United Nations Development Programme
Event Report

Private Sector Engagement Roundtable, 18-19 May 2021: Future of Technology and Institutional Governance in Identity Management

Woman registering her biometric signature for her new National ID card in Roatán, Honduras, November 2020 (photo: UNDP Honduras)

From the People of Japan

This activity is funded by the kind contribution from the Government of Japan

18-19 May 2021

The views expressed during the event and in this report are those of speakers and participants and do not necessarily reflect the views of the United Nations, UNDP, the UN Legal Identity Agenda Task Force or other participating UN agencies, funds, donors or programmes.

Editor in Chief: David Wooff

Copy Editor: Erin Barrett

Author: Christine Gerlier

Table of Contents

1. Overview

1.1 Objectives

UNDP is co-chair, along with UNICEF and the UN Department of Economic and Social Affairs (UNDESA), of the UN Legal Identity Agenda Task Force, established in 2018 by the UN Deputy-Secretary-General to allow the UN system to assist Member States in achieving universal legal identity for all, including birth registration, by 2030. Without proof of identity, hundreds of millions of individuals are marginalised; unable to access numerous public and private services; and excluded from many elements of the formal and informal economy.

With increasing demands from Member States to provide support for digital legal identity, UNDP (and the Task Force) needs to be informed of developments in the private technology sector identity space that will affect public management of identity in years to come. To engage with the private technology sector more formally, UNDP organised an online roundtable event, on 18-19 May 2021, where both the UN and the private technology sector learnt how technological innovation will likely affect and influence future debate around civil registration and identity management (as well as its institutional governance).

The purpose of the event was strictly policy dialogue. UNDP and the UN Legal Identity Agenda Task Force do not endorse any of the participating private sector companies or their products. UNDP is grateful to the Government of Japan for funding this stream of work.

1.2 Participants

While the roundtable event welcomed anyone who was interested, the objective was to foster dialogue between UNDP and the private technology sector. As such, speaking roles were predominately given to representatives from the private sector. In excess of 200 people from the private sector, governments, academia, development and UN agencies registered for the event, representing 45 countries and regions.

1.3 Format and Output, and Structure of this Report

The event took the form of an online roundtable session where the facilitator encouraged participants to present their views on different thematic topics. Prior to the roundtable commencing, participants were requested to register and complete a set of survey questions. This summary report of the policy dialogue roundtable is being forwarded to all facilitators, speakers and participants, as well as all members of the UN Legal Identity Agenda Task Force (for their consideration when advising on, or adopting, digital innovations in identity management with national partners and their client populations). The report is not meant to chronologically summarise all of the sessions. Rather, it gives a flavour of some of the viewpoints raised within the sessions, as a means of documenting the contributions and recognising the variety of perspectives represented. Some of the contributions documented here do not align fully with the UN Legal Identity Agenda, but they are recorded for the purposes of documenting policy debate, with some key quotations included in emboldened text. Some of the bullet points are best read as standalone statements and do not appear chronologically in how they were presented.

1.4 Agenda

Day 1: 18 May 2021 CENTRAL EUROPEAN TIME (GMT+1)

Session Name	Time / Speaker (GMT+1)	Issues
Introduction to the dialogue (15 minutes)	1400 – 1415, *Sarah Lister, UNDP*	• **Purpose of the dialogue**
Session 1: Ownership, control and management of legal identity systems and data (60 minutes)	1415 – 1515, *Facilitator, Dr. Joseph Atick, ID4Africa*	• **Ownership** – Does the private sector think that UN Member States will, or should, outsource any elements of **granting** legal identity (via birth registration or registration in national ID schemes) in years to come? • **Management** – Does the private sector think that UN Member States will, or should, outsource specific elements of legal identity **management** (e.g., digital keys issuance to access services online) in years to come? • **Management** – Does the private sector think that there are alternatives to centralised state management of legal identity that would elicit greater public trust? How could civil society, academia, digital rights advocates, and private sector innovators play a greater role?
Break (10 minutes)	1515 – 1525	
Session 2: Ownership, control and management of legal identity systems and data (continued.) (60 minutes)	1525 – 1625, *Facilitator, Stéphanie de Labriolle, Secure Identity Alliance*	• **Control** – How much control can, or should, an identity data subject (citizen or non-native resident) reasonably expect to have in changing, editing or deleting certain identity data (e.g., such as name or sex/gender), or an ability to limit access to it, by public bodies in years to come? • **Control –**What role, if any, will decentralised IT architectures (such as blockchain) have in organising/archiving civil and national population registers in the years to come?
Break (10 minutes)	1625 – 1635	

<u>SESSION 3:</u> **Digital vaccine certificates and the future role of health data in identity systems** (55 minutes)	1635 – 1730, *Facilitator, Ms. Jhalak Mrignayani Kakkar, National Law University, Delhi*	• Why stop at COVID-19 vaccination data? Does the private sector think that the 'Yellow Vaccination Book' (e.g. for Hepatitis, Yellow Fever vaccination) will go fully digital? Will it be part of the data variables linked to digital passports? What additional health data, if any, is likely to be added to legal identity systems in the coming years?

Day 2: 19 May 2021 CENTRAL EUROPEAN TIME (GMT+1)

Session Name	Time / Speaker (GMT+1)	Issues
<u>SESSION 4:</u> **Is the clock ticking for paper and plastic?** (60 Minutes)	1400 – 1500, *Facilitator, Ms. Kaliya Young 'Identity Woman'*	• Does the private sector think that UN Member States will still be issuing paper and plastic identity documents in 10 years time? • If credentials using paper and plastic disappear, how can data subjects be empowered to contest the accuracy of digital records? • Can/should paper and plastic identity credentials retain legal primacy over digital ones? • In legal identity systems where biometrics play an increased role, with increased presence of biometric data, does the private sector think that identity variables such as name and gender will become more, or less, important to both individuals and states? What is the implication of technological development on data collection?
<u>SESSION 5:</u> **International identity data sharing and granting of access of foreign states to sovereign identity databases** (60 minutes)	1500 – 1600, *Facilitator, Dr. Emrys Schoemaker, Caribou Digital*	• Does the private sector expect that there will be an increase in intergovernmental agreements to access core national identity databases to verify the 'breeder identity tree' of an individual's credentials? • Will migration – and the need to apply appropriate tax regimes based on residence –

		mean more intergovernmental identity data sharing? What are the implications for digital solutions? • Will increased digitalization of civil registration credentials (e.g. marriage certificates) lead to greater recognition across borders, i.e. without 'official translations'? Will/should they be added as data fields to digital passports?
Break (10 minutes)	1600 – 1610	
<u>CONCLUDING DIALOGUE:</u> **Is there an ideal future national and international legal identity eco-system?** (80 minutes)	1610 – 1730, *Facilitator, Mr. Naman M. Aggarwal, Access Now*	If the private sector was now asked to design the 'ideal' legal identity system, from scratch, covering the full life cycle from birth to death, what would it look like? **Would these features appear in such a system?** a) State monopoly on ownership and management of the system and data? b) Biometric data as the primary identifier? c) Birth-to-death management by the same body? d) A public-private-academic-civil society 'national identity authority'? e) Unique identity across systems or multiple identities across different functional use cases? f) Right of individuals to pro-actively change or hide identity variables from the state? g) Right of individuals to opt-out?

<u>Sessions 1-5 adopted the following format:</u>

- Facilitator introduced the session (5mins)
- 2-3 speakers from the private sector make initial comments (3mins per person)
- Roundtable discussion (35-55mins)
- Summary by the facilitator (5mins)

A citizen receiving his new national identification card in Comayagua, Honduras, March 2021 (photo: UNDP Honduras)

2. Contextual Background

Everyone has the right to 'legal identity,' i.e. the right to be recognised as a person before the law, as enshrined in Article 6 of the Universal Declaration on Human Rights and several international human rights instruments.[1] However, hundreds of millions of people continue to live without valid proof of legal identity, with an estimated 166 million births unregistered.[2] A fully functioning system for the universal registration of births and deaths, essential instruments for conferring legal identity, is lacking in almost half of the world's countries.[3] In order to close the global identity gap, a UN inter-agency task force, the United Nations Legal Identity Agenda Task Force (UN LIATF, co-chaired by UNDESA, UNDP and UNICEF) is working towards the objective of reducing the global identity gap by over 300 million by 2025.

The Task Force is cognisant of the enormous expansion in the use of digital technologies in civil registration and in the management of peoples' identities by UN Member State governments in recent years. This includes developments such as the digitisation of databases and issuance of national identity cards/numbers (as part of the national identity register/national population register process) to adults (and some younger teenagers) in over 130 Member States. However, it also includes more recent developments such as:

- The capture and de-duplication of biometric data (usually fingerprints but also recently iris and/or facial recognition data) in order to ensure uniqueness of a person's presence in an identity database;
- Increased use of biometric data as a means to identify or authenticate a person's identity in order to access many public services;
- Increased digital 'interoperability' between different government databases (e.g. social security, taxation, driver licensing) via either 'above water' markers (such as unique ID numbers, issued to and known by each person) or 'below water' digital markers (not communicated to the person), to help notify different state agencies where the same person is registered for different services;
- Use of digital legal identities to access public (and some private) services online;

---

[1] *1948 Universal Declaration of Human Rights, Articles 6 and 15; 1951 Convention on the Status of Refugees, Arts 25 and 27; 1954 Convention on the Status of Stateless Persons, Arts 25 and 27; 1961 Convention on the Reduction of Statelessness, Arts 1-4; 1969 International Convention on the Elimination of All Forms of Racial Discrimination, Article 5(d)(iii); 1966 International Covenant on Civil and Political Rights, Article 24; 1979 Convention on the Elimination of All Forms of Discrimination Against Women, Art 15.2; 1989 Convention on the Rights of the Child, Arts 7-8; 1990 International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families, Art 29; 2006 Convention on the Rights of Persons with Disabilities, Art 18.* The right to personhood before the law is non-derogable—meaning it is c*onsidered such a fundamental human right that it can never be restricted nor be suspended, even in an emergency.* Under the *1966 International Covenant on Civil and Political Rights,* Art 4 (2), non-derogable rights are: the right to be free from arbitrary deprivation of life; the prohibition of torture and other ill-treatment; the prohibition of slavery, imprisonment for debt and retroactive penalty; recognition as a person before the law; and freedom of thought, conscience and religion.

[2] UNICEF (2019). 'Birth Registration for Every Child by 2030: Are we on track?'

[3] ID4D Dataset. The methodology used to calculate these data is the subject of ongoing discussion between the UN and the World Bank.

- Use of third-party private sector actors (such as banks) to verify physical identity credentials and issue digital credentials, under licence or authority from the state, for public service online access;
- Issuance of digital certificates either in place of, or an addition to, paper or plastic credentials such as birth certificates, driver licences and national identity numbers;
- Pilots in using distributed ledger technology as the system architecture for national ID schemes.

Less prevalent have been adaptations in the institutional governance of civil registration and identity management. With some noticeable exceptions, the broad trend across the world appears to remain that civil registration of major life events (primarily births, deaths, marriages, divorces) has remained under the control of local government structures such as mayor's offices and municipalities/communes. Management of national population registers or national identity registers (with or without the issuance of national Identity cards) has largely been placed under the authority of either a central ministry (such as an 'interior' ministry) or the police, or a national body created specifically for that purpose (e.g. a 'unique identity authority' or a 'national registration bureau').

Challenges

'Centralising' national identity registers under the control and management of one state ministry/agency, while maintaining decentralised civil registration, however, tends to result in fractured systems and less than universal coverage in either system, where:

- Birth and death registration are treated as standalone 'life events' (rather than the beginning and end of a seamless, holistic management of a single identity);
- Adult population registers (most schemes tend to start at either the age of 16 or 18) are populated with countless numbers of young people whose identity cannot be accurately verified when they enter the system (as they often enter without a birth certificate), and where deceased people can only be removed with great difficulty (thus resulting in bloated registers with ever-increasing numbers of deceased persons).

'Merging' civil registration with identity management systems such as national population registers, however, brings its own challenges and may not be suitable for many societies. For example, one legal identity derived from a 'source' legal identity (e.g., birth certificate or national ID), which could be used across all state functional identity systems (e.g. voting, driver licensing, social security, tax) is financially cheaper, more institutionally efficient and helps combat identity fraud. It also creates a 'single point of failure', however, and presents a target for hackers. It also allows for easier surveillance and profiling of citizens by autocratic governments. Conversely, having multiple, unlinked functional identities that are separately entered and verified across different systems may potentially be more secure. They are financially and institutionally unsustainable, however, and create easier opportunities for identity fraud.

These issues and debates, many of which have been around for decades, have been added to by a newer series of challenges. For example, the efforts of some digital rights groups in

recent years have raised profound questions about where the boundaries should lie between:

- The state's right to impose identity variables on an individual within an identity system that the individual may not recognise (such as religion or sex as recorded at birth), and;
- The right of an individual to demand that the state recognise, in identity systems, elements of identity centrally important to their sense of self (e.g. gender or ethnicity), on the sole basis of their self-declaration.

These issues will become even more complex as identity management "internationalises" further in the coming years. The COVID-19 pandemic has dramatically increased remote working, for example, a noticeable amount of which has seen people work remotely from foreign locations. Expansion of 'digital nomad visas' will no doubt increase in the post-pandemic world. This will be coupled with an anticipated mass migration from the Global South to the Global North in the coming decades, where an increasing proportion of people will likely make their living – both temporary and permanent – in foreign countries. Subsequently, a larger proportion of the global population will live with legal identities issued by a foreign state, and these increased migration flows, particularly seasonal or temporary, may render concepts of 'permanent residence' obsolete. In turn, this will lead to inevitable discussions as to how foreign governments can, or should, be facilitated to access identity management systems other than their own, to both:

a) verify a person's identity and their identity history, and;
b) document economic activity conducted in different jurisdictions so as to apply appropriate taxation regulations.

How can, or should, technology influence these debates? These were some of the issues that each of the Roundtable sessions were designed to address.

Registrar and a Lenca woman showing receipt after registration from a new ID in Esperanza, Intibucá, Honduras, Sept 2020 (photo: UNDP Honduras)

3. Session Discussion Summaries

3.1 Welcoming and Opening Remarks

178 participants were welcomed from the private sector, governments, academia, development partners and UN agencies, who joined from more than 45 countries and regions. It was emphasised that dialogue about technological progress and its implications for governance, specifically legal identity systems, is important for the UN. Matters related to identity, and how it is documented by UN Member States, are primarily governance issues surrounding the relationship between the state and the individual.

> **"Digital transformation and governance are critical for governments to offer inclusive, transparent, and efficient public service to their citizens. Legal identity is fundamental to access public and private services and the importance of digitisation of legal identity systems is indisputable. It also has various human rights implications and it is incumbent on the UN, and all stakeholders, to have discussions about the human rights implications and the policy aspects."**
>
> **Ms. Sarah Lister**,
> Director of Governance, UNDP

It was acknowledged that with the sophistication of digital solutions (and the increasing use of machine-learning technology), governments are able to collect more data (including biometric data) about their citizens and foreign residents. While this will continue to enhance service delivery and make public services more convenient, it will also change the relationship between governments and people, as well as the relationships with other actors, including the private sector.

A National Registration Bureau (NRB) officer assisting a citizen to collect her national ID card while others patiently wait their turn in Malawi (photo: UNDP Malawi)

Registrars checking online citizen ID status before delivery in Danlí, El Paraiso, Honduras, March 2021 (photo: UNDP Honduras)

3.2 Ownership, Control and Management of Legal Identity Systems and Data – Part 1

Ownership – Does the private sector think that UN Member States will, or should, outsource any elements of **granting** legal identity (via birth registration or registration in national ID schemes) in years to come?
Management – Does the private sector think that UN Member States will, or should, outsource specific elements of legal identity **management** (e.g., digital keys issuance to access services online) in years to come?
Management – Does the private sector think that there are alternatives to centralised state management of legal identity that would elicit greater public trust? How could civil society, academia, digital rights advocates, and private sector innovators play a greater role?

The facilitator introduced the questions (outlined above) and emphasised that the discussion should focus on legal identity, a sovereign right granted by the State and traceable from one's birth. By asking "What is the role of the private sector?" it questions whether the private sector will be participating, or in some individual's views, 'interfering', with the sovereign right of the state.

Some of the points raised, in the course of the discussion, were as follows:

> **"The role of the State actors is a credentialing one. In the past, it was mixed with the idea that the State had to produce a card, they had to produce a document, and they had to produce a necessary support that was needed in order to carry that identity. In the future, because digital identity is now accessible and because self-sovereignty is now feasible, maybe the role could be shifted. Maybe the State is moving in a direction where they accredit traceability."**
>
> **Dr. Joseph Atick**
> Executive Director, ID4Africa

It was acknowledged that the private sector has a role to play in legal identity due to many factors: (i) digital transformation of society, which has mostly been driven by the private sector; (ii) the COVID-19 pandemic, which has devastated numerous government processes and created a role for the private sector; and (iii) new technological platforms, like blockchains, which are causing people to relook at the classical paradigms by which governments register, declare and accredit individuals.

Several paradigms where discussed:

- The 'Classic Paradigm', where legal identity is in the hands of the Government, and;
- 'Alternative Paradigms', including:
  - A data driven model led by the private sector;
  - A self-sovereign model where the individual has more control.

Classic Paradigm

The classic model for legal identity is one where a government solely grants legal identity to its people and the private sector supports what the government is doing to achieve this. For example, linking an individual's SIM card with their national ID number and motivating individuals to register for same.

> **"While we believe that the goal of ensuring legal identity for all should sit with the governments, that does not mean that governments cannot partner, or licence, private sector players to support them, while at the same time operating within defined frameworks, terms and conditions."**
>
> **Mr. Yiannis Theodorou**
> Senior Director, Digital Identity Programme, GSMA

Three examples were given of how Public-Private-Partnerships (PPPs) are taking place to support the legal identity journey in Nigeria, Pakistan, and Tanzania.

Nigeria – The Nigerian Government has recently partnered with mobile telephone operators to support a new national ID enrolment scheme. It is estimated that the majority of 100 million Nigerians who do not have legal IDs will be enrolled by partners who are mobile telephone operators.

Pakistan – Mobile Network Operators (MNOs) have worked with the Pakistan Government and UNICEF to support digital birth registration, allowing over 3 million new born children to be registered via MNOs. This has shortened the previous paper-based birth registration process from one that used to take two to three months; to a mobile-enabled digital model that now takes a couple of days (or even hours).

Tanzania – Mobile telephone operators have worked with the Tanzanian Government to reform the digital identity framework from a traditional paper-based birth registration process to a mobile-enabled digital birth registration process.

Alternative Paradigms

It was questioned whether the classic model could be turned around, and if there could be:

- **data driven models**, in which the private sector could lead and the Government could follow by granting approval after due diligence was carried out?
- a paradigm shift with a **self-sovereign model**?
- a balance embracing both of these models?

> **"The notion that one central authority has complete control over identity is something that worked when there was no digital space, when there was no digital economy, when there was no technology that could sit in the hands of anyone as long as they had the knowhow."**
>
> **Ms. Titi Akinsanmi**
> Public Policy Lead, West and Francophone Africa, Google™

It was recognised that the traditional model for birth registration has changed. For example, Nigeria used to have the model where birth registration was dependent on going to a physical location, if the parents were able to get there. Now there is a new digital national ID scheme which is supported by mobile telephone operators. While it was acknowledged that this provides access to some individuals who were not able to register in the past, it was also recognised that a significant number of people are excluded, as many Nigerians do not use mobile telephones and hence cannot be engaged in this way.

> **"Context for legal identity really matters, as identity is an increasingly fluid concept which changes according to the context and needs of the user. It can be linked to the similitude of the person's persona; where at different times and in different circumstances, the persona we present to the world varies (on and offline). It is a multi-faceted concept shaped at different times by our gender, our race, our background, our status. The question of the 'right' to present these as legal identity changes. The question should be: Should core legal identifiers be utilised only when needed? Could we work towards a consensus based on a definition of what legal identifiers would be relevant to share?"**
>
> **Ms. Titi Akinsanmi**
> Public Policy Lead, West and Francophone Africa, Google™

While it was proposed that society should remain within that classical model, as much as possible; where legal identity resides with the Government, and they control it; it was proposed that the classical model could be revised to one where different forms of legal identity sit in different spaces; and individuals are placed at the centre of decision-making regarding the information they would like to share, based on the identity the individual connects with.

It was noted that we are facing interesting questions, both as national societies, and as a global society, about how we organise belonging and movement.

> **"Identity pre-exists law. This is materially evident in the fact that stateless people and people without legal identities exist. We can think of law as a 'social operating system' that makes people visible and legible to the state. But, just like software, the legal operating system isn't evenly distributed – which is why we are convening to discuss what to do about the hundreds of millions of people without legal identity. Law has limits. We wouldn't be having this conversation if the legacy means of ensuring identity were universally adopted and working for everybody equally well."**
>
> **Ms. Natalie Smolenski**
> Senior Vice President, Business Development
> Hyland Credentials

It was argued that one of the benefits of law is that it provides a method of arriving at the truth. There are, however, other methods of arriving at truth, such as; cryptographic, (which is a method employed by blockchain technology to validate the truth of a ledger), and by proxy, the truth of digital identity; scientific methods of arriving at truth; and other social methods of arriving at truth.

It was also argued that we are at a historic moment in time, where these various epistemologies, these various ways of knowing, are coming into direct contestation in ways never before experienced in human history. It was commented that it is "*an exciting time, rife with many possibilities*".

