate to traditional verifiable facts and biometrics, we have identified a need to place people at the heart of design, implementation and governance of digital identity systems. It is important to note that the use of behavioural attributes for the purposes of targeted marketing has played a significant role in the commercial success of organisations such as Facebook and Google, who are now looking for expanded growth in commercial markets and concurrently are playing a role within the digital identity arena.

We have considered both developed and developing settings and whilst the technical challenges are very similar, the priorities are different. Strong governance models and the wide availability of traditional verifiable identity attributes in developed markets leave behavioural attributes as a relatively low risk route to enhance convenience. In developing markets, the lack of verifiable identity attributes (such as birth certificates) mean that carefully collected behavioural attributes can have a significant impact for individuals. However, low levels of digital inclusion and disposable income alongside unproven business models may be hampering innovation in this space at present. In the context of weak state-level identity systems, poor governance and infrastructure, there is an urgent need for frameworks and regulation to ensure that identity systems are robust and built ethically, safeguarding privacy, dignity, autonomy, and agency.

Fears about the low-governance roll out of commercial services in developing markets spring from their well-recognised ability to drive change from the demand-led paradigm. The attitude to commercial risk in the private sector provides opportunities as well as risks - durable partnerships will help to control and harness this drive.

We have found that technology itself is playing a role in enabling the changes that are being sought. Distributed servers and the GSM network may place sections of the 1.5Bn within reach of a digital future. Questions remain not just around digital inclusion, but also around who will control the information and the algorithms, alongside who we should trust to have this control and to what means it might be used.

Finally, we have found that the role of behavioural attributes in digital identity systems is vastly unexplored in both policy and development practice although used to some extent within private enterprise. With our current trajectory with regards to digital technology and its integration with society, how these developments are shaping how we act, how we think and what we can do, it is evident that these attributes will play an increasingly significant role in both developed and developing settings. It is essential that identity related policy keeps a pace with these developments, in order to enable innovation that is responsible, ethical and can enhance the freedoms of the 1.5 billion people who do not have access to legal identity.

# 5. Priorities for research and action

Following our discussions at the workshop and subsequent desk based research we have identified a number of key areas for further research:

# 5. Priorities for research and action

### Person-centred design

- How can we enable individuals to be involved in the design, implementation and governance of digital identity systems?
- How are publics informed about identity systems and what agency do they have in the design and use of such systems?
- What are the incentives for adopting identity systems (i.e. the push and the pull) and how are these incentives built into the system?
- What innovative communication/education techniques are used to reach and encourage uptake in hard-to-reach communities?
- What are the various touch-points where individuals may be excluded from a digital system?
- What innovative research methods have been used to identify and articulate these touch-points, in particular with marginalised communities (i.e. bottom of the pyramid, women in rural areas, refugees and migrants)?
- How have agencies responded with innovation in design?

### Legal and regulatory frameworks

- What are the key legal frameworks and how do these intersect with identity systems and provision?
- How do legal norms and institutions that regulate procedures and processes, differ across countries and regions and what are their impact on implementation?
- How can we develop international standards, norms and agreements for person-centric identity provision on a global scale?
- What is the role of international actors in encouraging regulation and norms at a country level?
- How will legal responsibilities and liabilities be negotiated in complex systems with many providers, devices, algorithms and users?

### Public, private and person partnerships

- What are the relationships between the personal interests, the commercial interests and the state's interest in the control of data and identity?
- What is the role of regulation within these partnerships? What are the regulatory frameworks required to enable innovation but protect human rights of individuals?
- How to identify and manage the many disparities of power and influence between the individual and the state or commercial organisation?
- What are the business models that might drive innovation?
- What values do corporate organisations use, and to what extent are they in keeping with development provision? Can those values sustain themselves overtime?
- How can different attitudes to risk be understood and integrated into the development of digital identity systems?

# 5. Priorities for research and action

### Social and ethical considerations

- What are the normative societal expectations around legal identity and digital identity systems?
- How do systems impact agency, resilience, vulnerability and trust?
- Who are the 1.5 billion people without legal identity? What are the different groups that exist (i.e. refugees, migrants, rural communities) and how do we design systems for and with them? In what ways do identity systems enhance or restrict their freedoms?
- What are the different attitudes to privacy for different groups and how might these attitudes shape policy and behaviour? To what extent are new schemes needed to raise digital literacy and awareness of rights around privacy, access etc.?

