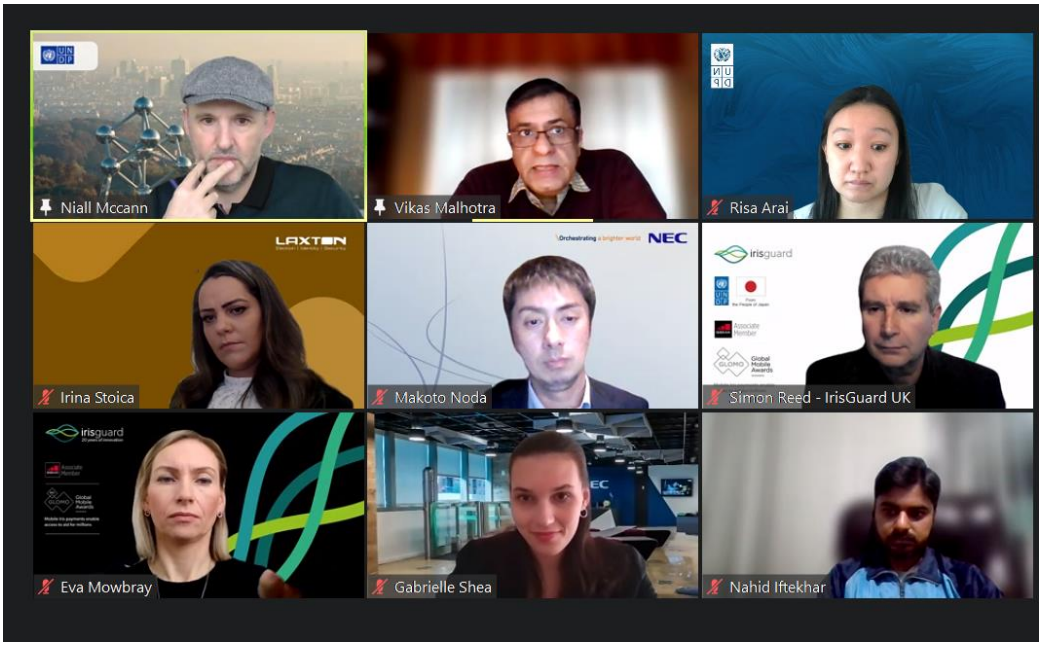
UNITED NATIONS DEVELOPMENT PROGRAMME (UNDP) LEGAL IDENTITY AGENDA ONLINE FORUM: PRIVATE SECTOR ENGAGEMENT ROUNDTABLES: DATA PROTECTION AND PRIVACY

ROUNDTABLE REPORT



FEBRUARY 10, 2022

Table of Contents

Acknowledgement

This event was hosted by UNDP BPPS Governance Legal Identity team led by Niall McCann (Policy Advisor on legal identity) and Risa Arai (Programme Specialist of Legal Identity). This report was prepared by an online UNV, Karen Rhoda Mutiso, under the guidance of the legal identity team.

1. Overview

1.1. Introduction, Contextual Background and Objective

A second Private Sector Engagement Roundtable was held on February 10, 2022 building on the first roundtable held in May 2021. The forum drew 74 virtual participants. Hosted by the UN Legal Identity Agenda (LIA) Task Force[1], the roundtable with members of UN entities and the private technology sector addressed, core questions about data protection and privacy, as well as policy issues concerning legal identity systems.

As his opening remarks, Mr. McCann (Policy Advisor/Programme Manager (Legal Identity), UNDP) provided contextual background to help guide the discussion, as follows:

1.1.1. UN Legal Identity Agenda

"UN LIA is not focusing on private identities or self asserted identities for social media access, but identities with which individuals can assert their rights as either citizens, resident aliens, refugees or migrants in foreign countries."

Policy advisor Legal identity UNDP, Niall McCann

- The UN has partnered with the World Bank, ID4 Africa, and Biometrics Institute to assist hundreds of millions of people worldwide who are unable to prove their identity and consequently denied access to public and private services.