Emerging from the discussion was the notion that when we talk about legal identity, we are talking about recognition of identity by the social operating system in a country, that is lawful for specific purposes including:

i. the delivery of government services and benefits;
ii. for legal protection of individuals;
iii. for enfranchisement of the person;
iv. for a kind of social platforming that creates a basic trust layer – the category of citizen.

The question then becomes - how does that social designation get proven and transported digitally? There are many vehicles for doing this, some which can be provided by state actors; others which can be provided by private actors. It was noted that the legal identity designation which is visible by the State is not comprehensive of human identity at large and is not the base condition for human identity itself.

It was proposed that identity is fundamental to human social personhood and that broad domains within identity can be considered as a **public good**. It was stated that this is

beneficial to both public and private sectors, in the same way that creating an open web infrastructure through TCP/IP has been a boom for the private industry and governments around the world.

> **"Today we are fortunate to have digital tools available that can extend the reach of social operating systems. But the way we implement those tools will determine the possibilities they enable and foreclose for the people of the world. That is why a trustworthy and empowering digital identity system must do two things: (i) enable issuing institutions to attest to claims that are their prerogative to attest; and (ii) give data subjects control over when and how those claims are used and verified. This gives everyone access to verification of legal identity and when they need it (for example, to travel or receive government services) without creating ever-more bloated databases of user data that are vulnerable to exploitation and attack. In my view, open standards for verifiable credentials are the best way to achieve this vision in a collaborative and interoperable way."**
>
> **Ms. Natalie Smolenski**
> Senior Vice President, Business Development
> Hyland Credentials

It is also important to note that other participants in the discussion disputed that identity is a 'public good' stating instead, that identity is private to the individual.

Definition of Legal Identity

The definition of legal identity was also discussed. According to the UN Operational Definition, approved by the UN ECOSOC and the World Bank, "*legal identity is defined as the basic characteristic of an individual's identity (e.g., name, sex, place and date of birth) conferred through registration and the issuance of a certificate by an authorised civil registration authority following the occurrence of birth*."

It was noted that a critical part of this conversation revolves around the ***proof of legal identity***, which is defined as "*a credential, such as a birth certificate, identity card or digital identity credential that is recognised as proof of legal identity under national law and in accordance with emerging international norms and principles*." This proof provides flexibility for the credential to be issued by a non-state entity, so long as it is recognised in law.

"There is no such thing as 'one identity'. When we talk about identification, there are many ways by which we can assert our identity for different purposes. The reason the State had the monopoly on identity management in the past is because they had the infrastructure and the platform. They were organised to do this. The State accredits individuals. They attest that this person has certain rights because the person is traceable to certain birth events. The State is an independent authority recognized by the law; it's not necessarily the identity management platform. The identity management platform could be done by the private sector; it could be done by the Government; it could be done by non-governmental organisations; schools, universities; etc."

Dr. Joseph Atick
Executive Director, ID4Africa

The Government has one obligation which the private sector does not have – legally the Government is supposed to register everyone that is born in its country. In the absence of social civil registers, the source of truth is reduced to attestations. For example, in countries like Somalia, where it is necessary to prove that a person was born in that country, and multiple witnesses are necessary to attest to this. The electoral commissions are confronted with this issue where they have to rely on the community, in the absence of a birth certificate, which is deemed in many countries as the source of truth.

"In the jurisdiction I come from, which is Ghana in West Africa, I believe that identity should start from birth and end at death. With this said, the hospital, or birth and death institution, have a huge role to play when it comes to identity".

Mr. Precious Baidoo
Digital Frontiers Institute, Ghana

During the discussion it was argued that perhaps the private sector may be able to offer a better mechanism to provide the source of truth since they have developed the social connections and networks and they can help people get attestations rather than needing to physically travel to local communities to get letters signed by notables.

"The private sector has a significant role to play in enabling government to rethink and understand in a different way, how they need to be able to manage legal identity."

Ms. Titi Akinsanmi
Public Policy Lead, West and Francophone Africa, Google™

It was recognised that in the same way the internet has come to shift boundaries, and remove boundaries, the system defining identity has also shifted. Governments used to be the full gatekeepers and knowledge holders of birth registration, but birth registrations sit very much on platforms and structures that are technically developed and owned by the private sector.

There are two important things about management of legal identity: (1) standardisation (contextually relevant standardisation) because what will work in the United States of America will not work in many other countries, for example, because the ability to access the infrastructure that enables the registration is different; (2) willingness to sit at the table with a range of stakeholders, including those in the private sector, and develop a trust framework; which ensures that the identity being presented, or managed, is one that is accepted.

Historically, the notion has been that an individual is born in a particular place, and therefore their identity is based on the person's place of birth. This is something that will shift. A person can be born in one country and live in multiple other countries during their life. Some of those countries will grant citizenship or permanent residence. In as much as the blood lines are linked to a person; the identity the person chooses to present in a social sphere differs as it could be linked to places they have chosen to live, or other factors.

> **"To the extent that it is possible, private sector will play more of a role in terms of management but that does not remove the sovereignty of the State – and that's the biggest fear for many people and where the contentious conversation sits.**
>
> **Ms. Titi Akinsanmi**
> Public Policy Lead, West and Francophone Africa, Google™

The platforms are already there, the attestations could come from the community, and then the State could come in and provide accreditation.

Role of Governance in Legal Identity in the 21st Century

One of the most interesting conversations that is happening is about how governance is changing in the 21st Century. In other words – what is the social mandate of different human collectives? The reason States have historically had a monopoly on legal identity is because they have a monopoly on the enforcement of law. It makes sense that the institution with which individuals have a social contract to protect them from harm is also the same institution that is the most legitimate attestor of an individual's legal identity.

The power of private actors in some areas, however, has come to rival the power of the State. For example, in the United States of America, some private sector companies are beginning to incorporate governments at the municipal level, which allows them to directly exercise

State power. The question for some is not whether this is bad or good, but whether we are going into these social arrangements with the understanding of what that social contract is between the different parties in the agreement.

In the case of a software provider that contract is often an explicit legal agreement that has been negotiated in exchange for money or an adhesion contract for the free use of service, where the end user does not have much input.

> **"We are in an interesting place now where the efficiencies of the delivery of services by software providers places them in a State-like relationship to their users, but without the political history of contestation and a social contract that binds the power of the State in state society relations."**
>
> **Ms. Natalie Smolenski**
> Senior Vice President, Business Development
> Hyland Credentials

The private sector should not have the authority of fully empower individuals, for example. While Google™ could empower an individual to do certain things, they could never empower an individual to vote, or empower an individual to have a passport. As long as the laws make it very clear what the State responsibility is, and they are not going to outsource it, it does not remain an issue. Diversity in identity is going to be in digital format, but when we come back to the issues which are dictated by the law, we still see the State as the main actor that needs to empower individuals.

An example of a successful public-private legal framework for delegation of sovereign powers was given – which is the notarial system that exists in most countries in some form. By means of the notary, governments delegated certain limited aspects of sovereign powers to a regulated system of distributed trust. It was proposed that this could be done with aspects of digital identity and legal identity as well.

Uniqueness of Identity

We are converging at a point where we are mixing ***digital identity*** and ***legal identity***. It was noted that *legal identity has to be unique*, but *digital identity does not*.

Legal identity has to be unique because it confers certain benefits on the holder, and more importantly, legal privileges and rights. Fundamental to many laws in human society, there is a uniqueness of those rights, for example, an individual can only vote once in a single election (but not more); receive benefits once (not more); pay taxes once (and not zero). That does not mean that a digital identity has to be unique. There could be one legal identity, but multiple digital identities residing in different contexts. It could be sectoral for example, with different digital identities in sectors such as health or banking.

"Legal identity, in my perspective, is a tiny case of space of all identities that we could own and empower ourselves through these means. It doesn't mean that legal identities are undermined by the multiplicity of the digital identity, it just means that there is no need that it would be universal. The context is so important, which is something all of you have been pushing for, which is saying – depending on who a person is interfacing with, different aspects of that persona could be presented, and therefore those could be different identities. The human is unique, but the representation doesn't have to be.

Dr. Joseph Atick
Executive Director, ID4Africa

The context brings back home the different manifestations of our identity. It was argued that every individual is unique in real life and the representation of the individual should be unique. One participant summarised that the ideal digital identity model involves people controlling a wallet of different credentials, issued by a multitude of authoritative sources (i.e., foundational ID systems, driving licenses, passports, etc.) with the ability for relying parties to verify those credentials and to determine if that person is unique within that relying party's context.

Argument for Single Identity

The idea of a single unique identity, that is universal, becomes the basis for establishing and verifying the identity of individuals and for issuing functional ID documents including bank cards, health insurance cards, etc. Using a universal, lifetime unique identity helps to harmonise an individual's profile across different databases, which lessens the opportunity for fraud associated with multiple identities.

A person could have various tokens, or attributes, which allow them to access different services (e.g., health services), however these attributes would all connect to a single (one person) centrally issued identity. In this model, verification is completed by the State, but access to resources can be undertaken in a decentralised manner.

"My view on identity is that there has to be one identity for a human. If we take the structure of how digital identity came into being, it was essentially created because tech companies, mostly playing in the digital world, were created to bring their services to the world, which is a great effort. However, the human has so many identities out there in the digital world, we need to combine

them under one single umbrella. The State has to be the root for the issuance of identity, and when looking at the concept of how systems are managed, there are attributes associated with that identity. We have to create a structure where some attributes are changeable and some attributes are not changeable. We should look at attributes as tokens that are sub to the primary identity of a user, but ultimately there should be one single identity. "

Mr. Vikas Malhotra
Founder & CEO
WOPLLI Technologies
(Previously with-Microsoft, Cloud Services)

Argument for Diverse Modes of Identity

Typically, the concern with providing a unique identity is linked to efficiencies relating to the delivery of services. If you have multiple citizens with the same name, it is easy to confuse them in a database, then it can be unclear how to attribute legal agency and how to distribute benefits to a specific individual. Having a unique identity is both functional and practical. Where you are a State, or a corporation, or a church, or any other type of organisation, efficiencies have to be created in the services which are being delivered to its constituents.

That very multiplicity of organisations suggests that you do not necessarily need to have the same identity, or identifiers, across each of these platforms and, in fact, most people do not. The legal uniqueness of identity is a very special case of identity. There is a broad universe of cases that can go beyond that.

It was suggested that a universal model could be adopted as a best practice guide, but countries should be able to deviate from it, as appropriate, to suit local needs.

"I disagree with this idea of having a unique identity. In India, we have multiple IDs. There is a functional ID for voting; there is a function ID for a driver's licence; there is a birth certificate; a passport. There are multiple forms of identities and none of them are unique. I am human and am unique, but the manifestation may not be unique. The idea of having one single identity does not make sense. We need to push for diverse modes of identification."

Mr. Srinivas Kodali
Researcher, Free Software Movement of India

Immutable versus Mutable Identifiers

The concept of mutable (the ability to change) versus immutable (something that cannot change after it is created) identifiers was discussed. It was noted that legal identity is anchored on immutable aspects of an individual's persona.

> **"Legal identity is the sum of data that doesn't change about an individual. There are some things about identity that cannot be changed, such as location of birth and date of birth. They are facts. Most legal frameworks rely on these immutable aspects of the framework."**
>
> **Dr. Joseph Atick**
> Executive Director, ID4Africa

It was proposed that an easier position to adopt, rather than stating that all control and management should remain with the State, would be one where immutable characteristics, which are unique to an individual, be presented, as and when needed, to access services, products, and exercise rights as a citizen (e.g., being able to vote).

Mutable Characteristics

It was also noted that legal identity is not static as an individual's identity changes over a lifetime. A person is born, and a person dies, and the events that happen in between may lead to changes in their legal identity. For example, a woman's name may change if her marital status changes, or a person's gender may change. Whilst changes may occur, the individual who experiences these changes remains the same even though their legal identity has changed.

> **"We are saying that we need to have standards for identity to be unique and universal. I think, by pushing the idea of a universal standard, you are taking away the power from the individual and giving it away to the nation states, which we individuals have fought for".**
>
> **Mr. Srinivas Kodali**
> Researcher, Free Software Movement of India

It was noted that identity systems often lag behind the changes an individual makes to his or her identity. Getting changes registered is often considered too cumbersome so individuals do not make them. However, it was also recognised that legal identity grants rights, benefits and opportunities to individuals, and technology is an enabler making this happen. Where the private sector can contribute, is in their ability to add attributes ensuring that the identity is 'real.'

For example, in many countries where people were unable to access brick and mortar bank accounts, but where governments and central banks in those countries allowed for private sector-led digital entities to be accepted, then individuals were able to access services, including benefits from the State, as a direct result of digital financial inclusion.

> **"When, and if, governments verify or accept private sector-led attributes around someone's identity, that's where you can see people, who were in the past underserved, be able to access services via digital means through the private sector."**
>
> **Mr. Yiannis Theodorou**
> Senior Director, Digital Identity Programme, GSMA

Legal Identifiers

The position was stated that we speak of ***legal identifiers***, which means there are certain **immutable characteristics for each individual** that need to be tested and trusted and that the relevant characteristics be presented, depending on the context of the service, product or engagement that the individual wants to have. The notion of having unique legal identifiers, as managed by the State, seems more palatable.

Immutable characteristics are things that are unique to an individual and are being collected by the State, or agents of the State, that enable an individual to access and to engage with services and benefits that are provided by the State. However, the question arises, should States have access to all of this information? It was agreed that context matters. In spaces where one is feeling unsafe, for example, there are genuine questions as to why the State should have access to all of an individual's biometric data.

How much personal information should be collected to create a complete 'legal identity'?

One of the participants asked if there was a reasonable limit to the amount of personal information that should be collected to create a complete 'legal identity' profile of an individuals and prevent over-zealous authorities from collecting excessive details, such as DNA profiles, location data and other personal information?

While there is no best practice model, it was acknowledged that legal identity should be inclusive, efficient, and secure:

- inclusive; meaning that identity should be without discrimination; and
- efficient; meaning that it should be affordable and sustainable; and
- secure in that it guarantees a level of confidentiality, and safety, ensuring information is not shared without consent from the individual.

The example of the Lesbian, Gay, Bisexual and Transgender (LGBT) community was raised in reference to concerns relating to security. If an individual is entering a zone, where is it dangerous be a member of the LGBT community, for security and non-discriminatory purposes, it is important that certain information is not shared.

It was, therefore, acknowledged that if a State wants to enforce standardised identity protocols, then it has to be in a position to protect the individual. The witness protection

programme was cited as another example. The State has access to unique, and changeable, information about an individual and that individual has to trust that the State will maintain security and confidentiality in relation to their identify. The role of the State, or public sector, should be to provide institutions with the infrastructure to make identity available.

Role of the Private Sector in Legal Identity

What can the role of the private sector be to support legal identity management and enrolment?

It was stated that those in the private sector are the enablers who can make a digital identity viable, where technology acts as a huge catalyst making a digital identity available to everyone. It was also positioned by GSMA that the issue of **reach** is something governments in developing countries have lacked. Mobile network operators have nation-wide reach and experience in dealing with customers face-to-face, and they can play a great role in facilitating issuance and enrolment of whatever the country's national identity system is. The private sector has access to additional data and attributes about individuals that can strengthen their digital presence, these could be added to the minimum level of credentials required to provide a unique digital identity.

Does the private sector, think that there are alternatives to centralised State management of legal identity that would elicit greater public trust and transparency?

The private sector does not speak with a unified voice on this. There are many within the private sector who would like to have the same amount of control over legal identity that governments do. However, there are others who explicitly renounce and refuse to accept that control, stating that they do not want any company managing legal identity. There could be a role for facilitating the verification of legal identity in a decentralised manner where the source of the truth could be centralised.

Conclusions

While various paradigms were discussed, it was recognised that:

- Legal identity is a sovereign human right.
- The role of granting legal identity should be primarily in the hands of governments and the private sector should support governments.
- Context matters in the way identity is viewed and used because identity is dynamic over the life cycle of an individual.
- Uniqueness of identity is applicable in a legal context, but not when it comes to digital identity, where there can be a multiplicity of identities in a digital context.
- There is a complementary role between the public and private sector. The traditional model, the dominant model, does not have to be completely revised. There are situations where outsourcing credentialling to the private sector makes sense, when

it accompanies the traditional model. The private sector could also verify legal identity in a decentralised manner, but collection of data could be State-centralised.

- We can live with centralised legal identity, but we need improved ways to allow control over verification so that the owner of the identity can choose to engage and participate and provide different identifiers, depending on the context and task.

- Three key ingredients that have contributed to successful public-private-partnerships in the legal identity space are:
  - Progressive governments with clear digital manifestos that have been developed through an open and consultative process;
  - Legal and regulatory processes and policies that are robust, especially in relation to privacy and data protection that engender trust in whatever the legal identity platform is;
  - An appreciation by governments that the private sector can bring value and innovation to the legal identity space.

- Legal identity comprises of data which, for the most part, does not change about an individual.

- Legal identity has to be unique, but digital identity does not.

- Legal identity is less effective when there is little trust between society and the State. This is a political problem which drives people to adopt forms of digital identity that are not State-managed.

- For people to trust the State control of identity, the State must offer safety, security, inclusiveness (no discrimination) and efficiency (affordable and sustainable)

- The private sector does not have one unified voice on matters related to legal identity.

- Identity is fundamental to human social personhood and the broad domain of identity can be considered a public good.

- The private sector are enablers to make digital identity viable and legal identity accessible to more individuals.

3.3 Ownership, Control and Management of Legal Identity Systems and Data – Part 2

Control – How much control can, or should, an identity data subject (citizen or non-native resident) reasonably expect to have in changing, editing or deleting certain identity data (e.g., such as name or sex/gender), or an ability to limit access to it, by public bodies in years to come?
Control – What role, if any, will decentralised IT architectures (such as blockchain) have in organising / archiving civil and national population registers in the years to come?

The facilitator opened the session highlighting that control is the topic of the second roundtable. The facilitator for this session was a representative from the Secure Identity Alliance (SIA), a private sector member organisation. Speakers in the second session were member companies of SIA, and while not policy makers, they have experience of implementing in the field and spoke in order to share pragmatic approaches to addressing the global identity gap in a way that protects personal data and privacy.

> **"The 'identity industry' that I represent draws on experience and expertise from hundreds of years in the field at the service of Governments and citizens, enrolling populations, producing and managing proof of identities, designing systems and architectures for both the physical and digital world, focusing on the security and inclusion of populations, protecting their personal data and privacy. Although there is a convergence of views, the industry competes on innovation and services according to international open standards. The industry has been constantly evolving and managing technology shifts. It's not about physical or digital; our DNA is security, privacy, and interoperability.**
>
> **We are not policy makers, but we know how to implement and make the solutions work in the field, the way to configure them, the way it is used. The speakers in this panel are member companies and we are very happy to share with policy makers pragmatic approaches and returns of experience to solving the global identity gap in a way that protects personal data and privacy."**
>
> **Ms. Stéphanie de Labriolle**
> Marketing Director
> Secure Identity Alliance (SIA)

The facilitator reviewed the results of the survey completed by participants before the roundtable commenced, and highlighted that an overwhelming number of people thought citizens should have more control of their data. With digitisation, more attributes and identity data are being shared, willingly or not, with various organisations, not only governments, but also those in the private sector. Two thirds of the respondents in the survey said that decentralising identity is a way to address the issue of control. Following this introduction, three experts from the identity industry were invited to share insights on the survey results.

Systems Software Perspective

> **"I was struck, in terms of the numbers that the consensus was in favour of citizens maintaining a very substantial level of control of their own data and also to minimise the role of government to one of management."**
>
> **Mr. Calum Bunney**
> Systems Software Product Manager, HID Global

It was argued that there are some identity decisions made by individuals with control, and other decisions which are made without their control. Individuals can make decisions about their private lives; however, they also make decisions about their children and descendants in core civil registration. Over the last 15-20 years, in the world of medical ethics, for example, there is a lot to learn regarding the issues of same sex parents and in vitro fertilisation. There are interesting parallels between what is thought of as 'control' in the medical ethics space, and the identity space.

> **"One of the roles we have as technical suppliers in this industry is to make sense of policies in the context of the real world. That doesn't mean we force people to do things our way. It means we engage in the nitty gritty debate with customers as to how to make things work in an acceptable way and we adapt to understand what controls are in place that should be used. A very good example of that would be the controls around GDPR.[5] Most of us now are very well conversant with GDPR and how it applies to our technologies and the processes around identity that we support. We, as suppliers in this industry, will continue to adapt, in a like way, as**

[5] The General Data Protection Regulation (GDPR) 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

the debate evolves with policies that are informative and interpretable. We are kind of interpreters in the discussion."

Mr. Calum Bunney
Systems Software Product Manager, HID Global

It was also argued that there are different layers of data, and we have to think about controls around core data for identity. But that should be separate from the data that relates to civil registration and support of other important attributes, such as someone's name or change of name, adoption, etc. There are also logarithmic elements which should be considered, as identity data has the potential to grow exponentially, or out of control, within our lives.

The OSIA Standards Group[6] has been working in the context of civil registration and the way it supports federated identity management. In that context, OSIA thinks of there being a control boundary between the centralised owner of the core identity information and organisations who would like to leverage the truth of it, but not necessarily represent it. Identity federation has made good progress in recent years in providing tools to allow users to make private and personal decisions about sharing identity, such as OpenID Connect, which empowers the attribute owner in the identity space.

Systems Integrator Perspective

The views presented in this section are those of a systems integrator who works on government projects, cybersecurity, and digital identity. It was suggested that globally there seems to be a consensus of some level of trust in government structures to manage or assert a minimum legal identity. However, in recent years, since many people are online and have access to data, individuals want to retain some control of part of their personal data, and identity is part of their personal data.