### Technology and innovation

- What are the innovation pathways for digital identity systems based on behavioural attributes?
- What is the likely road-map for digital infrastructure across different countries and regions?
- Which technologies are best placed to operate in this landscape?
- What are the limitations of the technologies and how could any restrictions be mitigated?
- What is the role of academic research and how can design knowledge be transferred?
- How can proof of concept experiments for behaviour based identity systems be run, both as augmentations of existing systems and as stand-alone systems?

## Workshop Participants

**Ana Beduschi,** Law School, University of Exeter

**James Boyle,** Technology, Media & Communications, Michelmores LLC

**Jonathan Cinnamon,** Human Geography, University of Exeter

**Richard Everson,** Computer Science, University of Exeter

**James Griffin,** Law School, University of Exeter

**Shyam Krishna,** Royal Holloway, University of London

**Joss Langford,** Coelition

**Mark Levine,** Department of Psychology, University of Exeter

**Chunbo Luo,** Computer Science, University of Exeter

**Joasia Luzak,** Law School, University of Exeter

**David Llewellyn-Jones,** Pico Project, University of Cambridge

**David Owen,** Gurukula

**Emrys Schoemaker,** Caribou Digital

**Edgar A. Whitley,** London School of Economics and Political Science

## Contributors

**David Alexander,** Mydex

**Mark Lizar,** Open Consent

**Michele Nati,** Digital Catapult

**Matt Reed,** Coelition

**David Snelling,** Fujitsu

# 6. References

# 6. References


**Ananny, M. (2016).** Toward an Ethics of Algorithms: Convening, Observation, Probability, and Timeliness. Science, Technology & Human Values 41(1): 93-117.

**Androutsopoulos, I., Koutsias, J., Chandrinos, K. V., Paliouras, G., and Spyropoulos, C. D. (2000).** An evaluation of naive bayesian anti-spam filtering Proceedings of the workshop on Machine Learning in the New Information Age, G. Potamias, V. Moustakis and M. van Someren (eds.), 11th European Conference on Machine Learning, Barcelona, Spain, pp. 9-17, 2000.

**Arora, P. (2016).** Bottom of the Data Pyramid: Big Data and the Global South. International Journal of Communication 10: 1681-1699.

**Atick, J., Dahan, M., Gelb, A., and Harbitz, M. (2016).** Enabling Digital Development: Digital Identity, World Bank Development Report

**Ball, KS., and Snider, L. (eds) (2013).** The Surveillance-Industrial Complex: A Political Economy of Surveillance. London: Routledge.

**Barocas, S., and A. D. Selbst. (2016).** Big data's disparate impact. California Law Review 104: 671-728.

**Barrios, J. (2015).** The Hague Colloquium on the Future of Legal Identity, The Hague Colloquium on the Future of Legal Identity

**BBC (2017).** Pakistan asks Facebook to help fight blasphemy, available online: http://www.bbc.co.uk/news/world-asia-39300270

**Beduschi, A. (forthcoming).** Vulnerability on Trial: Protection of Migrant Children's Rights in the Jurisprudence of International Human Rights Courts. Boston University International Law Journal 36(1) available online: https://ssrn.com/abstract=2971116

**Boyd, D., and K. Crawford. (2012).** Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society 15(5): 662-679.

**Breckenridge, K. (2014).** Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present. Cambridge: Cambridge University Press.

**Brewer, M., Menzies, N., and Schott J. (2015).** Identification Systems Don't Always Serve the Bottom 40%, Just Development, World Bank

**Caribou Digital (2016).** Private-Sector Digital Identity in Emerging Markets, Caribou Digital Publishing, UK

**Caribou Digital (forthcoming).** Identity Research, Presentation by Emrys Schoemaker at ESRC sponsored Building Digital Identities Workshop, 2017

**CESG & Cabinet Office (2014).** Good Practice Guide No. 45 Identity Proofing and Verification of an Individual, available online: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

**Coelition (2017).** COEL Standard, available online: https://coelition.org/business/resources/coel-standard/

**Coelition (2017b).** Visualising Life, available online: https://coelition.org/business/resources/visualising-life/

**Davies, S., Hosein, I., and Whitley, E. (2005).** The identity project: an assessment of the UK Identity Cards Bill and its implications, London: LSE Research Online. Available at: http://eprints.lse.ac.uk/archive/00000684

**Dijstelbloem, H. (2017).** Migration tracking is a mess, Nature, available online: http://www.nature.com/news/migration-tracking-is-a-mess-1.21542

**Douzinas, C. (2007).** Human Rights and Empire: The Political Philosophy of Cosmopolitanism, Routledge-Cavendish, Oxford

**ECHR (1950).** European Convention on Human Rights, available online: http://www.echr.coe.int/Documents/Convention_ENG.pdf

**ECHR (2002).** Case of Pretty v. The United Kingdom, European Convention on Human Rights, available online: http://hudoc.echr.coe.int/eng?i=001-60448

**Feldman, D. (1994).** Secrecy, Dignity, Or Autonomy? Views of privacy as a civil liberty, Current Legal Problems 47 (Part_2): 41-71.