- The UN has been supporting Member States for a number of years in developing various forms of national population registers, national identity registers, and national ID card schemes that are linked to the core civil registration function. Many of these schemes are now becoming entirely digital in nature.

- Member States have a tendency to prioritize digital legal ID schemes, which are primarily rolled out to support adults. However, this approach has a risk of children and other vulnerable people being left behind, because less investment goes into the birth registration system.

- It is critical that the digital legal identity system takes into account death registration by ensuring that dead people are removed from the databases to avoid major credibility issues—that is, a lack of public trust in the accuracy of the databases when it is discovered that dead people still exist in the database.

1.1.2. Objective of the Second Roundtable

- The objective of this roundtable discussion was to engage with the private sector and discuss some of the key policy issues surrounding the legal identity system—specifically, data protection and privacy.

- The discussion was guided by the following three key questions/points:

    1. What data protection and privacy standards help in the design of your products, particularly for customers in countries/regions without detailed data protection and privacy standards?**;**
    2. When developing and marketing digital identity and biometric technologies and services, whose needs are you planning your products for; government, business partners, or data

[1] The UNLIA task force comprises all UN entities involved in supporting UN member states in ensuring everybody on the planet has a legal identity, which allows an individual to be represented before the law. UNDP, UNICEF and the UN Department of Economic and Social Affairs (UNDESA) co-chair the UN legal Identity Agenda Task Force.

subjects/citizens?**;**

3. The centrality of biometric data in 'linking' digital identities across government systems, and 'control' of biometric data.

- At the same time, a couple of major policy themes were tabled for discussion, which include:
    - The role of cryptocurrencies and government regulation: Do you see a future in which the government provides its citizens with a 'official' digital wallet and sends them public stipends in cryptocurrency?;
    - Merger of health data and civil registration data: Do you believe there will be some sort of merger between the two data systems that will allow health data, such as vaccination data, to become a core part of a person's identity data variables?;
    - Centralized or decentralized identity system: Do you believe that government should move away from centralising identity systems and data and instead decentralize identity systems and data in a way that puts more power in the hands of individuals?;
    - Metaverse: What is the relationship between a person's real identity and their identity in the metaverse? Will names become obsolete, and will identity be verified solely by biometrics?

2. Discussion Summaries

2.1. Panelists

This engagement roundtable brought together the following panelists from the private sector:

- Irina Stoica, Laxton Group
- Gabrielle Shea and Makoto Noda, NEC Corporation
- Eva Mowbray and Simon Reed, IrisGuard UK Ltd
- Nahid Iftekhar, CodeMarshal IT System Ltd

2.2. Initial Remarks by Panelists

The introduction session also provided the panelists with an opportunity for collective reflection and stocktaking on the efforts being made by the private technology sector towards data protection and privacy in the context of the UNDP Legal Identity Agenda.

a) Irina Stoica, Laxton Group

As a manufacturer of multimodal biometric systems, Laxton:

- Covers just a small part of the process at the end of an integrated enrolment and verification system. Therefore, Laxton cannot solely ensure all the data protection, but it does cover endpoint security and encryption;
- Educates its customers on the fact that it is fundamental to ensure only minimal data is collected in order to develop a unique biometric identity;
- Constantly conducts research and development to ensure that its devices can be integrated with the latest technologies, and meet the highest standards.

b) Eva Mowbray and Simon Reed, IrisGuard UK Ltd

The success of IrisGuard UK Ltd innovations, which have been transforming the world of humanitarian aid since 2001 by providing iris recognition electronic payment solutions, can be attributed to the following factors that were considered during the design process:

- Lessons learned during the designing process of systems that work;
- The time dedicated to acquire knowledge;
- Provision to work together with those intended to operate the system, and;
- Display of good practices where there are ubiquitous globalized systems.