"Identity and data are inherently linked to each other and based on a trust relationship. Citizens rely on governments to assert and protect their foundational identity, but also want to be able to decide which elements to disclose for specific use cases, provided by the private sector. Today's technologies allow to give control to the users in a secure and trustworthy manner. It's all about the right combination of privacy, security and trust."

Mr. Dan Butnaru
Senior Advisor, Digital Identity, Atos

Regarding degree of control, for example, which attributes or part of identity do individuals want control of – and why? Is it to hide, change or delete certain data? The notion of culture is very important, as each culture may have a different aspect of what should be considered

[6] https://secureidentityalliance.org/publications-docman/osia/165-osia-initiative-framework-en-second-amend-20-12-14/file

private data. In some countries, religion for example, will be totally excluded when it comes to considering what should be included in identity systems. While citizens would like to have control of certain attributes, it is important, but difficult, to define a minimum data set that defines an individual's 'public' identity. When we talk about identity, data and trust have to be considered as they are interlinked. If one part is compromised, there will be an impact on another.

Technology evolution is interesting and private companies are looking at how to use distributed ledger/blockchain technology as it is a way of being able to manipulate certain parts of data to use in different cases. But the value of technology can only be measured by usage. If the goal is for citizens to adopt a certain type of technology, they have to be able to trust it, which means education on how to use it has to be provided and it has to be secure to ensure trust.

Perspective from a Private Sector Company in the Border Control and Biometrics Space

Portugal invested very early on in the e-Government scheme focused on digitisation of society, incorporating digital credentials, with biometric data at its core. The scheme brought together an individual's unique ID with their social insurance, tax and driving licence. In 2005, Portugal envisioned that the initial level of digitisation would be based on a combination of attributes that would be used for legitimate purposes, and shared on a need-to-know-basis with different public entities over the lifetime of an individual. The purpose was to alleviate the burden of administrative work experienced by government agencies.

The events in the United States of America on 9 September 2001 and the Visa Waiver Programme in 2001, triggered Portugal to be one of the first countries to adopt a biometric passport. This is the first level of digital identity and credentials that can be looked at when starting to trade transactions, such as biographic data and basic attributes, which are trusted and given by governments when an individual is born. Use of biometric data became the 'new normal'.

These elements of the border control arena are foundational, to be able to control what can be responsibly done in the private and public sector to provide populations with fundamental rights to use their identity as they wish, in a given context based on two important elements; (i) a need-to-know basis; and (ii) a legitimate purpose basis. This means the transaction will have to provide a benefit, or service, from the public or private sector, and that the citizen should be able to utilise a set of attributes to be able to access these services. These are the necessary elements to ensure responsible identity usage.

> **"The future of digital identity, and above all, our collective responsibility for inclusiveness in providing a trusted identity to each and every human being on earth, will undoubtedly have to rely on governments' leadership in delivering a trusted chain of identity framework, where industry players can help build robustness and sustainability in the process of empowering**

citizens with the right to choose which identity credentials they can use for each context and regulatory frameworks. Biometric technology will be crucial to achieve this goal, among other responsibly-used technology assets."

Mr. Jean-Françios (Jeff) Lennon
Vice President of Strategic Sales & Global Partnerships
Vision-Box

Citizens should be in control of their identity. However, when it is time to comply with law enforcement, certain regulations, certain democratic-based elements of control that guarantee a person is who they say we are, should not be debated. In the session, it was stated that foundations and standardisation elements do not have to be reinvented. There are enough of these already in place for governments and the private sector to work collaboratively to define the future of digital identity.

How much control should a citizen have to change, edit or delete certain identity data?
It was argued that we should have concentric circles or layers of data; some data is out of our control, it is what we are born with. There are some things which are immutable, then there is the registration function, where a recognised agency with some centralised legal status, has the role of aligning that data with names, places, and attribute-based information. Moving outwards from the centre of the circle, we encounter circumstantial data with derived identities in the digital identity space, where there is debate about what data we should be able to change. As we move even further away from the centre of the circle, into other concentric circles, the discussion is not just about data, it is also about the binding and linking of that to perform functions in an individual's life, and what that data is used for.

"My feeling is that we should be focusing on, especially in the derived spaces, on making the jump from CRVS central registries into multiple digital identities, focusing on how to give people control over the linkages. That's why I like OpenID as a starting point, as it recognises the fact that controlling your data, and what attributes to choose to associate with a transaction, is something that is put under the control of the person."

Mr. Calum Bunney
Systems Software Product Manager, HID Global

Not everyone understands what a *self-sovereign wallet* is or what it does. There needs to be a level of education to help people understand what technology to use to control their data, as this is something not understood by everyone. Just like the debate about data use for medical purposes, it will take time to figure things out and put proper structures in place.

The real control of the citizen is the ability to give access to a specific portion of data that is required for a specific use case, without having to provide all data for all use cases. It's about

having a consensus on the minimum data set that is asserted by the Government for a citizen. For example, a citizen may not want to show their birthdate on all occasions, or their address or other information. A citizen should be able to give minimum information, if they choose.

What role, if any, will decentralised IT architectures (such as blockchains) have in organising archiving civil and national population registers in the years to come?

Blockchains allow both transacting parties, as well as the transaction verifier, to interact together without knowing each other. It also certifies transactions between stakeholders without storing or sending private data, so in theory, more elements remain in control of the citizen. If societies want to 'scale up' use of blockchains in identity systems, one key principle needs to be defended; identity and biometrics should be owned by an individual citizen and verified by the Government.

The purpose of blockchain, when implemented well, is not to store human-readable data, but to serve as a decentralised verification infrastructure for 'off-chain' data. Off-chain data is aligned to 'on-chain' data (generally hashes or digital IDs (DIDs)) which is achieved through the use of open cryptographic standards and protocols. It was noted that a blockchain technological approach will only be successful if people adopt the technology, implemented transparently and in a user-friendly way. Blockchain is important because it has a private key which can sign digital data.

Given all the parameters that society is exposed to in terms of population growth and the fact that over one billion people lack access to basic services, it is important to build a trusted chain of identity with unique identifiers which are owned by an individual. The fact that individuals already have DNA elements which are unique to them (ie: voice, face, finger, etc.) and given the fact that pure biographic data cannot be relied upon, biometric technology is likely to continue to evolve and expand in terms of its use.

Facial recognition will continue to divide opinion. While it 'sees someone as a human being' and it can be argued, in some contexts, it is less intrusive (fingerprint analysis has always had a more forensic or criminal association), there is always the challenge of combatting intrusive use of facial recognition via closed circuit television cameras (CCTV), etc.

> **"The Government should continue to play the role of identity brokers or service providers to guarantee you are who you say you are, to ensure there is no identity fraud, with an integrated approach of which biometrics or other attributes of your identity as an integrated approach. The Government is the sovereign party to do that, and the rest of society needs to sort out beyond this how we manage the rest."**
>
> **Mr. Jean-Françios (Jeff) Lennon**
> Vice President of Strategic Sales & Global Partnerships, Vision-Box

In the case of border and seamless travel, the 'end game' is about interoperability and being able to have a consistent experience at the border and throughout the entire journey, where digital identity confirms it is always the same individual. In a hybrid model, decentralisation would be the foundation leading to an individual possessing either a physical document with electronic capability, or a digital wallet where authentication and security is guaranteed from the issuing national government. For cross-border crossings, where multiple governments and stakeholders are involved, blockchain and ledger technology can play a role in signing transactions; in giving a trusted contract between the issuer, the holder, and the verifier. No identity or biometrics should be stored in the 'cloud'.

A good example of user control occurs in a federated architecture which prevents a service provider dictating the specific system, technology, or identifier used. It simply asks for authentication. If a high level of authentication is required, there could be biometrics, or cryptography applications linked to mobile telephone smart ID keys, which empower a user, because they can use technologies which work for them to validate their data.

An interesting area to explore is in the space of creating pseudonymous identities to avoid traceability, as with the use of usernames, there is a possibility that a person creates a thread or footprint, based on the continuous use of a name, even if it is an invented name. There is a tokenisation layer which needs to be explored here, and the debate is not yet fully mature.

While blockchain is one technology, other standards and working groups are emerging, such as the work of the *Decentralized Identity Foundation*, which works to give developers support and ideas of how to make technologies more user-friendly.

When it comes to storing decentralised data, there needs to be further technological evolution, as blockchain data is difficult to erase. Additionally, blockchains tend to operate across boundaries, so if it contains some sensitive data which is supposed to remain in one national country, it is difficult to achieve using blockchains.

Blockchain is one layer in a software stack that comprises the actual identity ecosystem. Referring to "blockchain" is like referring to "the internet". It can be applied millions of ways, which is why attention to every layer of the stack is important. Emerging standards for identity that leverage blockchain put the decentralised identifier of the credential's issuer in a ledger. This can be accessed by anyone who is needs to verify a credential of a particular user.[7]

Open Floor Dialogue – Perspective from a Technology Provider Who Focuses on Displaced People: Refugees and Homeless Population

Looking back in history to 1539, where the first identity system was built in France, it was a record of continuous occurrences of a person's life events (ie: birth, marriage, divorce, death). Leading up to the Second World War, there was a shift from recording occurrences

[7] https://www.lfph.io/2021/02/11/cci-verifiable-credentials-flavors-and-interoperability-paper/

to recording identifiers that were inherently physiological, this fundamentally changed the way identification was viewed. This leads to two distinctions:

> **"The distinction of your identity as a fundamental right that guarantees State benefits (i.e., protection) and the notion of identity as an asset; where does the distinction lie in public-private collaborations in building a system for identity as a *right* versus identity as an *asset*? And when separating these two, what data actually requires permanence and what data can feature the principle of disposability? We often assume that identity systems need to be permanent and that the data needs to be permanent, and we need to trace the entire history of an individual's life, but not all data should be built with that in mind. Some data can be disposable and used for specific purposes at any given point in time and then utterly disappear."**
>
> **Ms. Lucia Gallardo**
> Founder & CEO, Emerge

How do we separate what belongs where in terms of how systems are built? This is important because it leads to an assumption that there is a causational relationship between identity and access to the world, and rights, services, and protection, but identity has served as an excluder, as much as it has been an includer, throughout history.

It was proposed that the Government has an obligation to ensure foundational identity for all of its citizens, and a digital identity, so it can be used as a means to access services.

Conclusions

The key conclusions drawn from this were:

- Citizens should have more control of their identity data.
- It is important, but difficult to define, the minimum data set that determines a public identity.
- Decentralising identity is a way to address the issue of control.
- A government should be an authority on the establishment of foundational identity; however there needs to be a degree of control by the citizen so they can decide which elements to disclose for use in specific cases.
- Agreeing on the elements of the legal foundational identity is a challenging task.

- Granting identity is not a lightweight responsibility on the State. It has an obligation to protect an individual's rights despite the type and volume of identity data which is gathered. This includes the most basic data, such as name (which can reveal religion) and gender.

- Data sharing between different government agencies and the private sector should be done in a controlled way, on a needs basis and underpinned by a framework that regulates such sharing.

- There should be a legitimate purpose, transparency, consent, and control of data subjected to data sharing; this builds trust in services.

- Identity has served as an excluder, and as an includer, throughout history.

- There is a distinction between identity as a human right, and identity as an asset which is used as a means to provide access to services.

- There needs to be the correct combination of privacy, security, and trust in relation to data and defining identity.

- It was proposed that governments have an obligation to ensure foundational identity for all of its citizens, and also a digital identity, which can be used as a means to access services.

- The real control of a citizen is the ability to grant access for a specific portion of data to be used for a specific purpose, without having to provide all data for use in all cases.

- Governments should continue to play the role of identity service providers to guarantee a person is who they say they are, using an integrated approach including biometrics and/or other identity attributes. Society should manage the rest.

- Lessons could be learnt from the medical ethics industry which has faced similar issues relating to the control of identity data.

- We should have concentric circles representing layers of data. Some data is out of our control, as it refers to something we are born with. There are some things which are immutable, whereas some things can be considered to be attribute-based information, and other things are considered to be circumstantial data.

- Education and trust are needed for users to engage in new digital forms of identity management in order for these new systems to serve their purpose.

- The move to digital identity is a journey with the ultimate goal of providing more control, privacy, and trust to individual citizens over the use of their identity attributes, whilst reducing the risk of creating a single entity which is viewed as being of 'high value' for hackers.

3.4 Digital Vaccine Certificates and the Future Role of Health Data in Identity Systems

- Why stop at COVID-19 vaccination data?
- Does the private sector think that the 'Yellow Vaccination Book' (e.g. for Hepatitis, Yellow Fever vaccination, etc.) will go fully digital?
- Will they be part of the data variables linked to digital passports?
- What additional health data, if any, is likely to be added to legal identity systems in the coming years?

The session was framed as a discussion focusing on the digital recording of health data (vaccinations) in a manner that will allow people to travel to other countries and to access public, and private, services within their home countries. The parallel was made to yellow fever, in that, for many years countries asked travellers to prove they were vaccinated against yellow fever, and that this was recorded in a little yellow vaccination booklet, which travellers had to show to a border official. In that context, the traveller carried a physical paper certificate, and the border official verified the document in order them to allow the holder entry into the country.

Where the dynamics have changed, is that now the conversation is about a digital system linked to a person's passport, which poses the question; who has access to what type of data, for how long, and for what purpose? If COVID-19 vaccination data is monitored today, what additional data will be monitored tomorrow? Will countries ask travellers if they were vaccinated against other infectious diseases? Will countries restrict the type of people that enter because they 'could' be carriers of particular types of conditions, diseases, or infections? Could it open up a world where only 'healthy' travellers are welcome?

Broadening the scope of the discussion, additional contexts were debated to explore not only the trade-offs between economic activity and privacy, security, and health risks; but also concerns around inequity, discrimination and exclusion that come up in the context of digital vaccine certificates.

Often infrastructure is deployed in a certain context for a limited purpose, which becomes permanent. For example, if we rush into building a digital vaccine certificate infrastructure, will we create dependencies which will create *function creep* in the way systems are used?

"We need to refocus the discussion around vaccine certificates beyond balancing the potential to open up economic activity against privacy concerns for individuals, to the fundamental questions of equity, liberty and exclusion that these proposals raise. It is likely that vaccine certificates will accelerate the adoption of digital identity programmes by governments globally and may enable the permanent entrenching of centralised and mandatory identity systems, that have been designed without adequate consultation and study as to their necessity, the required safeguards, the path dependencies they will create, and the function creep they may enable. They may also distract from the pressing need to focus on achieving global vaccination. History is testament to systems designed as a temporary measure getting entrenched in our society – negatively impacting the rights of individuals."

Ms. Jhalak M. Kakkar
Programme Manager, Technology & Society
Centre for Communication Governance (CCG)
National Law University, Delhi

There are concerns about how a digital vaccine passport will accelerate the adoption of centralising mandatory digital IT systems without necessarily giving enough thought to the structuring of the systems, and whether they are truly necessary. They may exacerbate inequalities and set up infrastructures where governments that do not adhere to the 'rule of law' or have strong democratic legitimacy, could build surveillance systems and use them to restrict rights and liberties of individuals.

It was expressed that separation of purpose is essential to protect privacy and to avoid *function creep*. If an existing ID system is leveraged to issue vaccine credentials, then the sensitivity of health-related data, including vaccines, must not be visible to a legal/foundational ID system.

Opportunities with rolling out digital vaccine passports

In relation to cross border travel, industry and governments do not want to refer to the term 'vaccine passports', which led to the creation of the "Good Health Pass Collaborative" [8] an open, inclusive, cross-sector initiative, bringing together leading companies and organisations from the technology, health and travel sectors. Members of the *Good Health Pass Collaborative* are creating a blueprint for interoperable digital health pass systems and building a safe path to restore international travel and restart the global economy. Inclusion

[8] https://www.goodhealthpass.org/

is a key component that they are trying to obtain, however getting health status certification requires resources, time and money. The *Good Health Pass Collaborative* has been working to support individuals in acquiring their own digital wallet to prove that they have been vaccinated, or have been tested for COVID-19, and to do it in a way that supports individuals having control over how they share and present that information.

Identity Binding

The topic of 'identity binding' was raised, with the point noted that if the certificates are going to have value they have to be bound to an identity.

> **"If health status certificates are going to have any value, they have to be tied to the presenter of that with a certain level of assurance that the presenter of the document, whether it's physical (a paper certificate) or virtual (a digital certificate), is the person who got the health test with the vaccine. We need to have faith in the health status itself and in some way bind it to the identity."**
>
> **Mr. Daniel Bachenheimer**
> Principle Director – Digital Identity Accenture
> Contributing Member - ID2020's Technical Advisory Committee

For example, New York's Excelsior Pass[9] requires an individual's first name, last name and date of birth. In order for an Excelsior Pass to be useful, an individual has to have a government-issued photo ID that has the individual's first name, last name and date of birth. With the two, a government can bind identity.

Public Good versus Discrimination

It was argued that public health is not about 'personal choice', rather it is about a public good which benefits the entire population as they have a right NOT to be infected.

The argument was made that there is a difference between proving vaccination status for international travel, where States have a legitimate interest in assuring the safety of their own residents and health systems, and domestic use within a State, where there is a risk of discriminatory practices, where vaccine access is inequitable. It is important to distinguish between the implementation of a credential that allows people to easily, and securely, attest to their vaccine status, and the policies regarding how it is used (e.g., required for travel or certain access).

Challenges with Creating Infrastructure for Governments to Roll Out

There were a range of views expressed with one participant stating that: "*Governments started using the word 'passport' as a word that lends legitimacy to the radical concept that a*

[9] https://covid19vaccine.health.ny.gov/excelsior-pass

personal choice about one's health should be the determinant of access to a wide range of public and private services in a domestic context." However, this was refuted by acknowledging that it is not a radical ideal to request proof of a vaccination as required condition to permit travel. This was first introduced in the 1890's and then officially adopted in the 1930's with the 'Yellow Card' system. There is already a widespread precedent for requiring the verification of immunisations for activities such as travel, enrolling children in school, etc. Adding proof of COVID-19 vaccination is only adding one more to this list.

Conceptual Frameworks around Digital Vaccine Certificates

Different architectures imply different underlying systems, and those underlying systems have different properties. One of the key architectures the *Good Health Pass Collaborative* has been working on is to give people digitally signed information from an authoritative source and let the individual choose when and how they share it. For example, a State could provide an individual with an assertation, digitally signed, which can be used anywhere (like a paper certificate), without having to recontact it to the facility where the vaccine was issued in order to verify authenticity). This would create a trial identifying where the individual is and in so doing, it infringes on the rights of the individual to control the use of that certificate.

> **"Identity is not "one thing." There are many angles and perspectives. I wrote the *Domains of Identity* to support decision makers to have a broader understanding of how different identity domains work and to have language to talk about the complexities that arise. It has been really useful in the current pandemic to have a language to name the complexity of bringing information from one domain; civil society transactions (healthcare COVID-19 test or vaccine certificate) into the commercial registration and transaction domains (booking and flying on commercial airlines) and government transactions (showing a passport at a border). Governments need to do right by their citizens and build CRVS and other identity systems that work for people and enable them to transact with each other and institutions. I've held a user-centric or citizen-centric perspective for my whole career, and I think that emerging decentralised identity technologies really provide a path forward that support governments do what they do well and let citizens and businesses transact and connect without the Government needing to be always in the middle (some earlier scheme designs called for). I'm optimistic about the future of how trustworthy, empowering digital identity systems will work."**
>
> **Ms. Kaliya Young, MSIMS**
> 'Identity Woman', Ecosystems Director, COVID-19 Credentials Initiative, Co-Chair, Interoperability Working Group for Good Health Pass

Public Health Perspective - Impact on Individuals Rights and Freedoms

From a public health perspective, it was argued that COVID-19 should not be put in the same category as yellow fever because it affects border control and allows people to travel even when they may present a public health risk. Yellow Fever is a disease for which there is a long lasting, highly effective vaccine. It is also a disease that is not spread through person-to-person contact; therefore, it does not present the same threats that COVID-19 does.

Better examples of history from International Health Regulations come from typhus and cholera; both of which were included in international health regulations and were removed when it became clear that vaccines did not protect the world from transmission.

> **"The extent to which vaccination status makes it safer for individuals to travel or meet is heavily context dependent and not a matter of identity. The same is true of immunity as a result of prior infection and recent negative tests. There may be circumstances where people will want to be able to confirm such health information to others, but that must remain a matter of choice. Yellow Fever vaccine certification is a poor analogy for COVID-19. The removal of cholera and typhus from listing in the International Health Regulations when it was discovered that vaccination against them was insufficient to stop outbreaks around the world is a more instructive example."**
>
> **Sir Jonathan Montgomery**
> Professor of Health Care Law, University College London
> Chair of the Ada Lovelace Institute, expert deliberation
> on vaccine passports

A further issue to consider is how useful the certification is in terms of identity status. A vaccination gives a degree of confidence about the health threat. Testing only gives a snapshot of the risk at a given point in time. If vaccine certification is a form of quasi-identity, that implies that a particular set of purposes and the context in which the systems are used, need to be defined. This raises questions about primary and secondary uses; government and private sector uses. That, in turn, leads to thinking about the design of the systems and how to secure public confidence, trust and legitimacy when using them.