# 6. References


**Gelb and Clark (2013).** Identification for Development: The Biometrics Revolution, Working paper 315, Centre for Global Development: https://www.files.ethz.ch/isn/159149/1426862_file_Biometric_ID_for_Development.pdf

**Hamilton, S. (2008).** Impersonations: Troubling the Person in Law and Culture, University of Toronto Press, Toronto

**Hamlin, K. (2011).** Personal Data Ecosystem talk at Digital Privacy Forum, Jan 20th, 2011 in NYC, available online: https://identitywoman.net/personal-data-ecosystem-talk-at-digital-privacy-forum-jan-20th-2011-in-nyc/

**Harbitz, M., and Tamargo, M. del C. (2009).** The Significance of Legal Identity in Situations of Poverty and Social Exclusion: The Link between Gender, Ethnicity, and Legal Identity, IDB. http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=2255297

**Harbitz, M., and Molina, J. (2010).** Civil Registration and Identification Glossary, Inter-American Development Bank, available online:https://publications.iadb.org/bitstream/handle/11319/402/Civil%20Registration%20and%20Identification%20Glossary.pdf?sequence=2

**Hashim, A. (2017).** Authorities ask Facebook to help fight blasphemy, Aljazeera, available online: http://www.aljazeera.com/news/2017/03/authorities-facebook-fight-blasphemy-170317081007397.html

**Heeks, R. (2003).** Most eGovernment-for-Development Projects Fail: How Can Risks be Reduced? Institute for Development Policy and Management, available online: http://idpm.man.ac.uk/publications/wp/igov/index.shtml

**ID4D (2016).** Identification for Development: Strategic Framework, World Bank Group, available online: http://pubdocs.worldbank.orgen/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf

**ID2020 (2017).** ID2020: Concept for Public/Private Partnership, available online: https://static1.squarespace.com/static/578015396a4963f7d4413498/t/589334bc5016e124bb583809/1486042340845/ID2020+White+Paper+-+Jan+2017

**ITU-T (2016).** Review of National Identity Programs, available online: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review%20of%20National%20Identity%20Programs.pdf

**Kitchin, R. (2016).** Thinking critically about and researching algorithms. Information, Communication & Society: 1-16.

**López, L., Sejersen, T., Oakeshott, N., Fajth, G., Khilji, T., and Panta, N. (2014).** Civil Registration, Human Rights, and Social Protection in Asia and the Pacific, Asia-Pacific Population Journal, ESCAP

**Makin, P. (2017).** Anti-Money Laundering, Know Your Customer, and Curbing the Financing of Terrorism, FSD Africa http://www.fsdafrica.org/wp-content/uploads/2017/03/17-03-30-AML-Report.pdf

**Lyon, D. (2014).** Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society 1(2).

**Lyon, D., and Ö. E. Topak. (2013).** Promoting Global Identification: Corporations, IGOs and ID card systems. In The Surveillance-Industrial Complex: A Political Economy of Surveillance, edited by Ball, K. and L. Snider, 27-43. London: Routledge.

**Marshall, J. (2014).** Human Rights Law and Personal Identity, Routledge, NEW YORK

**Mas, I., and D. Porteous. (2015).** Minding the Identity Gaps. Innovations: Technology, Governance, Globalization 10(1-2): 27-52.

**Mason, S. (2017).** Electronic Signatures in Law: Fourth Edition. University of London School of Advanced Study. http://humanities-digital-library.org/index.php/hdl/catalog/view/electronicsignatures/1/86-1

**McCrudden (2008).** Human Dignity and Judicial Interpretation of Human Rights, European Journal of International Law, 19 (4): 655-724

**Milieu Limited (2016).** The Legal and Political Context for Setting up a European Identity Document, Study for the AFCO Committee, EU, available online: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556957/IPOL_STU(2016)556957_EN.pdf

# 6. References


**Microsoft (2016).** Microsoft Security Intelligence Report, Vol 21

**Murakami Wood, D. (2013).** What is global surveillance? Towards a relational political economy of the global surveillant assemblage. Geoforum 49: 317-326.