The United Nations High Commissioner for Refugees (UNHCR) case was recounted, in which:

- IrisGuard UK Ltd systems were rolled out over a five-year period, effectively working across international borders and utilising services centralized as one database in Geneva, within a fully General Data Protection Regulation (GDPR) environment;
- Has a functional system which separates personal information from a unique digital identity number generated during the verified onboarding process. No personal information, only the unique digital number is used during the transactional process. Similar to a debit card process, the information it relates to does not pass through the transactional system.

c) Gabrielle Shea and Makoto Noda, NEC Corporation

Appreciating the joint discussion on data protection and privacy in the context of legal identity, the following was alluded:

- The forum afforded NEC Corporation the opportunity to share information and best practices gleaned through its 120 years of experience in advanced communication and IT services that helps promote safety, security, fairness, efficiency and a more sustainable world in which all people have the opportunity to reach their full potential;
- Governance frameworks for AI technology need to reflect input from and be applicable for diverse stakeholders, be use case-specific for risk-based decision-making, and be committed to protecting privacy, civil rights and civil liberties, racial and border social justice, and safety security accounts.

d) Nahid Iftekhar, CodeMarshal IT System Ltd

Highlighted the following fundamental questions for deliberation:

- Determine who the system solution being designed is intended for. Is it for the subjects or people to be identified, or for companies providing services?;
- Nobody buys identification; instead, they buy a solution or a service. As a result, identity is used to obtain services from entities other than the provider of identification, such as a financial institution. So, what are the potential challenges that should be considered in light of this?
- What is the primary goal of identification? Is it creating data security or an easy onboarding system for everyone who is currently unable to use standard identification solutions?;

- How do we protect data or who owns the data?

After the initial remarks, the panelists shared their experiences through the discussions therein addressing the gaps in data protection and privacy with proactive dialogue on the urgency of solutions, guided by the following priority questions:

2.3. What data protection and privacy standards help in the design of your products, particularly for customers in countries/regions without detailed data protection and privacy standards?

Context Setting by UNDP

- Designed by the European Union (EU) to harmonize data privacy laws across all its member states, GDPR has been in operation for a number of years; though not without its challenges. The Data Protection Officer of an organization with its headquarters in one of the EU member states, is responsible for enforcing GDPR standards to that organization on behalf of the rest of the EU. This presents a challenge to the government, the EU, and the organization, particularly for major American technology companies with their headquarters in the EU.

- It was acknowledged that solutions need to be sought for contexts where there are no intergovernmental global standards for instruments similar to GDPR. In one case, a government has asked UNDP to assist in the design and implementation of a new national ID card system that will register everyone over the age of 14, but the country's data protection law is non-existent. At the same time, assisting them in developing a data protection law that will govern how citizen data is captured digitally and with biometric data capture from each citizen. Deliberations were therefore focused on the private technology sector's approach to balancing upholding global human rights standards in the area of data protection against performance standards when working in countries with no data and privacy law.

- Data must remain anonymous in order to protect the beneficiaries and their entitlements. This necessitates determining who to entrust with data collection, storage, protection, management, and use. In addition, declining to facilitate data that will result in an invasive public portrayal or display of extremely sensitive personal data. In recent years, the United Nations Statistical Commission and the Economic and Social Council have approved standards outlining how specific data should never be collected, and how data linking to an individual should never appear on a public facing identity credential or document.

Highlighted Remarks from Panelists and Discussants

1. In the case of IrisGuard UK Ltd Internal policies stipulate custodianship and ownership of personal data. The financial world has an extremely protective regulatory standardization system, which moves trillions and trillions of dollars around. Hence caution should be taken when building a system that hooks into very internationally standardized environments. There are various ISO standards for both hardware devices and software systems that have to go through for instance, camera, cloud-based systems with the security levels mandated on database management of hooking into firewalls and IP.

2. In April 2019 NEC finalized a set of principles called, NEC Group AI and Human Rights Principles: 1) Fairness; 2) Privacy; 3) Transparency; 4) Responsibility to explain the effects, value, and impacts of AI utilization; 5) Proper utilization of AI technology; 6) Continued development and improvement of AI technologies; and 7) Dialogue with multiple stakeholders.