Digital Infrastructure Required to Operationalise the System

There is a spectrum of infrastructure required to operationalise the system– digital, paper and bar code-based. The construction of self-sovereign identity, or decentralised identity, also has an infrastructure associated with it. There is an *identity wallet* which could be housed on a smartphone which could be web-based/cloud-based. Blockchain could be used for decentralised identity which would not be as slow as it is for cryptocurrency because it

incorporates a different consensus model. The distributed ledger technology that is used in some, not all, self-sovereign identity systems is primarily used for decentralised public key infrastructure. In the TCP/IP four-layer architecture, the first layer is a registry; in some cases, it is a distributed ledger technology, an in other cases, it is achieved by other means, such as decentralised public key architecture.

> **"One of the key components that self-sovereign identity allows for is the individual to execute selective disclosure. An individual might have multiple verifiable credentials which are trusted, verified attributes. They could be health attributes, legal identity attributes, education attributes or any other verified credential. With self-sovereign identity, an individual can select which of those attributes to disclose, and that specific attribute can be verified against the registry to confirm if it is authentic. Selective disclosure and zero-knowledge proofs are part of decentralised identity."**
>
> **Mr. Daniel Bachenheimer**
> Principle Director – Digital Identity
> Accenture
> Contributing Member - ID2020's Technical Advisory Committee

Passports are the only global inter-operable trusted verified documents. Selective disclosure cannot be performed on passports. When a passport is handed to a border official and the integral chip is read, all of the information in the passport is disclosed. Self-sovereign identity is different as not all information has to be disclosed. A birthdate does not have to be given, for example, if it is not required.

The other side of the spectrum is paper-based, where there is a two-dimensional bar code that could be virtual (digital) or printed out as a portable document format (pdf) file, which is a low-tech and inclusive solution as it can be verified offline. The verifier would still, however, need an internet connection in order to verify the information presented.

However, in all cases, there are a lot of concerns relating to the privacy of health information. One feature of paper certificates is their lack of encryption, as it would be problematic to distribute an encryption key globally. It is encoded as a two-dimensional barcode, but anyone could take a photograph of it and access an individual's health information.

Paper-based digital representations of an individual's information presents a fraud risk. While this approach is framed as inclusive, anyone who reads the quick response (QR) code credential can reproduce it and access the information, whereas with a verifiable credential presented in a digital form, an individual is proving that they hold the credential without necessarily sharing the credential.

It was argued that in the same way an individual holds a physical passport and driving licence, they have more control over a credential if it is digital. Widespread use of printed, paper-based, digital representations (e.g., QR codes) can create and increase risk, even though this approach is positioned as being inclusive.

There are alternatives to paper-based digital representations, including smart cards which are not expensive (US$1 if purchased in bulk) capable of holding verifiable credentials which present fewer fraud risks.

Cross-border Interoperability is Required

When it comes to identity, the issue of cross-border interoperability should be considered. Many countries are not prepared, or ready, to receive digital solutions. Some countries do not have data protection regulations in place.

There were concerns that a digital certificate can create a space for more surveillance, specifically in centralised systems. *Access Now* published a paper highlighting concerns regarding exclusion and data protection with the proliferation of centralised ID systems.[10]

The *Good Health Pass Initiative* is creating a governance framework for managing trust registries. The intent is to confirm which certified testing laboratories can be trusted and which signatories of vaccine certificates can be trusted so this information can be shared with other countries. (The governance framework will also follow best medical practices).

It was argued that there are different ways to achieve interoperability. One way is to share information via direct connections, another is to derive standards; the minimum amount of data that has to be shared, in order to meet the requirements of the country a person is visiting. For example, *International Civil Aviation Organization* (ICAO) defined standards for ePassports with immigration. They defined two required data groups; data group one contains all the information that could be read on the documents; whilst data group two is a photograph. In-excess of 100 countries have agreed this is the minimum data that is required. There are other data groups present in passports which are optional, and for use in country specific contexts.

The *Health Pass* is similar, where the intent is to define the minimum standard, or data set, that is required. Many countries allow their provinces, or states, to define minimum requirements, meaning it is decentralised. It only becomes centralised by a federal government when an individual looks to cross borders.

[10]Access Now, Protocol for exclusion: Why Covid-19 'passports' threaten human rights; https://www.accessnow.org/cms/assets/uploads/2021/04/Covid-Vaccine-Passports-Threaten-Human-Rights.pdf

Consent is not synonymous with control

It was argued that linking health information to passports will stop some people from being vaccinated. For example, undocumented migrants or people living with HIV may be discriminated against if they are disincentivised to be vaccinated.

> **"While we hear about 'selective disclosure' when it comes to self-sovereign identity, we have to remember that *consent is not synonymous with control*. For example, the people who are going to ask for a vaccine certificate are those who have power over an individual, an employer, a landlord, etc. In that context, the individual does not have a choice and has to hand over their data."**
>
> **Dr. Tom Fischer**
> Senior Research Officer
> Privacy International

There should be balancing anti-discrimination provisions which go with the introduction of digital health passes. The biggest concern around certification is that it is a distraction from key human rights questions about access to employment and livelihoods. It was expressed that not having an ID should never be a barrier to obtaining a vaccine or vaccine credentials. This means alternative measures, and safeguards, must be put in place to prevent exclusion and discrimination.

The *COVID-19 Credentials Initiative* [11] has been exploring the application of verifiable credentials with an effort to define where it is appropriate to ask for health status information and where it is not. In some use cases, it is legitimate to check health status information to protect individuals. However, in some cases, such as those with a strong power imbalance, it is not appropriate.

Can there be an International Standard for Mutual Recognition of COVID-19 Vaccine/Immunity Certificates?

Bilateral and regional arrangements have been discussed, but to date there has not been acceptance of a set of global arrangements. Selective disclosure type vaccine credentials are key, as some vaccine credentials do not allow this functionality.[12]

Conclusions

The key conclusions drawn from this session were:

[11] https://www.covidcreds.org/
[12] https://www.lfph.io/2021/02/11/cci-verifiable-credentials-flavors-and-interoperability-paper/

- Public health is not about 'personal choice', rather it is about a public good which benefits the entire population as they have a right NOT to be infected by those carrying infections.

- Industry and the governments do not want to utilise the term 'vaccine passports.' The *Good Health Pass Collaborative*[13] is an open, inclusive, cross-sector initiative, bringing together leading companies and organisations from the technology, health and travel sectors to create a blueprint for interoperable digital health pass systems which is inclusive.

- Emerging decentralised identity technologies provide a path forward to support Governments to do what they do well, and let citizens, and businesses, transact and connect without the need for the Government to act as an intermediary,

- One of the key components that self-sovereign identity allows for is provision for an individual to execute selective disclosure. An individual might have multiple verifiable credentials which are trusted, verified attributes. They could be health attributes, legal identity attributes, education attributes, or any other verified credential. With self-sovereign identity, an individual can select which of those attributes to disclose, and that specific attribute can be verified against the registry to confirm if it is authentic.

- The topic of 'identity binding' was raised, and it was noted that if certificates are going to have value they have to be bound to an identity.

- It is important to distinguish between the implementation of a credential that allows people to attest to their vaccine status easily and securely, and the policies regarding how it is used (e.g., those required for travel or granting certain access).

- There are concerns about how a digital vaccine passport will accelerate the adoption of centralising mandatory digital IT systems without necessarily giving enough thought to the structuring of the systems, and whether they are truly necessary. They may exacerbate inequalities and set up infrastructures where governments that do not adhere to 'rule of law' or have strong democratic legitimacy, could build surveillance systems and use them to restrict rights and liberties of individuals.

- Paper-based digital representations of an individual's information presents a fraud risk. While this approach is framed that it is being inclusive, anyone who reads the quick response (QR) code credential can reproduce it and access the information, whereas with a verifiable credential presented in digital form, an individual is proving that they hold the credential without necessarily sharing the credential.

[13] https://www.goodhealthpass.org/

- In the same way an individual holds a physical passport and driving licence, they have more control over a credential if it is digital. Widespread use of printed, paper-based, digital representations (e.g., QR codes) can create and increase risk, even though this approach is positioned as being inclusive.

- There should be balancing of anti-discrimination provisions to accompany the introduction of digital health passes.

- Certain citizens, such as undocumented migrants or refugees, may be discouraged from seeking vaccine certification in order to avoid the attention of the Government.

- It was expressed that not having an ID should never be a barrier to obtaining a vaccine or vaccine credentials. This means alternative measures and safeguards have to be put in place to prevent exclusion and discrimination.

- Separation of purpose is essential to protect privacy and to avoid *function creep*.

Sanitising hand gel / biosecurity measures being used at an ID centre in Danlí, El Paraíso, Honduras, March 2021 (photo: UNDP Honduras)

A voter having his fingerprint and electronic ID read by a combination-reader in Kyrgyzstan (photo: UNDP Kyrgyzstan)

3.5 Is the Clock Ticking for Paper and Plastic Identity Cards?

- Does the private sector think that UN Member States will still be issuing paper and plastic identity documents in 10 years' time?
- If credentials using paper and plastic disappear, how can data subjects be empowered to contest the accuracy of digital records?
- Can/should paper and plastic identity credentials retain legal primacy over digital ones?

- In legal identity systems where biometrics play an increased role, with increased presence of biometric data, does the private sector think that identity variables such as name and gender will become more, or less, important to both individuals and states?
- What is the implication of technological development on data collection?

The context for the fourth session was established by asking participants how they see the future of identity credentials:

- Will paper and plastic credentials be replaced with fully digital credentials, or will paper and plastic cards still have importance?
- If credentials are completely digital, how can citizens ensure that someone doesn't change personal data without an individuals' consent?

It was noted by the facilitator that digital identity is not one agreed thing. Identity works differently in different domains. The facilitator wrote the book, '*The Domains of Identity: A Framework for Understanding Identity Systems in Contemporary Society*"[15] to support clarity regarding contexts of domains of identity.

Will paper and plastic identity documents be issued in 10 years' time?

The consensus in the session was an overwhelming yes, affirming that there will still be paper and plastic identity cards issued over the next 10 years. In the short-to-medium term, which can be defined as 10 years, physical documents will continue to exist as the process for changing international conventions takes a long time.

> **"Having worked in software implementation for many years, we know that there is a long adoption time. Even though 10 years may seem like a long time from now, understanding where the world is and the digitisation more broadly, suggests that, yes, paper form based will still be issued. They will probably be a much smaller**

[15] https://identitywoman.net/wp-content/uploads/Domains-of-Identity-Highlights.pdf

fraction of the identity documents that are being issued, but yes I think they will be around for a while."

Ms. Natalie Smolenski
Senior Vice President, Business Development
Hyland Credentials

"In terms of the systems that are being designed and rolled out, they need to cater for the possible eventual elimination of the paper, the physical card. The ultimate reason for that is the cost of the consumables, as well as the logistical elements for governments is massive. Funding a foundational ID system is more manageable. I think the biggest reason physical documents exist today is because offline verification is required. But offline verification can be replaced with a certificate or credential on a smartphone or even a 2G feature phone. A physical card may be required as a back-up because we need to take a practical approach, especially in developing nations where infrastructure is still a long way away from having a centralised digital ID system. It will become a backup certificate to the digital certificates, as well as the central record".

Mr. Lyle Charles Laxton
Founder and CEO
Laxton Group

"In the development of the standards for the mobile (digital) driving license and passport, we always consider that the physical document is the fall back. It is written in the international conventions; for the passport it is written in the 1944 Chicago Convention,[16] and for the driver's license, it is written in the 1968 Vienna Convention.[17] It takes time to change conventions, maybe four or five years. Also for the migration of identity documents it takes at least five years and for the complete displacement it takes 10 or 15 years."

[16] https://www.icao.int/publications/pages/doc7300.aspx
[17] https://en.wikipedia.org/wiki/Vienna_Convention_on_Road_Traffic

Mr. Kenichi Nakamura
Innovation Strategy Office
Panasonic Corporation

If paper and plastic records disappear, how can data subjects be empowered to contest the accuracy of digital records?

This question seeks to explore the breadth of technologies; how they work together, and what does the governance framework look like within which they are embedded. It also introduces the notion that sometimes there is a lack of trust in the State as the arbiter of legal identity.

The strongest tool that exists, from a technology perspective, to achieve trust is blockchain. In the short to medium-term, however, the world is not yet ready for blockchain.

It was suggested that the first step is to have a centralised clean trusted database of records. In this model, that centralised database would be the primary ID repository. To have a trusted database, there must be offline certificates which mirror specific credentials, which can be held in a digital form where they can sit in a wallet on a smart phone, as well existing as a physical card or paper certificate.

> **"It's the full ecosystem of those three – digital, paper and physical. It's moving one's primary token into the digital ecosystem versus one's primary token being a physical paper or card. Transitioning that nuance is what digital ID is."**

Mr. Lyle Charles Laxton
Founder and CEO
Laxton Group

In order to go to fully digital, however, the digital divide gap has to be reconciled.

> **"Considering my jurisdiction of Ghana, I think 10 years is too early for three reasons. One, the cost of infrastructure. Ghana just started issuing the Ghana card. After about 16 years of independence, we are now starting to have an integrated nationwide identity and that is a plastic card. It's not realistic to throw any these investments after just 10 years. Two, the level of internet and penetration across States is different. The level of internet penetration in Ghana is different from India; and the level in Nigeria is different than South Africa. Unless we expedite and increase the level of technology penetration, even 50 years is too soon. The last point is the legal and policy frameworks within**

various jurisdictions. What does the law permit one to do and what kind of identity does the law permit one to have? What is the policy around digital identity?

Mr. Precious Baidoo
Digital Frontiers Institute
Ghana

When it comes to the issue of inclusion, it is important to consider; will everyone be able to have a digital form factor, and digital coverage, and will everyone be able to access it? In addition, there are also issues in the way passports are used. In Europe, for example, with the Entry/Exit System (EES)[18] that will go live in a few years, there are also the Schengen States,[19] (the 26 European countries that abolished passport and border control at their mutual borders with a common visa policy allowing free movement of people in harmony, with common rule,) will stop stamping passports. If the world migrated to fully digital passports, where would countries that are still required to physically stamp passports, stamp them? Unless the whole ecosystem around those physical documents' changes, it is not plausible to move to fully digital passports.

"I don't think they will be going away in the next two to three decades. The issues of inclusion and technology adoption throughout the whole ecosystem will take a long time. Also, we will need paper or plastic as back-ups. If everything is fully digital, there will be network and server outages, and individuals will need a backup in their wallets."

Mr. Daniel Bachenheimer
Principle Director – Digital Identity
Accenture
Contributing Member - ID2020's Technical Advisory Committee

An argument was also put forward that the cost of technology is decreasing and eventually there will be a conversion point where digital passports become more viable.

"I would say, in 20 years, because the cost of technology is going down. I think there will be some conversion point that the technology will be very cheap, and then modernisation will go up exponentially.

Mr. Cristiano Blanez
Manager, Global Relations Division
NEC Corporation

[18] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/ees_en
[19] https://www.schengenvisainfo.com/schengen-visa-countries-list/

It was pointed out that electronic identification and trusted services (eIDAS)[20] already exists in Europe, where a' trusted list' defines electronic identification schemes (eIDs) that are issued and accepted between different Member States. The stated intention is for eIDAS to migrate to the verifiable credential's standard, which will support interoperability. The timeframe for such migration is not known.

Is it ideal for paper or plastic to go away?

Most digital identity programmes, at least foundational digital identity programmes, are leapfrogging and coming directly into the Global South. But what is the experience of the Global North? For example, is the Global North having conversations about moving their social security processes to a digital format? If that is happening, it would be good to learn from the Global North, instead of jumping from legacy identity programmes directly to digital identity programmes in the Global South, without first learning from the experience in the Global North.

When it comes to identity, there are many things that need to work:

i. legal framework;
ii. technology framework;
iii. institutional framework; and
iv. implementation framework.

The legal framework has to work for data protection, otherwise a surveillance hub is being created for the Government. The right technology and system architecture is required so that people are able to interact with it. There is also a need for institutions which are equipped with the correct technology. Finally, it needs to be determined whether people are capable of interacting with a digital identity or even understanding what it is, and for this, digital literacy is required.

> **"Identity is an invention of the contemporary world. It must be recognised that identity literacy and digital literacy may not exist in remote places."**
>
> **Ms. Kaliya Young, MSIMS**
> 'Identity Woman'
> Ecosystems Director, COVID Credentials Initiative
> Co-Chair, Interoperability Working Group for Good Health Pass

It was noted that the debate of paper versus plastic versus digital-only is context dependent and will shift over time. If there is a shift to digital in the future, then non-digital alternatives (or offline backups) will be needed in the medium-term and maybe in the long-term. People-centric systems and the ability for people to choose which credentials can be obtained, depending on what they are comfortable with, is a key area to prevent exclusion.

[20] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

Can/should paper and plastic identity credentials retain legal primacy over digital ones?

Even digital form factors still have to exist in physical form factors, whether that is a smartphone, or a laptop, or some other hardware interface capable of interacting with the digital world. Perhaps the question of 'primacy' is the wrong question, and it is the question of 'integrity' of the credential itself. Cryptography and verifiable claims are platform-agnostic, for example. They can easily be ported between different digital and physical form factors.

While there were mixed views, of which form should take primacy, one participant felt strongly that digital identity should take primacy:

> **"Digital identity should take primacy. A certificate or card itself should act as certified copy. I think we should be working towards the goal of achieving a centralised digital system. "**
>
> **Mr. Lyle Charles Laxton**
> Founder and CEO
> Laxton Group

There were some participants who expressed their disappointed that central databases were being discussed as being a good idea. It was stated that "*...the ability to prove identity should exist without needing the permission of the State; including server ability*." The reason highlighted was because it could allow the State, or a coercive power of the State, to disable one's identity. It was also stated that core identity database exchanges are dystopian.

It was argued that paper/plastic identity documentation, with no digital features, may be the only way a citizen can be assured of safety from the State. A physical card has a metaphysical connotation of an individual possessing Evidence Of Identity (EOI). The individual feels empowered, as if they are in control. When an individual wants a service from a service provider, which includes the State, the individual can present it to claim an entitlement.

A participant from Panasonic stated that "*the benefit of the printed card is that it is visible and 'proof of possession'*", or in other words, because I have it, it must be me. This prompted the facilitator to enquire: "*how is possession of verifiable credentials similar to possession of a physical card?*"

> **"Public key cryptography has enabled the instant proof of ownership or custodianship of a credential. A digital device can be used to countersign a verifiable claim with a private key, thereby proving the individual owns the device. This combination of public key infrastructure (PKI), with various forms of identity proofing and verification is critical to the future of digital credentials."**

Ms. Natalie Smolenski
Senior Vice President, Business Development
Hyland Credentials

The State, or jurisdiction, an individual is living in should be considered when answering the question if paper or plastic should have primacy over digital, as countries differ. It was reiterated that identity is about trust, relationships, and personal data. The question of legitimacy must always be asked – does the credential have the data we want? A document which has the fundamental indicators should have primacy.

It was also noted that interoperability across more regions should be the focus, rather than primacy.

> **"I agree with the points that smart ID cards and paper documents will coexist. The question is which of these form factors will be dominant over the next 10 years? I don't think it will take 50 years to have this digital model, but the level of adoption will vary geographically. This is because of different economic factors, cultural values, attitudes, levels of literacy and costs of infrastructure."**

Mr. Dismas Ong'ondi
IT Elections and Civil Security Consultant
Nairobi, Kenya

The *Africa Initiative* is spearheading the regional digital transformation of Africa, with 30 out of 54 countries participating on a voluntary basis. One of its aims is to extend broadband services to Africa. The issue for Africa, is that every African Union Member State has rolled out national ID systems of varying levels.

As countries work towards embracing digital identity, or digital ID cards, they need to develop strong public-private sector partnerships nationally, initially focusing on the area of infrastructure. For example, some countries have policies that permit governments to provide online services through smart cards that are provided by the private sector. If the banking sector provides card readers, or even issues their own smart cards and allows government services to be accessed via those cards, that would make the affordability of these technologies sustainable in the long term.

As countries come together to form single trading blocks, they need to harmonise their legal and regulatory frameworks in the areas of cybersecurity and data protection.

It was also noted that disaster recovery plans and models have to be built if digital solutions assume primacy.

In legal identity systems where biometrics play an increased role, does the private sector think that identity variables, such as name and gender will become more or less important to both individuals and States?

It was argued that numerous data fields should be captured in a digital ID system, more than 'only' core biometric information. The reason given was that in order for certain services to be granted, such as child benefits to mothers with children, or State benefits for people of a certain age, certain identity variables will have to be presented.

> **"The visibility of the data is where the argument actually sits, and with the different e-Government services, apps and wallets that can apply for various types of services to decide what data is public and private. There is need to capture data and associate with biometrics and core identity."**
>
> **Mr. Lyle Charles Laxton**
> Founder and CEO
> Laxton Group

There was a position put forward that identity categories will be re-evaluated and that in the future, gender, for example, may not be considered relevant.

> **"I think we are globally in the process of re-evaluating the social and legal salience of identity categories like gender, sexuality and marital status. I can imagine a world where gender is not a relevant category for benefiting from government services. The content of identity documents can and will change over time."**
>
> **Ms. Natalie Smolenski**
> Senior Vice President, Business Development
> Hyland Credentials

It was noted that there is a distinction between different domains and what the appropriate flow of information is within those domains. For example, there is the domain of government registration, with the primary identifier being a birth certificate; and secondary identifiers being a passport, driver's licence, voter registration card, etc. There is also the domain of government transactions, or to give an example, how does an individual appear with an identifier already enrolled in a government system? Then there is the flow within those domains, or in other words, how does civil society register and transact with different services, such as healthcare, education, religious organisations, unions, professional associations and so on. Then we must consider commercial sector enrolment and transaction, relating to how goods and services are bought and sold.[21]

Emerging Areas of Research

Biometric data needs to be combined with *Public Key Infrastructure* (PKI). There are several technologies, like those developed by the *FIDO alliance*,[22] which use smartphones or secure storage to retain private keys. People can use biometric data to get access to a private key.