**Nakamoto, S. (undated).** Bitcoin: A Peer-to-Peer Electronic Cash System, available online: https://bitcoin.org/bitcoin.pdf

**OASIS (2017).** OASIS Classification of Everyday Living (COEL) TC, available online: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=coel

**OIX Open Identity Exchange (2013).** The Shared Signals Model, available online: https://www.openidentityexchange.org/blog/2013/10/05/shared-signals/

**Oppenheim, B. and Powell, B. (2015).** Legal Identity in the 2030 Agenda for Sustainable Development: Lessons from Kibera, Kenya, Open Society Foundation, available online: https://www.opensocietyfoundations.org/sites/default/files/legal-identity-2030-agenda-lessons-kibera-kenya-2051216.pdf

**Pasquale, F. (2015).** The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge, MA: Harvard University Press.

**Prevent Genocide International (2015).** Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing, available online: http://www.preventgenocide.org/prevent/removing-facilitating-factors/IDcards/samples/

**Samtani, K., and Sarawgi, S. (2017).** Building India's Digital Highway, Live Mint, available online: http://www.livemint.com/Politics/xLnErGf2Mq9xDQYj3VHWmI/Building-Indias-digital-highway.html

**UNHR (1966).** International Covenant on Civil and Political Rights, available online: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

**UN (1948).** Universal Declaration of Human Rights, available online: http://www.un.org/en/universal-declaration-human-rights/

**World Bank Group/GSMA (2016).** Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, World Bank Group, available online: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf

**World Bank Group and Centre for Global Development (2017).** Principles on Identification: For Sustainable Development Toward the Digital Age, available online: http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-PUBLIC-web-final-ID4D-IdentificationPrinciples.pdf

**World Bank Group/GMSA (2016).** Digital Identity: Toward Shared Principles for Public and Private Sector Cooperation, International Bank for Reconstruction and Development / The World Bank

**World Bank (2017).** Identification for Development, available online: http://www.worldbank.org/en/programs/id4d

**Zamfir, L. (2017).** Digital development in Sub-Saharan Africa, European Parliamentary Research Service

**Zuboff, S. (2015).** Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology 30(1): 75-89.

**Zuboff, S. (2016).** The Secrets of Surveillance Capitalism. Frankfurter Algemaine Zeitung. Available online (accessed 22 December 2016): http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html

# Programme Partners

**Coelition**
Coelition is an independent not-for-profit company that was founded in the UK in 2013. We support a global ecosystem for the responsible use of personal behavioural data. This ecosystem is built on openly published standards that we actively support and help develop.
https://coelition.org

**College of Engineering, Mathematics and Physical Sciences, University of Exeter**
Engineering, Mathematics and Physical Sciences brings together the excellent teaching and research of these complementary specialisms. Our collegiality facilitates a truly interdisciplinary approach to scientific innovation and learning.
http://emps.exeter.ac.uk

**College of Life and Environmental Sciences, University of Exeter**
The College of Life and Environmental Sciences brings together the complementary disciplines of Biosciences, Geography, Psychology and Sport and Health Sciences to provide a rich and diverse interdisciplinary teaching and research portfolio.
http://lifesciences.exeter.ac.uk

**Economic and Social Research Council (ESRC)**
The UK's largest organisation for funding research on economic and social issues. We support independent, high quality research which has an impact on business, the public sector and civil society.
http://www.esrc.ac.uk

**Gurukula**
Consultancy, research and insight providers with expertise in engagement, development and systems approaches to managing change.
http://www.gurukula.co.uk

**Law School, University of Exeter**
The Law School has a worldwide reputation for excellence in teaching and research, attracting academics, visiting lecturers and students from across the globe. We are an ambitious, dynamic and friendly law school delivering a first-class legal education at an elite Russell Group university.
http://socialsciences.exeter.ac.uk/law/

**Nick Ellwood**
Illustrator / reportage artist. The illustrations in this report are from a series drawings entitled 'I can see England', an Arts Council England funded project looking at evolving questions around migration and what it is we call home. The drawings are of people who were living in the Calais camps in December 2015. 'I can see England' is a non-for-profit project and for the reproduction of the drawings in this publication a donation was made to the charity Yorkshire Aid, supporting the plight of refugees in the UK and across Europe.
http://www.nickellwood.co.uk

**Studio Tom, Dick & Harry**
This report was designed by Tom, Dick & Harry.
http://studiotdh.com

Coelition

E·S·R·C
ECONOMIC
& SOCIAL
RESEARCH
COUNCIL

UNIVERSITY OF
EXETER