[21] https://identitywoman.net/wp-content/uploads/Domains-of-Identity-Highlights.pdf
[22] https://fidoalliance.org/how-fido-works/

There is another technology called *Public Biometric Infrastructure* (PBI),[23] which is a combination of biometric data and PKI, but secure storage is not needed because the biometric feature itself can be used as a private key. The private key is already part of an individual's body, such as their fingerprints. Biometric vendors have been trying to extract elements that can be added to the private key, but it is difficult as biometric patterns cannot always be the same.

There is a distinction between systems engaged in syndication, which is matching, and systems engaged in identification, which is determining who someone is (without the person necessarily interacting or connecting with the system). *Authentication* is the matching of someone to an existing record based on what was enrolled. It was noted that the primary use of biometric data is to determine uniqueness, secondary use is to authenticate something (e.g., an identity) with a varying degree of assurance.

There were some participants who highlighted that biometrics do not work for 100% of the population. An example was given of food subsidy programmes, where it was found that tobacco workers, for example, had little or no fingerprints as the materials they worked with had smoothened out their skin.

Another participant highlighted that facial recognition relies on three elements to hopefully obtain accuracy:

i. resolution, which is the number of pixels;
ii. the way a person is posed, and;
iii. lighting.

It was highlighted that in surveillance mode, accuracy is normally very low. It was also noted that there are demographic differentials and well-documented racial biases with facial recognition.

It was also noted that biometrics are probabilistic, not deterministic. There will always be 'type 1' and 'type 2' areas of 'accepts' and 'false rejects.' The FIDO technology is a good example of technology where a person's biometric identifiers never leave the individual's device. Authentication happens on the device using the authentication scheme which is located on the device itself. This is suitable for some applications, but when looking at levels of assurance, it is remote but not supervised remotely, which means the highest levels of assurance will never be achieved. Identity proofing, or creating an identity assurance level, is a government activity. The main activity of identity proofing is to determine uniqueness of that identity, which is typically done with biometrics, not with FIDO.

Conclusions

The key conclusions of the fourth session were:

[23] https://www.hitachi.com/rd/sc/story/pbi/index.html

- An overwhelming consensus that yes, there will still be paper and plastic identity cards issued in 10 years. Physical documents may constitute a smaller fraction of identity, but, yes, they will still be around.

- Some private sector participants articulated that physical documents will still be here for at least two to three decades, if not more. The primary reasons are the time it will take for inclusion, and for technology adoption throughout the whole ecosystem.

- If everything is fully digital, there will be network and server outages. Individuals will still need to have physical documents as a backup.

- Internet penetration is different in different States. The digital divide has to be addressed and adequate internet penetration, and uptake, has to be reconciled before the elimination of physical documents can be effective.

- It will take time for legal and policy frameworks to be created and adopted to define what kind of identity is permitted and for what purpose.

- The process for changing international conventions takes a long time, and the question was posed, "*should* intervention conventions around physical documents even change?" The 1994 Chicago Convention defines the standards for passports, for example, and the 1968 Vienna Convention defines the standards for driving licences.

- There will be a long adoption time before technology can replace physical cards, as the world is not ready for full digitisation.

- One complication of implementation could be a lack of trust in the State as the arbiter of legal identity.

- Blockchain may be the strongest tool for identity becoming digital in terms of trust, but that transition will not occur in the short-to medium-term.

- Governments could eventually use digital distributed ledgers/blockchain technology at a national level to create strong, clean records of ID.

- One reason that physical documents still exist is because of offline verification, but offline verification can be replaced with a certificate or credential.

- Systems that are being designed should cater for the possible eventual elimination of a physical ID card, however, a physical ID card may be required as a back-up, especially in developing nations where infrastructure is still a long way away from supporting a centralised ID system.

- When developing digital mobile driving licences, physical documents can be the 'backup.'

- If the world migrates to fully digital passports, where would countries that are required to stamp passports, stamp them? Unless the whole ecosystem around those physical documents changes it is not plausible to move to fully digital passports.

- When it comes to identity, there are many things that need to work:(i) legal framework; (ii) technology framework; (iii) institutional framework; and (iv) implementation framework.

- Whether people are able to interact with digital identity or even understand what it is, digital literacy is required.

- Identity is an invention of the contemporary world. It must be recognised that identity literacy and digital literacy may not exist in remote places.

- A disaster recovery plan, or model, has to be developed if digital processes become the primary method or proving identity.

- As countries work towards embracing digital identity, they need to develop strong public-private partnerships at the national level, especially in the developing world, to ensure that digital infrastructure and digital literacy is in place.

- Paper and electronic IDs will coexist for at least 10 years. The level of adoption of digital IDs will vary geographically because of different economic factors, cultural values, attitudes, levels of literacy and the maturity and costs of ICT infrastructure.

- In developing countries, if States allow policies for government services to be issued on a digital ID card, technology may be more sustainable than paper-based systems in the long-term.

- Globally we are in the process of re-evaluating the social and legal salience of identity categories such as gender, sexuality, and marital status. There could be a future where gender, or other identifiers, are not relevant in being able to access government services.

A woman receiving her new national identification card in Danlí, El Paraíso, Honduras, March 2021 (photo: UNDP Honduras)

Plastic identity card inserted into a combination-reader in Kyrgyzstan (photo: UNDP Kyrgyzstan)

3.6 International Identity Data Sharing and Granting of Foreign States to Sovereign Identity Databases

- Does the private sector expect that there will be an increase in intergovernmental agreements access core national identity databases in order to verify the 'breeder identity tree' of paper and/or digital credentials?

- Will migration – and the need to apply appropriate tax regimes based on residence – mean more intergovernmental identity data sharing? What are the implications for digital solutions?

- Will increased digitalisation of civil registration credentials (e.g., marriage certificates) see greater recognition across borders (i.e., without *official translations*?) Will / should they be added as data fields to digital passports?

When framing the final session of the roundtable, which focused on the internationalisation of identity data, and identity credentials, the question was posed; "Will governments start requesting access to core identity databases of neighbouring countries or foreign countries, instead of accepting the identity document that the individual produces when crossing the international border?"

It was noted that the no country has entered into an agreement with another, that guarantees their citizens will only have only one identity or be known by one identity. This may become problematic considering that different identities exist. For example, participants were asked to consider a scenario where a country introduces a digital ID scheme, which individuals can enter as an adult, with an identity they assert that has been verified by community leaders. If the individual has a birth certificate that does not match this identity, it presents a fundamental question – legally, who *is* the person?

Another example was given in area of migration. It was suggested that in the coming decades, there will be an increase in two types of migration: (i) foreign migration, with people coming from the Global South to the Global North, and (ii) transitional migration, with people moving from one country to another and moving back. This temporary migration will not only be for agricultural workers or temporary migrants working in construction, but also for people who hold digital nomad visas, something which is increasing in a post COVID-19 pandemic era. More people will be living and working across borders, which means more people may have legal identities issued by foreign governments.

> **"As the drivers for increased intergovernmental data sharing grow, especially forced and elective cross-border movement, the demand for effective tax regimes and coordinated health status, it's imperative that we maintain considerations that strengthen the**

social contract – recognising the States need to know certain things about us to provide rights and entitlements balanced with the individual's right to privacy and security. Getting digital ID right will be critical to getting this balance right – and getting this balance right is critical to building the right kind of digital architecture in which we will increasingly live our lives."

Dr. Emrys Shoemaker
Researcher and Advisor on Digital Transformation
Caribou Digital

It is very likely that countries will want to receive more identity data on both their citizens and foreign citizens as countries are accepting more foreign migrants from neighbouring countries. Countries who are accepting foreign migrants from neighbouring countries may inevitably ask – do these individuals have alternative identities in other countries? Governments may also want to know how many citizens are moving into other countries for tax purposes. The session facilitator highlighted some examples in order to expand on the framing.

Refugee Registration

A research exercise was conducted on refugee registration between Lebanon and Syria. The research showed that there are different expectations that both States and individuals have around the process surrounding different forms of identification and different rights and entitlements. Individuals chose whether they were in Lebanon as a migrant worker, which gave them certain rights in terms of access to work, but no legal rights in terms of settlement, or whether they chose to re-register themselves as refugees in other to gain access to other rights and entitlements.

To simplify, there was a transition between different forms of legal identity in Lebanon, which sought to establish a form of control over the kind of benefits that people coming from the border areas would receive. Increasingly significant issues are:

i. the data and the database that holds information;
ii. the legal frameworks regarding what is and is not shared;
iii. the rights and entitlements which accompany how people move across borders;
iv. and the regulatory regimes.

Digital Nomad Visas

The rise of digital nomad visas is also something to monitor. Estonia has launched a digital nomad visa, for example, which allows an individual to register as an e-Nomad in Estonia.[24] It is not clear what the implications are for tax or residency in the person's home country, or who will track and have access to data for digital nomad visas? How much control will individuals have as they move around and across borders?

[24] https://e-resident.gov.ee/nomadvisa/

Does the private sector expect that there will be an increase in intergovernmental agreements accessing core national identity databases in order to verify the 'breeder identity tree' of paper and/or digital credentials?

After framing the session, the facilitator, explained that Yoti is a digital identity platform that enables approximately 10 million people globally to prove who they are, with an unusual architecture of giving the individual the private key, which can be used for public sector login or private sector login. When Yoti looks at the question, they are doing it from the lens of one identity platform.

> **"We are not seeing rapid progress on intergovernmental accessing of core national identity databases as yet. Currently we are seeing aggregators and credit reference agencies accessing a patchwork of national identity databases and a minor of governments allowing basic interrogation of certain databases (e.g. passport or driving license data) to identity providers or aggregators."**
>
> **Ms. Julie Dawson**
> Director of Regulatory and Policy, Yoti

The EU Settlement Scheme (EUSS)[25] is an example of a model that relies on using individual citizens information on a digital identity application, using the ICAO Public Key Directory (PKD),[26] rather than interrogating remote databases. It allows individuals to put their passport on a device and read the chip. That type of enrolment is similar to services used by various financial bodies. While there is a community of interest in this model in Europe, the ICAO PKD has not been universally adopted globally as some countries do not fully adhere to it. There are a range of different identity documents in some States which have some fraud loopholes. One recommendation is to adopt the ICAO PKD model as an interim solution, rather than checking documents directly, as it puts the solution in the hands of the individual.

> **"There is clearly progression in terms of the private sector offering individuals to set up digital identity apps or wallets to store credentials such as passports, driving licenses and credentials for health or employment under the governance of trust frameworks. The scanning of passport chip using the ICAO chip and PKD, is gaining recognition by financial services regulators, such as the Joint Money Laundering Steering Group – and so we would suggest that the recognition of the passport chip as a practical interim**

[25] ttps://commonslibrary.parliament.uk/eu-settlement-scheme-applications-figures-in-final-month/
[26] ttps://www.icao.int/Security/FAL/PKD/Pages/default.aspx

approach for remote proofing is worth consideration. Mutual acceptance of access to core national databases is more likely to occur in regions with common data protection frameworks, such as within the EU, using eIDAS."

Ms. Julie Dawson
Director of Regulatory and Policy, Yoti

It is also important to look at fraud, intelligence and transparency, to give governments more confidence in data sharing. The wider question is about accessibility**.** What is the widest level of accessibility for the private sector, NGOs and governments, and who uses what? For example, what documents and/or devices are used for people with disabilities, and what is used to support diversity (people who might change their name, gender or other attributes during their lifecycle)?

Intergovernmental Data Sharing – Financial Services Perspective

Mastercard® framed the issue by asking: "*What is the stimulus that is causing intergovernmental data sharing to happen?*" A participant from Mastercard® then stated that there are three mega-trends causing this:

i. immigration; people moving from the Global South to the Global North;
ii. the rise of the *gig economy*; and;
iii. the aggregation of data on a domestic basis.

There are some openly published principles by which Mastercard® operate which include interoperability, privacy and security, which it holds at its core. Data that crosses a network is based on the 16 digit card number, there is hardly any consumer data that passes through a network. Mastercard® believe in minimising the amount of data they collect.

"The way we see the landscape evolving is that while there have been some discussions at the intergovernmental level, we don't see much progress happening without an institution framework or policy framework to facilitate the data sharing. From a private sector lens, we would be looking to understand – what are the policy frameworks that are enabling data sharing to happen? A framework has to precede any other actions from the private sector. What we see from the financial sector perspective is the evolution of government verification services. We do not see data being increasingly moved central into a government agency. We see the continued evolution of federated identities; layers of providers that may emerge in the future that are able to connect governments who are looking to authenticate documents to issuing

bodies around the world to keep privacy and data managed. From a financial sector and evolution perspective, we are focused on keeping a privacy-centric view."

Mr. Shashi Raghunandan
Senior Vice President, Humanitarian and Development
Mastercard®

In many countries there has been an increasing movement to set up data centres within their jurisdiction so that data sharing with the Government is easier and they have more control. Governments are thus moving to more localised data regimes.

Intergovernmental Data Sharing – What Does it Mean to Create an Infrastructure to Support Identification?

A participant from 'IrisGuard' reported that 12 million, out of an estimated 30 million refugees registered in UNHCR's systems have been processed through their iris recognition system, which helps to provide refugees with an identity that is recognised by all of the States that have ratified the 1961 Refugee Convention.[27] 'IrisGuard' started working with UNHCR by focusing on identity, which was achieved by adding another biometric field to their certificate. However, over the past five years, it has morphed into providing daily authentication for services, sometimes multiple times in a single day. The 'IrisGuard' system has been running for 17 years and has processed 126 trillion matches to date.

"Robust identification, verification and payment systems powered by iris recognition technology would ensure that digital identities are protected and owned by individuals starting with verified onboarding. Private sector and non-governmental agencies, working in partnership, can enable access to financial and non-financial services within country and allow the migration of that identity across borders, whilst retaining standardised Know Your Customer (KYC)[28] requirements to ensure continuity of that identity. A clear data access framework is required for data protection. An iris biometric proof-of-life removes identity fraud and protects entitlements, is secure, anonymous, contact-free and

[2] https://www.unhcr.org/ibelong/wp-content/uploads/1961-Convention-on-the-reduction-of-Statelessness_ENG.pdf

[28] Know Your Customer (KYC) refers to the process of verifying the identity of your customer, either before or during the time of doing business with the person. KYC also refers to the regulated banking sector to identity and verify a customer to assess and monitor customer risk. The procedure fits within the broader scope of a bank's Anti-Money Laundering policy.

does not discriminate, empowering the concept of identity without borders."

Mr. Simon Reed
Deputy Director, IrisGuard

The participant from 'IrisGuard' noted that it is important to focus on how systems are setup, and the separation of the identity they provided, from the receipt of services. Digital identity is only useful if usage is being provided. It is about giving people inclusivity who have previously been excluded. It is important to establish proper proof of life of who somebody actually is. For example, 148,000 migrants have been supported by IOM to pass through 32 different countries by using biometric data.

The participant from 'IrisGuard' commented that although they provide iris recognition biometric services to UNHCR, they do not hold the biometric database and they do not share data. The database for refugees is held by UNHCR in Geneva, who is able to provide access to it for other UN Agencies or NGOs, such as the World Food Programme (WFP), through data sharing agreements.

Another example of separation is found within the financial services sector. An individual can take a Mastercard® to any country globally that accepts the card and use it by allowing the retailer to pass the Mastercard® 16 digit identifying number through the system. The retailer does not have to know anything about the individual's own identity.

The increasing fluidity of borders may be challenging the basis upon which social contracts are established. For example, when people have a legal identity, they are entitled to certain rights and benefits in a certain jurisdiction. However, a legal identity also comes with certain social contract obligations for paying taxes. When migration increases; either forced (e.g. refugees) or chosen (e.g. skilled nomads who are at the other end of the socio-economic spectrum), demands for appropriate tax regimes to enable and fulfil their social contract increases. What does that mean for intergovernmental data sharing?

What trends are the private sector seeing that might be demanded by the increase in migration?
There is a big separation between provision of services and actual identity information which does not cross borders. In Lebanon, for example, supermarkets are using blockchain technology to allow refugees to buy groceries, without knowing any information about the refugees' identity itself. Banks provide ATM services without knowing anything about the person utilising the services, but it is usually done in a very secure manner.

There are two areas of conflict:

i. identity from a government given to an individual;
ii. identity of an individual for the services the individual requires.

The participant from 'IrisGuard' noted that there will be an increase in the second form of identity, with an individual providing their identity for services, rather than the traditional

model where governments grant identity. It was stated that there will be a growing demand for digital certificates, so individuals can possess a certificate which they control and share with governments or other bodies who will provide services.

> **"There will be increasing requirement for individual to control their own identities, rather than it being imposed by governments. It's all about access to service and services can be separated from provision of movement of full identity. Individuals can be protected and have a degree of anonymity."**
>
> **Mr. Simon Reed**
> Deputy Director, IrisGuard

The facilitator summarised that the above information was a useful overview about data governance and the ability of different parties to access that data, and the consequence for rights, entitlements, and privacy. He also confirmed that there is a big movement towards self-sovereign identity which many participants confirmed they embraced.

> **"We want our consumers to have full control of their own identity, to have full control of the data they are registered with at various agencies, and to be able to use that data to avail services in a fully secure and privacy-enhancing way."**
>
> **Mr. Shashi Raghunandan**
> Senior Vice President, Humanitarian and Development, Mastercard

The roundtable was told that Mastercard® have an ID service which tackles problems of digital inclusion. Consumers can use the ID service on a smart device and access provision and services through that. For consumers who do not have the benefit of a foundational ID, which makes availing themselves of services a problem, Mastercard® provides a functional identity which allows them to authenticate themselves in a privacy-enhancing way, so that they do not have to reveal information that they do not want to.

> **"There is likely to be increased demand for governments to access the data and use it for various purposes, such as for tax regimes. The private sector is looking for institutional and policy frameworks to support that data sharing."**
>
> **Mr. Shashi Raghunandan**
> Senior Vice President, Humanitarian and Development, Mastercard

It was noted that the OECD published a report on tax where they request gig economy platform providers share data,[29] so they can determine levels of tax that can be applied. From an ID perspective, it means that as governments start collecting the data, they will see that each aspect of the data points to a different facet of the identity of the individual. There will have to be systems that are developed over a period of time to triangulate this information. This will also necessitate the development of government verification services which allow governments to validate information across various federate identities.

It was also noted that throughout the COVID-19 pandemic, the world has seen a rise in digital nomads, where people are located in many different places. There will be an increase in the technology and fintech sectors for hard-to-access skillsets of digital nomads. There is an interesting evolution occurring around trust frameworks in relation to employment credentials, and individuals coming 'ready-checked' into an organisation. Here the idea is that different credentials are curated, which have to be proven to the party requiring the verification (e.g., the employer, the bank, the property rental agency). The *Velocity Foundation Network*[30] is looking at how to remove friction when exchanging information using blockchain and letting the individual have control.

At the other end of the spectrum what has to be considered are the devices and documents people have access to, and the different types of people who need to access them, including those with disabilities and those experiencing a variety of diverse and adverse conditions. Where possible, try to ensure people can be enabled with access to a mobile device and also initially with a facial biometric.

> **"It is imperative that the private sector, public sector and NGOs collaborate to widen inclusion and consider the range of credentials that an individual could assert to prove their identity over their lifespan and how 'identity binding' can be achieved. Let us hope that some learnings from the Covid pandemic in terms of health credentials and identity binding can be transferred – here we should look at the excellent work of a wide range of bodies including the CCI,[31] VCI,[32] Good Health Collaborative, CommonPass."[33]**
>
> **Ms. Julie Dawson**
> Director of Regulatory and Policy, Yoti

[29] https://www.oecd.org/tax/exchange-of-tax-information/oecd-releases-global-tax-reporting-framework-for-digital-platforms-in-the-sharing-and-gig-economy.htm
[30] https://www.velocitynetwork.foundation/

[31] https://www.covidcreds.org/
[32] https://vci.org/
[33] https://commonpass.org/

It is also important to consider both ends of the spectrum:

i. the journey for people who are digital natives or digital nomads, and;
ii. the journey for the excluded.

All interested parties have to consider a wide breath of attributes that could be used to prove someone's identity. The governance and ethics across the spectrum are very important. Interoperability also has to be considered along with trust frameworks, with efforts to have standardisation around credentials where possible. The collaboration, currently happening on the health front, linking different parts of government, is forcing constructive dialogue.

Conclusions

The key conclusions in this session were:

- As the drivers for increased intergovernmental data sharing grow, due to elective cross-border movement, the demand for effective tax regimes and coordinated health status, it is important that the information States need to know to provide entitlements that are balanced with an individual's right to privacy and security.

- One recommendation which emerged was the adoption of the ICAO PKD[34] model as an interim solution, to verifying peoples identity, as it puts the solution in the hands of the individual.

- The rise of digital nomad visas is something to watch.

- The financial sector does not see data being centrally moved to a government agency, instead it sees the continued evolution of federated identities, layers of providers may emerge in the future who are able to connect governments who, in turn, are looking to authenticate documents globally to issuing bodies to manage privacy and data.

- The financial sector is focusing on keeping a privacy-centric view.

- Three mega-trends are currently causing the demand for intergovernmental data sharing: immigration; people moving from the Global South to the Global North; the rise of the gig economy; and the aggregation of data on a domestic basis.

- There is a distinction between identity and authentication allowing access to services.

- It is important to focus on how systems are setup, and the separation of the identity being providing versus the receipt and provision of services.

- Services can be separated from provision of movement of full identity. Individuals can be protected and have a degree of anonymity.

[34] https://www.icao.int/Security/FAL/PKD/Pages/default.aspx

- The increasing fluidity of borders for some demographic groups may be challenging the basis upon which the social contract is established.

- There is a growing interest towards trust frameworks as ways of governing decentralisation.

- There is an acknowledged conflict between; identity from a government which is given to an individual and, identity of an individual allowing access to services the individual requires.

- It was stated that there will be a growing demand for digital certificates, so individuals can possess a certificate which they control and share with governments, or other bodies, who will provide services. There will be an increasing requirement for individuals to control their own identities rather than it being imposed by governments.

- Between the private sector, and the Government, there is likely to be increased demand for governments to access data for various purposes, such as for tax regimes. The private sector is looking for an institutional and policy framework to support that data sharing.

- There will have to be systems that are developed over a period of time to triangulate information as each occurrence of the collection of data can point to a different facet of the identity of an individual.

- There will also have to be the development of government verification services that allow governments to validate information across various federate identities.

- It is important to consider both ends of the spectrum; the journey for people who are digital natives or digital nomads; and the journey for the excluded. All interested parties have to consider a wide breath of attributes that could be used to prove someone's identity. The governance and ethics across the spectrum are very important. Interoperability also has to be considered along with trust frameworks, with efforts to have standardisation around credentials where possible.

- Future work should learn from responses to the COVID-19 pandemic, both in terms of health credentials and identity binding, specifically work by bodies such as Covid-19 Credentials Initiative (CCI), VCI, Good Health Collaborative, and CommonPass.

3.7 Is there an Ideal Future National and International Legal Identity Eco-system?

If the private sector was designing an ideal legal identity system now from scratch, across the full life cycle from birth to death, what would it look like?

- State monopoly on ownership and management of the system and data?
- Biometric data as the primary identifier?
- Birth-to-death management by the same body?
- A public-private-academic-civil society 'national identity authority'?
- Unique identity across systems or multiple identities across different functional use cases?
- Right of individuals to pro-actively change or hide identity variables from the state?
- Right of individuals to opt-out?

Session six, the Concluding Dialogue, was framed as the summary of the event. The intent was to address a range of issues in the identity ecosystem, from governance to technological perspectives. The context was set by asking the question; "*Is* there an ideal future national and international legal identity eco-system?" Responses to the survey completed by participants prior to the roundtable commencing highlighted that there were diverse opinions on the topic.

The facilitator, Mr. Naman Aggarwal from Access Now,[35] stated that the session topic posed a lot of questions as it is complex to design an inclusive birth-to-death identity ecosystem.

> **"Designing an identity system is a multi-variate problem which has to be seen from a local context. What is the use case it will be used for? What is the legal environment in which it will be operating? What are the tech solutions that can be deployed for the particular use case? What are the institutional governance systems? And probably the most ignored component is the implementation – how does this solution interact with the life of a person? Are there some foundational needs which need to be addressed within the use case to make sure the people who are using the identity are able to interact with it properly?"**
>
> **Mr. Naman M. Aggarwal**
> Global Digital Identity Lead and Asia Pacific Counsel
> Access Now

[35] Access Now is a non-profit organisation, which has been working closely with UNDP on the human rights aspect of legal identity. Access Now defends the digital rights of users at risk globally.

One of the participants sought clarity by addressing definitions, stating that:

> **"There is a lot of confusion around the terminology. What we are talking about is *legal identity*, whether it be digital or physical, but it's still legal identity, which is a subtype of identity at large. Legal identity has three main characteristics: (i) it's a sovereign right given by the State; (ii) it is unique; and (iii) it is composed of data points which could be both mutable and immutable, which makes the topic complex because there are no defined data points internationally since countries have different laws and different definitions."**
>
> **Ms. Debora Comparin**
> Senior Marketing Manager, ID Systems IDEMIA
> Chair of the OSIA Initiative

Primary Component of Identity Management System

It was noted that there is no right or wrong answer regarding the question of what makes an ideal identity system, however in order to have a holistic system from birth to death, there is a need to have a primary solution for a foundational part of legal identity, which has always traditionally been a birth certificate issued by the civil registry, which acknowledges the existence of a person in front of the State.

The civil registry frequently acts as an 'update engine' for a national identity registry which is a collection of few data points that can be used to define the uniqueness of a person. The two systems, a civil registry, and a national identity registry, should be synchronised, in line with the UN Legal Identity Agenda. However, the same State or agency do not have to manage both registries.

Additional Functional Components of Identity Management System

There are a lot of other identity management systems that are functional systems which the State runs in parallel, such as tax systems, voting systems, healthcare systems, State-aid, etc. These parallel identity management systems are rooted in legal identity, but they collect different data points that are linked to core data points such as birth.

It is important that there is segregation of data in parallel identity management systems, and there is also no need to 'over-collect' data. For example, if State-aid is providing benefits to a parent who has three children, it is important to collect information that will confirm the parent has indeed three children, but it is not necessary to collect additional information about each child.

Parallel systems not only create new data points, but they also issue credentials. It is important that each of these credentials is able to be verified, recognising that they could exist in a digital or physical form.

> **"In an ideal solution, the one credential that is very important to have in a physical form is the ID card. There is discussion as to whether this can move to a digital form, but a physical credential empowers and individual to prove who they are. A physical form still has value."**
>
> **Ms. Debora Comparin**
> Senior Marketing Manager, ID Systems IDEMIA
> Chair of the OSIA Initiative

State versus Private Sector

Debora Comparin, Chair of the OSIA Initiative, stated that the State is the institution which one has a social contract with, and is the attestor of one's legal identity. The State is not only the institution that empowers people, but the State is also the institution that is accountable. It is important that the State is the authority who issues the legal identity; whereas the private sector is the technological partner. It is important to recognise that it is not easy to set up identity solutions on a national scale. There is a lot of *know-how*, not just technically, but also with implementation, training and education.

Private Sector Perspective – Google™

> **"If the question about an 'ideal' identity system was posed to group of Millennials, Baby Boomers, Generation X, or another label, the response would be significantly different. When putting forward recommendations, the UN should ask – who are you solving for: the past, the present or the future? Our capacity to grasp that we are solving for today, with a mind for the future, is critical."**
>
> **Ms. Titi Akinsanmi**
> Public Policy Lead, West and Francophone Africa
> Google™

Historically, legal identity has been solely the purview of government, but this is increasingly changing in the digital world. The concept that one State entity owns the entirety of all legal identifiers is not going to work in the future. Many people have residencies in multiple countries, for example. An individual should have the ability to present the identifiers they choose to share to access services. The ability to present various identifiers to access commercial, social, or other kinds of services and products should be something that

happens in a fluid manner. The concept of one international passport, one identity document is one that will shift to fit into the world we are evolving into.

NGO Perspective – Privacy International

> **"There is not a one-size-fits-all model. And ID systems are not being designed from scratch. There is always the context in which the identity exists – the social context, and the exclusions and discriminations in that country. The key point when looking a designing an ID system is asking – what problem is one trying to solve? And what is the evidence that it is a problem? That's necessary to make sure the system is legal in human rights terms, constitutional terms, data protection terms."**
>
> **Dr. Tom Fisher**
> Senior Researcher
> Privacy International

The position was put forward that before a system is designed, civil society has to be engaged, as they understand what is happening on the ground and what the needs of such a system are.

Private Sector Perspective – Technology Company - NEC

It was proposed that a discussion with all stakeholders (i.e., governments, private sector, civil society, and citizens) was necessary to understand all perspectives, this was felt to be important in order to think through all of the layers of the problem.

> **"Transparency and strong collaboration among stakeholders, which includes government, civil society, private sector and citizens is one of the key factors for a sustainable legal identity system. The citizen receiving the identity must know very clearly why and how this identity will be used."**
>
> **Mr. Cristiano Blanez**
> Manager, Global Relations Division, NEC Corporation

Private Sector Perspective – Software Provider - Mozilla®

The participant from Mozilla® asked whether legal identity has to be digital. Identity is not a new problem, States have been assigning identity to constituents for centuries.

> **"I think identity has become a more mainstream topic because certain technologies can solve certain problems that traditional identity systems have. While it is incredibly hard to say what an ideal legal identity system is, it is fairly easy to say what a legal identity system is not. I think one of the things is not necessarily is digital. In the majority of use cases for identity systems, there have been paper-based systems that work."**
>
> **Mr. Udbhav Tiwari**
> Public Policy Advisor, Mozilla®

The Mozilla® participant also added that it is hard to limit the scope of a unique digital identifier. If a government provided an alpha numeric code that uniquely identified every individual in its territory, it would be difficult to use it for a particular purpose requiring minimal information and nothing else. The imperatives around national security intelligence, law enforcement, and environmental situations, such as public health, support the use of a single unique digital identifier as a compelling alternative, which ignores exploitative and exclusionary risks that exist.

Governance

It was argued that biometric data does not guarantee uniqueness because biometric scanning does not work for an entire population; exception mechanisms must always be provided. It was also noted that technology for duplication is not technology for verification. Whoever is authorised to offer a biometric exception could be corrupt, and corruption is not a technology problem, corruption is a governance problem.

There will always be people in the database, who do not need to be in the database. For example, if a foreign visitor comes into a country, such as India, and is given an ID number for legal purposes, then this new ID number was created. When that person leaves they will have no use for the number. Giving rise to the question; can that identity then be faked by someone locally?

In the case of a death, the technical design of biometric data scanning does not work on dead bodies. This means that if people are in a database because of biometric data, they cannot be removed from the database through biometric scanning. If someone is able to fake a dead person's fingerprints, which, it was argued, is possible because fingerprints are easy to make, then there are two identities in a system and the technology cannot identify who is the dead person and who is the real person. Only governance can answer this question.

> **"The desire to replace technology for governance is a huge source of problem, which reflects a deeper problem – the discussion has assumed that there is a stable State, a well-behaved State, whereby technology would be used to augment the States desires and responsibilities to its citizens. An unstable State has not been accounted for; a captious State."**
>
> **Mr. Kiran Jonnalagadda**
> Co-founder and CTO, Hasgeek

There are several examples where it is justified to have multiple identities and the identity changes between documents (e.g., in naming conventions.) The example was given where the United States of America requires an individual's first name, middle name and last name to be registered separately. While India does not have a naming convention. It was further explained by the participant from Hasgeek, that he has a traditional place name as his last name which becomes his first name. When he travels to the United States of America, his middle name moves to his first name, which becomes an identity change. He is a different person in the United States of America than he is in India, which means he has two documents from two different countries with two different names on them. Having multiple legal identities is necessary to live in India. Enforcing a single database will not work. In concluding, it was stated that "*States are not stable, and identity is a negotiation between the individual and the State. To move over to technology only and to lose the negotiation with the State means that citizens will lose their rights.*"

Multi-layered Approach

The participant from *Emerge* noted that in Honduras, the multi-layered situation of public-private sector collaborations deserves more scrutiny. She emphasised that there was a lot of discussion about public-private sector collaboration from a horizontal approach, looking at system design and what role the private sector can play. What was being discussed were aspects related to function (e.g., verification, authentication), but there is a difference between collaboration for function versus defragmenting data sharing for security. There is still a lot of vulnerability as the system architecture allows for a centralised approach to data collection and data storage.

One Identity versus Multiple Identities

How do we start to think about the need for one identity versus multiple identities and fragmentation horizontally versus vertically to ensure user rights are protected? It was argued that multiple identities can mitigate risks more than one single identity can.

> **"It's very risky to have one ID for a person. It's good for tracking and profiling, but it (i) can allow governments or private sector to have control over an individual; (ii) doesn't reflect who we are as human beings, as there are changeable things; and (iii) excludes people."**
>
> **Dr. Tom Fisher**
> Senior Researcher, Privacy International

Rights

There were varying perspectives about rights. One participant suggested that the right to legal identity is a non-derogable right. It is recognised and enshrined in numerous human rights treaties.

> **"An individual holds the inherent right to their personal data. The ability to consistently ensure access to and accountability and security around it, is a shared resource."**
>
> **Ms. Titi Akinsanmi**
> Public Policy Lead, West and Francophone Africa, Google™

The participant from Google™ also stated that approximately 1.1 billion out of the approximately 7.5 billion people on earth cannot securely prove their identity. She went on to explain that this means the conversation is fragmented. There was another perspective from the participant representing *Privacy International*, where they argued that legal identity is not the same as the right to be a person before the law. Their rationale was that even people who do not have a legal identity still have a right to be a person before the law.

When it comes to the broad perspective of how rights can be protected in digital ID programmes, it was proposed that solutions can align with both technical and policy considerations. When designing technology systems there are many choices made which presume legislation will be able to account for them, which is often not the case. There are also policy solutions based on presumptions that technology will work within the solutions, which may also not be the case. At a very high level there needs to be some guidance relating to how IT systems should account for these to ensure they prevent exclusion, something which is reasonably high in current digital ID systems.

> **"Often digital identity systems are built by governments, and they are opaque systems that are only open to certain parts of the private sector. They don't have the right level of consultation that is required at the national or international level. To design proper digital ID systems, the right experts have to be consulted and the**

affected communities have to be involved. Something has to be done with those consultations and they cannot be facades."

Mr. Udbhav Tiwari
Public Policy Advisor, Mozilla®

It was also argued that accountability is extremely important and is a pre-requisite for building a well-designed identity system. In this case, accountability takes the form of regulatory measures, such as data protection (which do not exist in all countries) and technical measures, such as building certain audit systems which are made public, whereby people can contest fundamental components if necessary. The lack of accountability leads to a variety of governance issues.

Centralisation versus Decentralisation

The issue of centralisation (i.e., give one person a key and they have access to information) versus decentralisation (i.e., give multiple people keys and they have access to parts of the information to ensure there is consistent accountability and improved security) is one of context; deciding what would work in most situations, and what set of identifiers a State or governing institution needs to have to prove who the individual is.

Many people think digital ID systems should be decentralised because it reduces risk, since multiple identity systems will create a multiplicity of choices concerning how an individual utilises the system, rather than allowing failure to occur on one centralised system due to malicious or non-malicious behaviour. Decentralisation combines the benefits that technology offers, with the benefits of traditional paper-based identity systems.

It was noted that trust is a core requirement for any system to work, but is complex because multiple stakeholders are involved.

"Our ability to engage with and securely identify people is one that has multiple players, across multiple layers who have varying roles to play at any point in time."

Ms. Titi Akinsanmi
Public Policy Lead, West and Francophone Africa
Google™

Engagement of Private Sector and Government

How much is the private sector able to influence the conversation about what an ideal identity system is? Is the private sector simply developing a system based on the needs of the State as they define it? Does the private sector have a set of minimum common principles of what they will, and will not, do when designing identity systems? Is there a consensus across the industry?

Technology versus Governance

The private sector, it was argued, does not have the power to define the governance of identity systems. The private sector provides and implements a defined solution for a defined purpose. It was also noted that 'private sector' is a phrase that represents different industries.

> **"I represent the identity industry, which is comprised of private sector players that have experience and expertise in setting up digital identity management systems for governments. In the past, this was the issuance of physical credentials. Then there was the introduction of another industry linked with the internet. These two industries are trying to meet halfway to try to build a web identity infrastructure. Where there was a need in the past for a physical credential to be issued to prove a citizen's identity, now there is a need for the private sector to issue data points or credentials."**
>
> **Ms. Debora Comparin**
> Senior Marketing Manager, ID Systems IDEMIA
> Chair of the OSIA Initiative

The private sector is starting to work together on best practices in technology. For example, the OSIA Initiative[36] was launched, which was aimed at bringing around interoperability. It was recognised that it was time to end the monolithic big end-to-end solutions that governments were purchasing to manage foundational, and sometimes functional, identity systems. It was important to break the solutions into modules which could be interoperable with each other and sold by different vendors. This would allow a government to facilitate multi-source procurement.

There are ethical practices which the private sector follows around privacy, and the use of data. For example, there were sensitivities around the use of biometric data linked to surveillance of individuals.

> **"NEC follows a Framework of Ethics in terms of providing solutions. If we think there could be a misuse or it could cause harm, we won't do it."**
>
> **Mr. Cristiano Blanez**
> Manager, Global Relations Division
> NEC Corporation

[36] https://secureidentityalliance.org/osia

Interoperability

Interoperability is essential, but what is meant by interoperability? When there is a need for multiple identities which are interoperable, who controls that interoperability? Does the user control their data where they can define who can access it, or does the State control the interoperability, where different ministries are able to exchange data? In *Access Now's* view, interoperability does not occur if ministries are sharing data; rather, that is viewed as data exchange.

> **"Technology and governance have to be isolated, in terms of the actors who are responsible for it, but they also have to be unified when it comes to the impact of its users. Interoperability also has to be within the control of users. There is a scope for the identity industry to interact more with civil society as that would allow technology and governance to come together in a more transparent way."**
>
> **Mr. Naman M. Aggarwal**
> Global Digital Identity Lead and Asia Pacific Counsel
> Access Now

It was emphasised by the participant from *Privacy International* that civil society are experts in local contexts. It was also highlighted that interoperability does not just exist between different agencies, or across different solutions, to verify credentials and data points. It also exists between components within a single identity management solution, be it foundational or functional.

> **"What I see as interoperability is to allow someone to have services that can be replaced at any time. It can be scaled by another provider, or a component can be exchanged or replaced without any harm to the entire architecture."**
>
> **Mr. Cristiano Blanez**
> Manager, Global Relations Division, NEC Corporation

It was argued that privacy will be better controlled from an end user perspective if individuals have control of their information.

> **"It should be user driven when someone is trying to share their data, information and attributes. This will be good for privacy and good for individuals."**
>
> **Mr. Vikas Malhotra**
> Founder and CEO, WOPLLI

What are the barriers when it comes to interoperability, are multiple identities with different use cases the answer?

Power Differentials

What does control actually mean when it comes to identity transactions? Often the people who have power over someone are the same people asking for identity (e.g., employer, landlord, police, etc.). Having control to provide identity information is not just about consent, it is about power differentials – why does any individual have to share their data and what will the other party do with it? Solutions are hard to derive, and strong regulatory structures are required.

It was noted also noted by the participant from *Privacy International* that "*there is a lack of transparency when it comes to governments and international organisations in their dealings with identity systems. People do not have control of what the system is. Civil society organisations have challenges in getting basic information out of States and organisations rolling out systems.*"

Differential Authentication Standards

When it comes to one identity, or biometric identities, the highest standard is being created for managing risks to the rights of users. This raises the question, is there a need for different standards of authentication based on different situations?

> **"Whenever identity systems are designed, they should always be done in consultation with the local communities, keeping local contexts in mind. If this were done, then in a vast majority of scenarios, most criteria would be met, such as offering multiple choices, having alternatives to technological measures and things would automatically fall into place because they are necessary for any identity system to work at scale."**
>
> **Mr. Udbhav Tiwari**
> Public Policy Advisor, Mozilla®

The participant from Mozilla® argued that the broader international development community played a role in promoting the benefits of digital identity, which may exceed the truth and reality of what a digital identity actually does. They argued that digital identity has been positioned as a solution to problems that nation states have been dealing with for many decades. He stated that frameworks need to be in place to guarantee the level of privacy and security for its citizens, and residents, against whom those digital ID systems are being implemented.

Terminology

It was recommended to have a common vocabulary of identity versus identifier and legal identity versus digital identity because people's understanding and usage of the same terminology is different.

Proof of legal identity is provided by either a birth certificate or national ID card/number. People often interchange the terms digital identity and digital ID which is incorrect. A person can have many digital identities (e.g., Facebook profile, Google™ account, etc.), but the same person usually only has one digital ID, which is often understood to mean a digital version of that person's legal identity.

> **"There is a distinction between *identity* versus *identifier*, and *legal identity* versus *digital identity*. Legal identity is unique. There cannot be different manifestations of legal identity, especially when it comes to functions like voting. Digital identity, which is not legal identity, can have different manifestations of a persona, which means the identity online depends on the context. Identifiers or credentials can be different in different single functional registries."**
>
> **Ms. Debora Comparin**
> Senior Marketing Manager, ID Systems IDEMIA
> Chair of the OSIA Initiative

> **"We are aiming for a system that is effective, secure, inclusive and trustworthy, whether it is for legal or digital identity. In the context of legal identity, we are looking for effective, secure, inclusive and trustworthy legal identities in a participatory model that is relevant for the local context it is being used for."**
>
> **Ms. Titi Akinsanmi**
> Public Policy Lead, West and Francophone Africa
> Google™

Conclusions

Key conclusions from the final session were:

- An ideal legal identity system does not exist because context matters, and systems have to account for a local context.
- Multiple identities, or interoperable identities, are preferred over one single identity.
- Designing an identity system is a multivariate problem which has to be seen from a local context. Questions which need to be considered are:
    i. what will it be used for?;
    ii. what is the legal environment;
    iii. what are the technology solutions?;
    iv. what are the institutional governance systems?;
    v. how will the system be implemented?;

vi. are there foundational needs which have to be addressed to ensure people who are using the identity will be able to interact with it properly?

- There is confusion around terminology. Legal identity, where it be digital or physical, is a subtype of identity at large. Legal identity has three main characteristics: it is a sovereign right given by the State; it is unique; it is composed of data points which could be both mutable and immutable, which makes the topic complex because there are no defined data points internationally since countries have different laws and different definitions.

- To have a holistic system stretching from birth to death over the lifespan of an individual, there should be primary components (a civil registry for a birth certificate and a national identity registry). The primary components should be synchronised, but do not have to be managed by the same agency. There are parallel functional management systems to manage tax, voting, healthcare, State-aid, etc. where there should be a segregation of data. All parallel systems should have verifiable credentials.

- When putting forward recommendations, the question should be asked – who are we solving problems for? Is it solvinf problems for the past, the present or the future, as Baby Boomers, Generation X and Millennials will all have a different perspective on what an ideal identity system is? It is critical to understand that problems which are being solved in the present, must also consider what is likely to happen in the future.

- The concept of one international passport, one identity document is something that will shift to fit into the world we are evolving into.

- There is no one-size-fits-all model. There is always a context in which identity exists, including the social context and the exclusions and discriminations that exist within that context.

- All stakeholders should be engaged (i.e. governments, citizens, private sector) before designing a system. This will ensure that the problem is reviewed from all perspectives.

- Corruption is not a technology problem; corruption is a governance problem. Replacing governance with technology does not help in addressing this.

- There is a difference between public-private sector collaboration for function (i.e., verification or authentication) versus de-fragmenting data sharing for security. There still are a lot of vulnerabilities as the system architecture allows for a centralised approach to data collection and data storage. It was highlighted that a multi-layered situation has to be considered in more detail.

- The right to legal identity is a non-derogable right. It is recognised that it is enshrined in numerous human rights laws. About 1.1 billion out of the approximately 7.5 billion people on earth, however, cannot securely prove their identity. This means that the conversation is fragmented.

- Often digital identity systems are built by governments, they are often opaque systems that are only open to certain parts of private sector. They do not have the right level of consultation that is required at the national or international level. To design proper digital ID systems, the correct experts have to be consulted and the affected communities have to be involved. In order for those consultations to be meaningful, something useful has to emerge which can influence policy and/or practice.

- Accountability is extremely important and is a pre-requisite for building a well-designed identity system. In this case, accountability takes the form of regulatory measures, such as data protection, which does not exist in all countries, and technical measures, such as building certain audit systems which are made public, whereby people can contest fundamental components, if necessary. The lack of accountable results leads to a variety of governance issues.

- The issue of centralisation (i.e., give one person a key and they have access to information) versus decentralisation (i.e., give multiple people keys and they have access to parts of the information to ensure there is consistent accountability and improved security) is one of context; deciding what would work in most situations, and what set of identifiers a State or governing institution needs to have to prove who the individual is.

- Many people think digital ID systems should be decentralised because it reduces risk.

- Individuals hold the inherent rights to their personal data. The ability to consistently ensure access to, and accountability and security around it, is a shared resource.

- The private sector, it was argued, does not have the power to define the governance of identity systems. The private sector provides and implements a defined solution for a defined purpose. It was also noted that 'private sector' is a phrase that represents different industries.

- The OSIA Initiative[37] was launched which was aimed at bringing interoperability.

- It was highlighted that interoperability does not just exist between different agencies, or across different solutions, to verify credentials and data points, but it also exists between components within a single identity management solution, be it foundational or functional.

[37] https://secureidentityalliance.org/osia

- There is scope for the identity industry to interact more with civil society because that would allow technology and governance to come together in a more transparent way. Civil society are experts in local contexts and therefore need to be engaged.

- Frameworks need to be in place to guarantee the level of privacy and security for citizens and residents, against whom digital ID systems are being implemented.

- Two industries, the ID industry, and the web/internet industry, are starting to collaborate to bring legal identity to the ID web infrastructure.

- It was recommended to have a common vocabulary of *identity* versus *identifier* and *legal identity* versus *digital identity* because people's understanding and usage of the same terminology is different.

- Legal identity is unique. There cannot be different manifestations of legal identity, especially when it comes to functions like voting. Digital identity can have different manifestations of a persona.

- We are aiming for a system that is effective, secure, inclusive, and trustworthy, whether it is for legal identity or digital identity.

- Transparency is important in order to provide the best service.

Pilot birth registration linking health sector with civil registration in DR Congo. Nurses and midwives are using tablets equipped with an application and the information is communicated in real time to the Civil Registry (photo: UN Economic Commission for Africa)

UNDP staff with biometric registration kits in the Supreme Commission on Elections and Referenda (SCER) warehouse in Sana'a, Yemen, 2012. (photo: Niall McCann, UNDP)

4. Summary of the Roundtable

The main points which were expressed during the roundtable were:

- Legal identity is a sovereign right.
- A birth certificate is the gold standard of legal identity in which an individual can be empowered to access rights.
- The ability and right for people to change their identities and have new identities issued and recognised by governments is important.
- Consultation with all stakeholders (government, private sector, civil society) must occur before digital ID systems can be designed and implemented.
- Every country should have some forum where digital rights advocates, women's groups, academics, researchers, marginalised communities, foreign migrants, refugees, the private sector, political actors and the Government can come together to discuss complex issues and design identity systems that empower individuals, rather than exclude or disenfranchise them.
- As countries work towards embracing digital identity, they need to develop strong public-private partnerships at a national level, especially in the Global South to ensure that digital infrastructure and digital literacy is in place.
- There is not an 'ideal' legal identity system. Context matters in the way identity is looked at and used, as identity is dynamic over the lifecycle of a person. The social context, and the exclusions and discriminations in that context matter.
- There is a complementary role between the public and private sector. The traditional model, which is the dominant model, does not have to be completely changed. There are situations where outsourcing to the private sector can make sense in achieving the traditional model. The private sector could verify legal identity in a decentralised manner, but collection of data could be centralised via the State.
- *Legal identity should be unique*, but *digital identity does not have to be*.
- For people to trust the State controlling identity, it must offer safety, security, inclusiveness (no discrimination) and efficiency (affordable and sustainable). We are aiming for a system that is effective, secure, inclusive, and trustworthy, whether it is for legal or digital identity.

- Government should be an authority on the establishment of foundational identity; however there needs to be a degree of control by the citizen so they can decide which elements to disclose for specific purposes.

- Granting identity is not a lightweight responsibility of the State. It has an obligation to protect an individual's rights despite the type, and volume, of identity which is gathered. This includes the most basic data, such as name (which can reveal religion) and gender.

- There should be a legitimate purpose, transparency, consent, and control of data subjected to data sharing - this builds trust in services.

- There is a distinction of identity as a human right and identity as an asset; one which is used as a means to access to services.

- Identity has served both as an excluder, and an includer throughout history.

- The move to digital identity is a journey with the ultimate goal of providing more control, privacy, and trust to individual citizens over the use of their identity attributes, whilst reducing the risk of creating a single entity which is viewed as being of 'high value' for hackers.

- Emerging decentralised identity technologies provide a path forward to support governments to do what they do well and let citizens, and businesses, transact and connect without the need for the Government to act as an intermediary.

- It was expressed that not having an ID should never be a barrier to obtaining a vaccine or vaccine credentials. This means alternative measures and safeguards have to be put in place to prevent exclusion and discrimination.

- Some private sector participants articulated that physical documents will still be here for at least two to three decades, if not more. The primary reasons are the time it will take for inclusion, as well as technology adoption throughout the whole ecosystem.

- The level of adoption of digital IDs will vary geographically because of different economic factors, cultural values, attitudes, levels of literacy and the maturity and costs of ICT infrastructure.

- Systems that are being designed should cater for the possible eventual elimination of a physical ID card, however, a physical card may always be required as a back-up, especially in the Global South, where infrastructure is still a long way away from having a centralised ID system.

- Internet penetration is different in different States. The digital divide has to be addressed and adequate internet penetration, and uptake, has to be reconciled before the elimination of physical documents can be effective.

- Blockchain may be the strongest tool for identity becoming digital in terms of trust, but that transition will not occur in the short-to medium-term.

- Governments could use digital distributed ledgers/blockchain technology at a national level to create strong, clean ID records in the future.

- When it comes to identity, there are many things that need to work: legal framework; technology framework; institutional framework; and implementation framework.

- Globally we are in the process of re-evaluating the social and legal salience of identity categories such as gender, sexuality, and marital status. There could be a future where gender, or other identifiers, are not relevant categories for accessing government services.

- The financial sector does not see data being centrally moved to a government agency, instead it sees the continued evolution of federated identities. Layers of providers may emerge in the future who are able to connect governments who, in turn, are looking to authenticate documents globally to issuing to manage privacy and data.

- Three mega-trends are currently causing the demand for intergovernmental data sharing: immigration (people moving from the Global South to the Global North); the rise of the gig economy, and; the aggregation of data on a domestic basis.

- There is a distinction between identity and authentication for services.

- There is a growing interest towards trust frameworks as ways of governing decentralisation. Participants in the private sector are working hard on building out governance systems that can work for many different industries and different purposes.

- It was stated that there will be a growing demand for digital certificates, so individuals can possess a certificate which they control and share with governments, or other bodies, who will provide services. There will be an increasing requirement for individuals to control their own identities rather than it being imposed by governments.

- Designing an identity system is a multivariate problem which has to be seen from a local context. Questions which need to be considered are:
    i. what will it be used for?;
    ii. what is the legal environment;
    iii. what are the technology solutions?;
    iv. what are the institutional governance systems?;
    v. how will the system be implemented?;

vi. are there foundational needs which have to be addressed to ensure people who are using the identity will be able to interact with it properly?

- Corruption is not a technology problem; corruption is a governance problem. Replacing governance with technology does not help address this.

- Accountability is extremely important and is a pre-requisite for building a well-designed identity system. In this case, accountability takes the form of regulatory measures, such as data protection, which does not exist in all countries, and technical measures, such as building certain audit systems which are made public, whereby people can contest fundamental components, if necessary. The lack of accountable results leads to a variety of governance issues.

- The issue of centralisation (i.e., give one person a key and they have access to information) versus decentralisation (i.e., give multiple people keys and they have access to parts of the information to ensure there is consistent accountability and improved security) is one of context; deciding what would work in most situations, and what set of identifiers a State or governing institution needs to have to prove who the individual is.

- Many people think digital ID systems should be decentralised because it reduces risk.

- The private sector, it was argued, does not have the power to define the governance of identity systems. The private sector provides and implements a defined solution for a defined purpose. It was also noted that 'private sector' is a phrase that represents different industries.

- Two industries, the ID industry, and the web/internet industry, are starting to collaborate to bring legal identity to the ID web infrastructure.

- There is a scope for the identity industry to interact more with civil society because that would allow technology and governance to come together in a more transparent way. Civil society are experts in local contexts and therefore need to be engaged.

- Legal identity is unique. There cannot be different manifestations of legal identity, especially when it comes to functions like voting. Digital identity can have different manifestations of a persona.

- It is difficult to define what is legal identity and how to use it. Lessons could be learnt from the medical ethics industry which has faced similar issues relating to the control of identity data.

- Future work should learn from responses to the COVID-19 pandemic, both in terms of health credentials and identity binding, specifically work by bodies in the private sector.

- A disaster recovery plan, or model, has to be developed if digital processes become the primary method or proving identity.

- It is important to focus on how systems are setup, and the separation of the identity being providing versus the receipt and provision of services.

- Between the private sector and the Government there is likely to be increased demand for governments to access data for various purposes, such as for tax regimes. The private sector is looking for an institutional and policy framework to support that data sharing.

- There will have to be the development of government verification services that allow governments to validate information across various federate identities.

- It is important to consider both ends of the spectrum; the journey for people who are digital natives or digital nomads; and the journey for the excluded. All interested parties have to consider a wide breath of attributes that could be used to prove someone's identity. The governance and ethics across the spectrum are very important. Interoperability also has to be considered along with trust frameworks, with efforts to have standardisation around credentials where possible.

- There is confusion around terminology. It was recommended to have a common vocabulary of *identity* versus *identifier* and *legal identity* versus *digital identity* because people's understanding and usage of the same terminology is different.

- Legal identity, whether it be digital or physical, is a subtype of identity at large. Legal identity has three main characteristics: it is a sovereign right given by the State; it is unique; it is composed of data points which could be both mutable and immutable, which makes the topic complex because there are no defined data points internationally since countries have different laws and different definitions.

- In order to have a holistic system stretching from birth to death, encompassing the lifespan of an individual, there should be primary components (a civil registry for a birth certificate and a national identity registry). The primary components should be synchronised, but do not have to be managed by the same agency. There are parallel functional management systems to manage tax, voting, healthcare, State-aid, etc. where there should be a segregation of data. All parallel systems should have verifiable credentials.

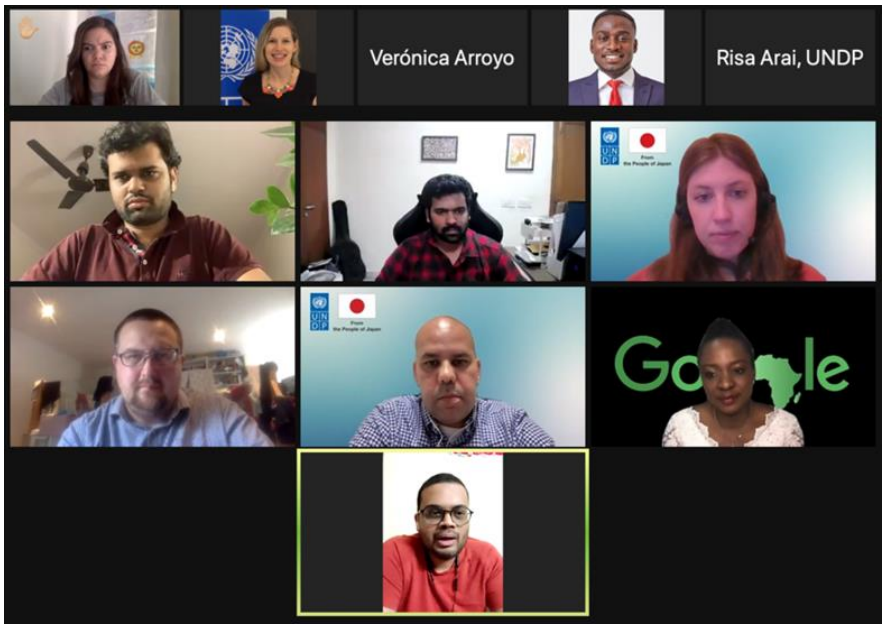
- When putting forward recommendations, the question should be asked – who are we solving problems for? The past, the present or the future? Baby Boomers, Generation X and Millennials will all have a different perspective on what an ideal identity system is. It is critical to understand that problems which are being solved in the present, must also consider what is likely to happen in the future.

- There is a difference between public-private sector collaboration for function (i.e., verification or authentication) versus de-fragmenting data sharing for security. There still are a lot of vulnerabilities as the system architecture allows for a centralised approach to data collection and data storage. It was highlighted that a multi-layered situation has to be considered in more detail.

- Frameworks need to be in place to guarantee the level of privacy and security for citizens and residents against whom digital ID systems are being implemented.

- Transparency is important in order to provide the best service.

A selection of screen shots taken during the roundtable.



5. Literature

Below is a list of links to relevant documents and internet-based resources.

- United Nations Legal Identity Agenda Task Force Guidelines: Maintaining Civil Registration and Vital Statistics during the COVID-19 Pandemic (living document)
- Guidance to UNDP Country Offices on the privacy, data protection and broader human rights dimensions of using digital technologies to combat COVID-19
- UN Strategy on Legal Identity for All
- UN Legal Identity Agenda website
- Principles and Recommendations for a Vital Statistics System (Revision 3)
- Handbook on Civil Registration and Vital Statistics Systems: Management, Operation and Maintenance (Revision 1)
- Handbook on Civil Registration, Vital Statistics, and Identity Management Systems: Communication for Development (Draft)
- Guidelines on the Legislative Framework for Civil Registration, Vital Statistics, and Identify Management
- Survey results on how Member States are conducting Civil Registration and Vital Statistics services under COVID-19

6. Annexes

Annex I: Biographies (Bios) of Moderators and Speakers

Welcome and Opening

Bio – Ms. Sarah Lister

Head of Governance, UNDP

Sarah Lister is UNDP's Head of Governance and oversees policy and programme support to its governance portfolio globally, which includes electoral cycle support, parliamentary development, anti-corruption, legal identity, youth empowerment and disability inclusion. She has more than 25 years' experience working on democratic governance, including civic engagement, media and communication, social accountability, public administration reform and governance measurement. From 2015-2019 she was the Director of UNDP's Oslo Governance Centre where she led the team bridging research, policy and practice on governance and peacebuilding in transitional contexts, with a particular focus on Sustainable Development Goal 16. She worked previously for UNDP, BBC Media Action, the Afghanistan Research and Evaluation Unit in Kabul and the Institute of Development Studies, UK. She has also consulted for multilaterals, bilaterals, think-tanks and NGOs. She has lived and worked in Asia, Africa, Latin America and Europe. Sarah holds a PhD and MSc in Social Policy from the London School of Economics, and a BA in History from Cambridge University, UK.

Master of Ceremonies

Bio – Mr. Niall McCann

Policy Advisor/Project Manager, Legal Identity Advisor, UNDP

Niall McCann is UNDP's Policy Advisor and Project Manager on Legal Identity, based at the UNDP office in Brussels. In this position, he provides programming and advisory support to UNDP Country Offices engaged in supporting national civil registration and identity management schemes (approx. 30 per year), as well as contributing to the development of the UN's policy on civil registration, national identity schemes, privacy, data protection, and regulating the use of biometric technologies.

Session 1: Ownership, control, and management of legal identity systems and data

Bio – Dr. Joseph Atick (Moderator)

Executive Chairman, ID4Africa

Dr. Joseph Atick is a recognised, world-renowned advocate and expert on identity matters. As one of the founders of the identity industry nearly 30 years ago, he has led several companies in that domain and developed some of the foundational algorithms underlying secure digital identity today, including the first commercially viable face recognition algorithm. He retired from the industry in 2010 to focus on promoting identity for social and economic development around the world. In that mission, he partnered with the World Bank and other UN agencies, and was heavily involved in the development and field testing of the methodology and analytic tools that would guide the subsequent activities in that space, and lead to the launch of the IDA4D initiative at the World Bank. In 2014, he co-founded ID4Africa as a pan-African Movement to promote responsible digital rights and continues to provide counsel to governments and international organisations on the use of identity for public good. Dr. Atick holds a Ph.D. in Mathematical Physics from Stanford University.

LinkedIn: https://www.linkedin.com/in/dr-joseph-j-atick-13b6b0a/

Speaker - Session 1

Bio – Ms. Titi Akinsanmi

Public Policy Lead, West and Francophone Africa, Google™

Titi Akinsanmi is a public policy thought leader on the digital economy focused on shaping the enabling environment needed for innovation. She has spent the last two decades globally advising and delivering on laws and policies connecting the public, civil and private sector. Her areas of expertise include discerning which, where and how public policies are used to harness digital opportunities while mediating emerging tensions, building allies and addressing gaps.

Within Google™ she leads the West and Francophone Africa cluster, Academia regional and international policy institutions engagements; and drives the work of the team as it pertains to Privacy, Identity & Data protection, access, AI and digital governance.

She served as a Berman Klein Fellow from 2018-2020 (Faculty of Law, Harvard University), an advisory member for the World Economic Forum's Global Future Council on the Digital Economy and on the strategy and advisory team for WEF on Digital Identity. She sits on the board of non-profit organisations including the Yemi Shyllon Museum of Arts, Junior Achievement Nigeria and, Afrilearn, amongst others. She holds a Master's Degree in Law specialising in Privacy and Cybersecurity (Osgoode Law School, York University) and a Master's in Public Policy & Development Management (University of Witswatersand).

Speaker - Session 1

Bio – Mr. Yiannis Theodorou

Senior Director, Digital Identity Programme and Policy & Advocacy, GSMA

Yiannis Theodorou is a Senior Director within the GSMA's Mobile for Development (M4D) Group and leads the Digital Identity programme as well as several policy and advocacy initiatives in Development and Humanitarian contexts. He is currently exploring the role of mobile and government policy in accelerating digital identity ecosystems to support the digital and financial inclusion of underserved populations (focusing on women and refugees). He has been researching and advising governments and mobile operators on Mobile SIM registration and Know-Your-Customer (KYC) regulations across Africa, Asia, the Middle East and Latin America.

Yiannis also delivers several Capacity Building courses on 'Mobile for Development' topics and represents the GSMA at various public fora globally, closely engaging with key partners such as the World Bank and UN bodies.

He previously led public policy initiatives and related to the use of Big Data for Social Good and the Internet-of-Things, focusing on consumer data protection and Privacy-by-Design. He authored a number of reports and policy recommendations on these topics. Prior to GSMA, Yiannis was a Strategy Associate at the UK regulator Ofcom, developing strategic and regulatory policy insights across the Internet, TV, and telecommunications sectors. Yiannis holds a MSc. in Management from Cass Business School and a Law Degree from UCL (London).

Speaker - Session 1

Bio – Ms. Natalie Smolenski

Senior Vice President, Business Development, Hyland Credentials

Natalie Smolenski leads business development for Hyland Credentials, a solution for verifiable digital credentials anchored in blockchain technology. As an author and public speaker, she focuses on the intersections of identity, technology, and government. By bringing a scientific perspective to distributed digital technologies and social transformation, she helps audiences from all backgrounds understand how individuals connect to form communities and build the infrastructures of the future.

Session 2: Ownership, control, and management of legal identity systems and data (continued)

Bio – Ms. Stépahnie de Labriolle (Moderator)

Marketing Director, Secure Identity Alliance (SIA)

Stéphanie de Labriolle is Marketing Director of the Secure Identity Alliance, the organisation dedicated to supporting the provision of legal, trusted identity for all, and to driving the development of inclusive digital services necessary for sustainable, worldwide economic growth and prosperity. She has been coordinating and implementing the Alliance's programme since creation of the Alliance in 2013.

Prior to this, she has held several Global Marketing and Communication Director roles within blue chip, private sector and non-profit B-2-B companies. During that time, she oversaw and drove the launch of many products, services and partnership projects across Europe, Asia and America. Stéphanie graduated in English from Montpellier University, France and in Business Studies from Nottingham Trent University, UK.

Speaker - Session 2

Bio – Mr. Jean-François (Jeff) Lennon

Vice President of Strategic Sales & Global Partnerships, Vision-Box

Jean-François (Jeff) Lennon is Vice President of Strategic Sales & Global Partnerships at Vision-Box, a leading provider of Seamless Travel and Digital Identity Solutions. He is a Senior Executive with over 20 years of experience in the security and digital technology industries. Jeff's career broadened his market insights and expanded his international experience by opening and growing markets throughout the world.

Since joining Vision-Box in 2012, Jeff embarked on wide-ranging projects spearheading the exponential growth of the company. He currently leads strategic sales and partnerships on a global basis and is a key contributor to the scaling plans of the company. Jeff has a growing reputation as an industry thought leader and digital ID evangelist, combining his proficiency in transversal entrepreneurship and strategic thinking with a profound understanding of transformational trends.

Speaker - Session 2

Bio – Mr. Dan Butnaru

Senior Advisor Digital Identity, Atos

Dan Butnaru is a Senior Advisor Digital Identity, working in the "Digital ID" Business Unit, part of the Atos BDS Cybersecurity Products division which develops Public Key Infrastructure products for public and private sectors, electronic signature, and related digital identity solutions.

As Senior Expert with almost 25 years of professional experience in the fields of digital identity, cryptography, public key infrastructure, e-banking and smart cards, Dan has sound knowledge in eGovernment projects, such as e-ID and e-Passport infrastructures.

Speaker - Session 2

Bio – Mr. Calum Bunney

Systems Software Produce Manager, Citizen ID, HID Global

Calum Bunney has worked on both government and supply sides of government ID management for more than twenty years. His focus has been on end-to-end solutions building, and on specific technology development around biometrics, PKI, and digital identity components.

Session 3: Digital vaccine certificates and the future role of health data in identity systems

Bio – Ms. Jhalak M. Kakkar (Moderator)

Programme Manager ,Technology & Society,
Centre for Communication Governance (CCG) National Law School, Delhi

Jhalak M. Kakkar leads the work of the Technology and Society team at the Centre for Communication Governance (CCG), National Law School, Delhi, India. CCG is the only academic research centre dedicated to working on information law and policy in India. CCG seeks to embed human rights and good governance within the information policy and examine the evolution of existing rights frameworks to accommodate new media and emerging technology. It seeks to protect and expand freedom of speech, right to assembly and association, and the right to privacy in the digital age, through rigorous academic research, policy intervention, capacity building and support to litigation.

Jhalak works across pressing information law and policy issues such as data governance/protection, privacy, legal identity, platform regulation and design, misinformation, governance of artificial intelligence, and surveillance, and manages the programmatic work of the Technology and Society team. She is the Indian representative at the Asian Dialogue on AI Governance (a collaborative initiative between the Singapore Management University and Microsoft).

Prior to this role, she was a Visiting Researcher at Harvard Law School (HLS) focused on the governance of artificial intelligence, mass surveillance and facial recognition, and the regulation of fintech and blockchain. She has also served as an Editor on the Harvard Journal for Law and Technology. Additionally, she was part of the founding Board of the HLS Blockchain and Fintech Initiative and has since been an advisor to the Board.

Jhalak began her career at PRS Legislative Research, New Delhi, India and spent six years at PRS working across various roles to provide non-partisan analysis to Indian federal state legislators on policy, budgets and legislation. She led PRS' engagement with members of Parliament and provided them with analytical input and briefings on the cross-section of legislative and policy issues. Before this role, she was an analyst with the research team at PRS tracking legislation, budgets and policy on science, technology, strategic affairs and natural resources.

Jhalak graduated with an LLM from Harvard Law School, Cambridge, US on a Fulbright-Nehru Masters Fellowship. She has a five-year integrated social science and law degree from the National University of Juridical Sciences, Kolkata, India.

Speaker - Session 3

Bio – Mr. Daniel Bachenheimer

Principle Director - Digital Identity, Accenture

Mr. Daniel Bachenheimer is the Technical Lead within Accenture's Digital Identity Innovations organisation and has been designing and delivering identity solutions for various clients for over 20 years including; Department of Homeland Security US-VISIT, Unique Identification Authority of India (UIDAI) Aadhaar, UNHCR, BIMS, CBP Trusted Traveller Programs, Transportation Security Administration Transportation Worker Identification Credential (TSA TWIC), World Economic Forum Known Traveller Digital Identity (WEF KTDI). Dan is the ISO/IEC SC37 (biometrics) liaison officer to ISO TC307 (blockchain), participated in Trust Over IP's Technology and Governance Stack Working Groups and is an IEEE Certified Biometrics Professional. He is also a contributing member of: ID2020's Technical Advisory Committee, International Association for Trusted Blockchain Applications (INATBA)'s Identity working group, and MOBI's Vehicle Identity standards, is vice-chair of IATA's Identity Management Working Group, is a Biometrics Institute Director, and has contributed to World Economic Forum and World Bank reports related to identity.

Speaker - Session 3

Bio – Ms. Kaliya Young, MSIMS[40]

'Identity Woman'

Kaliya Young known as "Identity Woman" is the Ecosystems Director at the Covid Credentials Initiative and co-chair of the Interoperability Working Group for Good Health Pass at Trust over IP Foundation. She co-founded the Internet Identity Workshop in 2005. She is the author of The Domains of Identity: A Framework for Understanding Identity Systems in Contemporary Society and A Comprehensive Guide to Self-Sovereign Identity. In 2012 she was named a Young Global Leader by the World Economic forum and in 2017 she received a Master of Science in Identity Management and Security from UT Austin. In January 2020 she was featured in Wired UK.

[40] Master of Science in Identity Management from University of Texas at Austin.

Speaker - Session 3

Bio – Sir Jonathan Montgomery

Professor of Health Care Law, University College London

Sir Jonathan Montgomery is the Professor of Health Care Law at University College London, UK. He is also chair of Oxford University Hospitals NHS Foundation Trust, and co-chair of the Moral and Ethical Advisory Group within the Department of Health and Social Care for England, UK. In 2021, he led an expert deliberation for the Ada Lovelace Institute on vaccine passports (https://www.adalovelaceinstitute.org/report/checkpoints-vaccine-passports/).. He has previously chaired a number of national bioethics bodies, including the Nuffield Council on Bioethics, the Health Research Authority and the Human Genetics Commission.

His research focuses on health care law and governance of bioethical issues. In addition to academic publications, he has been involved in developing guidance for health professionals and policy-makers. This has included work on confidentiality for the General Medical Council and co-authoring a chapter on 'ethics and the social contract for genomics in the NHS' in the Chief Medical Officer for England's report for 2017.

He was knighted for services to bioethics and healthcare law in the 2019 New Year Honours and elected Fellow of the Academy of Medical Sciences in 2021.

Session 4: Is the clock ticking for paper and plastic?

Bio – Ms. Kaliya Young (Moderator)

'Identity Woman'

Kaliya Young known as "Identity Woman" is the Ecosystems Director at the Covid Credentials Initiative and co-chair of the Interoperability Working Group for Good Health Pass at Trust over IP Foundation. She co-founded the Internet Identity Workshop in 2005. She is the author of The Domains of Identity: A Framework for Understanding Identity Systems in Contemporary Society and A Comprehensive Guide to Self-Sovereign Identity. In 2012 she was named a Young Global Leader by the World Economic forum and in 2017 she received a Master of Science in Identity Management and Security from UT Austin. In January 2020 she was featured in Wired UK.

Speaker - Session 4

Bio – Mr. Kenichi Nakamura

Technology Liaison Department, Innovation Strategy Office, Panasonic Corporation

Kenichi Nakamura is working in the Innovation Strategy Office of Panasonic Corporation. He is an active ISO/IEXC JTC1/SC17 expert working on Machine Readable Travel Documents and ISO-compliant Driving Licenses. Kenichi recently focused on the standardisation of digital credentials such as Digital Travel Credentials (DTC), Mobile Driving License (mDL) and Mobile IDs.

Speaker - Session 4

Bio – Ms. Natalie Smolenski

Senior Vice President, Business Development, Hyland Credentials

Natalie Smolenski leads business development for Hyland Credentials, a solution for verifiable digital credentials anchored in blockchain technology. As an author and public speaker, she focuses on the intersections of identity, technology, and government. By bringing a scientific perspective to distributed digital technologies and social transformation, she helps audiences from all backgrounds understand how individuals connect to form communities and build the infrastructures of the future.

Speaker - Session 4

Bio – Mr. Lyle Charles Laxton

Founder and CEO, Laxton Group

Lyle Charles Laxton is the founder and CEO of the Laxton group of companies. Laxton is a global leader in providing cost effective, high-technology Election, Identity and Security systems to governments and corporations. Lylie is a qualified Chartered Accountant (Deloitte) and has over 17 years of experience designing robust processes and leveraging key technologies to implement secure biometric identity management solutions in order to reduce the immense operational risks and associated costs in the key verticals of civil identity, elections, border control and law enforcement.

Session 5: International identity data sharing and granting of access of foreign states to sovereign identity databases

Bio – Dr. Emrys Schoemaker (Moderator)

Researcher and Advisor on Digital Transformation, Caribou Digital

Dr. Schoemaker is a researcher and advisor on digital transformation with a focus on digital identity at Caribou Digital and the London School of Economics. He has extensive experience researching the use and implications of digital technologies in the Global South and advising governments, the World Bank and UN amongst others on ways to influence digital transformation towards human centred outcomes.

Speaker - Session 5

Bio – Ms. Julie Dawson

Director of Regulatory and Policy, Yoti

Julie Dawson is known internationally for driving the ethical framework development at Yoti digital identity platform.

Julie leads regulatory and government relations for Yoti digital identity platform; developing policy approached for fraud prevention and safeguarding, liaising with national and sectoral trust frameworks, in conjunction with Yoti's internal and external ethics boards.

Julie is an authority in digital identity policy, ethics and governance. She represents Yoti at numerous fora including the World Economic Forum Digital Identity Innovators' techUK Public sector, Data Ethics and Digital Identity Boards, ADA Lovelace Citizens Biometric Council Oversight Board, the All Party Parliamentary Group for Digital Identity, the Sprite + Network – Security, Privacy, Identity, and Trust Engagement Network, IEEE SA Children's Advisory Group, OSTIA Online Safety Tech Industry Association, and Project Member of the Centre for Digital Citizens.

Julie has a proven track record for developing advanced strategic insight, impactful thought leadership, stewarding strategic opportunities, and differentiated policy positioning.

Speaker - Session 5

Bio – Mr. Shashi Raghunandan

Senior Vice President,
Humanitarian and Development, MasterCard

Shashi Raghunandan leads the Network Services team at MasterCard, responsible for building products for Humanitarian and Development organisations. In his role, Shashi is responsible for designing and building the digital rails (like identity and payments) for Mastercard's products for the under-served communities.

Most recently, Shashi was the Personal Payments Solutions (PPS) product lead for Asia Pacific, where he has been responsible for drawing out the product strategy and executing upon it for the region. Prior to this Shashi worked at Mobile Payment Solutions (MPS), a joint venture between MasterCard and Smart Hub Inc., where he was the product solutions expert delivering mobile payment services and solutions with several of the market programs. He has extensive experience in financial services, and has held previous roles in JP Morgan Chase, Times of Money and ICICI Bank. He has a Master's degree from the Indian Institute of Management Ahmedabad and his undergraduate degree from the Indian Institute of Technology Madras. Shashi loves to paint and play tennis in his free time.

Speaker - Session 5

Bio – Mr. Simon Reed

Deputy Director, IrisGuard

Simon Reed has over 25 years of senior level international experience in strategic business marketing and technology developments and has helped to set-up and chair several industry forums (the SIMalliance and Java Card Forum) which have shaped the mobile communications and payments world we currently live in.

He has worked with specific software/VM platforms such as Java, EMV banking and ID / biometric usage and has consulted for several Asian countries and global clients such as Bain, Goldman Sachs, BT, AT&T, Telefonica, and Orange.

Previously he was Applications Director at Morpho in Germany as part of the global €30 billion French defence and aerospace specialist Safran Group (Formerly Sagem/Org, GmbH), one of the world's top four companies that specialises in smart cards, systems, and software. Here he helped card product growth from €50 million to over €300 million in turnover.

Working with IrisGuard, Simon has been instrumental in the development and now the extension of their global transactional business into the mobile money sector working with a number of verticals including humanitarian assistance, healthcare and pharma, social payments and Fintech.

He is a recognised international speaker and a world expert in the implementation of SIM's eSIM's and applications for the global GSM mobile telecommunications and internet and security marketplaces. Simon is degree level educated and has several post degree qualifications including the Henley Centre Chartered Institute of Marketing and Pirbeck Sales Training.

Session 6: Concluding Dialogue: Is there an ideal future national and international legal identity eco-system?

Bio – Mr. Naman M. Aggarwal (Moderator)

Global Digital Identity Lead and Asia Pacific Counsel, Access Now

Naman M. Aggarwal serves as the Global Digital Identity Lead and Asia Pacific Policy Counsel for Access Now, based in Delhi. Naman is also the Founder of Crux – a new media initiative for communicating policy and socio-political issues to millennials. Before Access Now, he worked with Nishith Desai Associates, an Indian law firm with their Technology, Media, and Telecommunication team. He has completed law from the University of Delhi and is also a Computer Science Engineer.

Speaker - Session 6

Bio – Ms. Titi Akinsanmi

Public Policy Lead, West and Francophone Africa, Google™

Titi Akinsanmi is a public policy thought leader on the digital economy focused on shaping the enabling environment needed for innovation. She has spent the last two decades globally advising and delivering on laws and policies connecting the public, civil and private sector. Her areas of expertise include discerning which, where and how public policies are used to harness digital opportunities while mediating emerging tensions, building allies and addressing gaps.

Within Google™ she leads the West and Francophone Africa cluster, Academia regional and international policy institutions engagements; and drives the work of the team as it pertains to Privacy, Identity & Data protection, access, AI and digital governance.

She served as a Berman Klein Fellow from 2018-2020 (Faculty of Law, Harvard University), an advisory member for the World Economic Forum's Global Future Council on the Digital Economy and on the strategy and advisory team for WEF on Digital Identity. She sits on the board of non-profit organisations including the Yemi Shyllon Museum of Arts, Junior Achievement Nigeria and, Afrilearn, amongst others. She holds a Master's Degree in Law specialising in Privacy and Cybersecurity (Osgoode Law School, York University) and a Master's in Public Policy & Development Management (University of Witswatersand).

Speaker - Session 6

Bio – Mr. Cristiano Blanez

Manager, Global Relations Division, NEC Corporation

Cristiano has more than 20 years of experience working with ICT Solutions. He is an expert in Biometrics and Public Safety solutions with extensive experience in the South American region, working on projects for the public and private sectors. In recent years, Cristiano began working for NEC Corporation in Japan to support United Nations organisations achieve the Sustainable Development Goals (SDGs), working actively in several initiatives in Africa, South Asia and Latin America.

Cristiano is Brazilian with a degree in Electrical Engineering and a post-graduate degree in Computer Networks.

Speaker - Session 6

Bio – Ms. Debora Comparin

Senior Marketing Manager, ID Systems, IDEMIA
Chair of the OSIA Initiative

Debora Comparin is Senior Marketing Manager, ID Systems at IDEMIA and the Chair of the OSIA initiative. She is a strong advocate for interoperability in the identity market with the aim of building an open and sustainable ecosystem that drives innovation and competition for the benefits of governments and citizens. She has mobilised the identity industry towards this goal, launching the OSIA Initiative. OSIA is an interoperability framework as a set of Open Standards APIs/interfaces to connect public and private sector identity management building blocks.

Speaker - Session 6

Bio – Mr. Udbhav Tiwari

Public Policy Advisor, Mozilla®

Mr. Udbhav Tiwari is a Public Policy Advisor for Mozilla® where he works towards keeping the internet open, secure and accessible by advocating for progressive regulations in the technology sector. He primarily focuses on data governance, content regulation and connectivity in the Asia-Pacific region. He has also worked with the public policy team for Google™ and the Centre for Internet and Society (CIS). Udbhav was also a Co-Rapporteur at the International Organisation for Standardisation (ISO), participated actively at the Institute of Electrical and Electronics Engineers (IEEE) and was a part of India Todays' 'India Tomorrow' list in 2020.

Speaker - Session 6

Bio – Dr. Tom Fisher

Senior Researcher, Privacy International

Dr. Tom Fisher is a senior researcher and heads the work on digital identity at Privacy International, a London-based NGO which works with global partners to advocate for legal and technological solutions to protect people and their data from exploitation. Dr. Fisher has a PhD from the University of Edinburgh and has researched digital identity around the world including in Africa, South America and Asia.

Annex II: Survey Questionnaire

This survey questionnaire collected initial ideas from the participants during the registration process to encourage an interactive dialogue during the roundtable.

SESSION I - PLENARY – PART I

Ownership, control and management of legal identity systems and data

Q1: Do you think that UN Member States will or should – outsource specific elements of legal identity management to the private sector in years to come?

- ☐ Yes
- ☐ No
- ☐ Partially

If yes or partially, which elements (granting of legal identity? Database management?)

Q2: Do you think that there are alternatives to centralised government management of legal identity that would elicit greater public trust?

- ☐ Yes
- ☐ No
- ☐ Partially

If yes or partially, what should the alternative models be?

SESSION II - PLENARY – PART II

Ownership, control and management of legal identity systems and data (Continued)

Q3: How much control can, or should an identity data subject (citizen or resident foreigner) reasonably expect to have over their data?

- ☐ Government has exclusive management and control
- ☐ Government should manage but citizens should have authority to (check where applicable):
  - ☐ Instruct the state to hide or change data on public-facing documents (e.g., sex/gender or date of birth)
  - ☐ Unilaterally change data in the database to reflect self-identity (e.g., sex/gender)
  - ☐ Unilaterally hide or delete data in the database to reflect self-identity (e.g., ethnicity, religion, where recorded)

Q4: Will distributed ledger technology / blockchains have any roles in organising/archiving civil and national population registers in the coming years?

- ☐ Yes
- ☐ No
- ☐ Partially

If yes or partially, what role?

SESSION III - DIGITAL VACCINE CERTIFICATE

Q5: Do you believe vaccination data (e.g., such as COVID-19 or other vaccination data currently included in the 'yellow vaccination book' such as Hepatitis, Yellow Fever, etc.) will 'go digital' in coming years?

☐ Yes
☐ No

Q6: If yes, do you think such data will form part of a person's passport data, either hidden or public facing?

☐ Yes
☐ No

Q7: What additional data, if any, is likely to be added as core identity variables to legal identity systems in coming years? (e.g., biometrics, digital wallet, DNA, voting, driving, access to public services)

Q8: What additional data should NOT be added to legal identity systems?

SESSION IV - IS THE CLOCK TICKING FOR PAPER AND PLASTIC?

Q9: Do you think that UN Member States will still be issuing paper and plastic identity document in 10 years' time?

- ☐ Paper/plastic credentials will continue to be issued as standard
- ☐ Paper/plastic credentials will only be issued in addition to digital credentials
- ☐ Paper/plastic credentials will be completely replaced by digital credentials

Can/should paper and plastic identity credentials retain legal primacy over digital ones?

- ☐ Yes
- ☐ No

Q10: In legal identity systems where biometrics play an increased role, do you think that names, or other identity variables such as gender, will become less important to both individuals and states?

- ☐ Yes
- ☐ No

SESSION V - ACCESS OF FOREIGN STATES TO SOVEREIGN IDENTITY DATABASES

Q11: Do you expect that there will be an increase in intergovernmental agreements to access core national identity databases in order to verify paper and/or digital credentials in years to come?

☐ Yes
☐ No

Do you think that migration, and the need to apply appropriate tax regimes based on residence, will mean more intergovernmental identity data sharing?

☐ Yes
☐ No

CONCLUDING DIALOGUE: WHAT COULD BE ELEMENTS OF AN IDEAL NATIONAL AND INTERNATIONAL LEGAL IDENTITY ECOSYSTEM?

Q12: What do you think is the ideal legal identity ecosystem?
(Select the component you think most appropriate from each component)

Data Ownership
- ☐ Government-Monopoly
- ☐ Individual has more power to change/edit/verify data
- ☐ Others

Identifier
- ☐ Biometrics
- ☐ Non-biometrics
- ☐ Combination of biometrics and non-biometrics

Governance
- ☐ CRVS and ID under the same authority
- ☐ CRVS and ID under separate authorities

Governing Institutions
- ☐ State Monopoly
- ☐ A public-private-academic-civil society 'national identity authority'

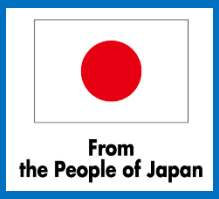
Centralization / De-Centralization
- ☐ Unique identity across systems
- ☐ Multiple identities across different functional use cases
- ☐ A 'third way' in between (e.g., interoperability between functional identities derived from a source foundational legal identity)

Software Code

Open-Source (code is publicly available e.g., Firefox browser)
- ☐ Proprietary (code is privately held e.g., Microsoft Edge browser)
- ☐ Government-controlled (code is owned and maintained by government)

Why?

This activity is funded by the kind contribution
from the Government of Japan



United Nations Development Programme

Bureau for Policy and Programme Support (BPPS)
One United Nations Plaza 1
New York, NY 10117, USA

www.undp.org