   NEC collaborates with customers around the world not only to design and deploy customer technological solutions, but also to facilitate multijurisdictional compliance and to consider any ethical issues that may arise. The NEC privacy policy and personal information protection management system mandate handling personal information in accordance with the requirements of Japan's Act on the

Protection of Personal Information and JISQ 15001. This is the Japanese industrial standard for the safe and appropriate management of personal information in corporations' and other organizations' operations. Additionally, the Corporation has developed and implemented data breach response procedures. However, since data privacy and data protection laws are not universal, guidance on how to ensure digital ID solutions comply with global privacy laws in jurisdictions where privacy laws and regulations do not exist is lacking. In this case, the EU GDPR and other national and regional privacy laws may offer guidance on how to address concerns about digital ID data privacy.

3. According to Ms. Stoica, the approach chosen may determine project winning or loss, particularly when added prerequisites intended to ensure delivery of a properly built system are not taken into consideration by end customers as well as other potential bidders. In the case where GDPR is a standard, she explained that in order to use a service, a person must consent to the use of their personal data. As a result of this conversation, Mr. McCann recommended anonymizing information with reference to the debit card transactional system previously shared by Mr. Reed.

4. Mr. Iftekhar noted that there are new services awaiting a good identification solution, yet there are countries unable to design a specification for identity providers. He added that a long turnaround time is expected when dealing with the government in countries where a standard specification like GDPR has not been adopted because a lot of time and money is spent on device specifications.

5. Dan Bachenheimer of Accenture suggested that focus ought to be made on establishing uniqueness within a population, which is a function of the government.

"This can be facilitated through decentralized identity constructs where foundational identity constructs can be maintained while functional basis proofs are shared, which may or may not include actual personal information."

Dan Bachenheimer, Accenture

2.4. When developing and marketing digital identity and biometric technologies and services, whose needs are you planning your products for; government, business partners, or data subjects/citizens subjects/citizens?

The discussion in response to this question covered critical points with the panel sharing their experienced challenges when navigating delivery of service while meeting the needs of the clients, who may be the government or a public sector body and the needs of the subjects/citizens being registered.

Highlighted Remarks from Panelists and Discussants

“The private sector has to make money, which drives innovation, improvements in technology and amazing services that we all benefit from throughout the world.”

Simon Reed, IrisGuard UK Ltd

“Safety, fairness and trust in digital systems is fundamental in forming architecture principles that are human centered providing control to a person, and that advocate decentralized identity constructs.”

Vikas Malhotra, WOPLLI Technologies

"The success of a technology company largely depends on how well citizens/subjects embrace the designed technology. The usability and trust in the technology are therefore paramount to success."

Irina Stoica, Laxton Group

“Aside from developing systems that uphold privacy standards, digital solution providers should also focus on working in partnership with the state, to implement security standards for ID registration.”

Isabelle LANDREAU, IDEMIA

“Working with partners to think through how to innovate on social value, which is important to NEC's business ecosystem and economic value, can help not only tackle short-term challenges, but also align everyone's interests more closely to the citizens' interests in the longer term.”

Gabrielle Shea and Makoto Noda, NEC Corporation

- Mr. Reed also emphasized that the private sector is bottom-line oriented, and needs are prioritized and met based on who pays the bills.

Most prominently, the following solutions were recommended as important considerations for success:

- The private sector needs to pursue marketing strategies that will raise visibility and create awareness to both the beneficiaries and implementers of the system, while distinguishing between the use of foundational identity and functional identity. The acquired information will enable the organization implementing the system to translate the service delivery of the technology so that it becomes acceptable and usable, fit for purpose for the end users and subjects.

- Identity solution providers to be granted the freedom to focus on product innovation and improvement. While an authorized body assumes the role of conscience in determining whether the provided solution is in accordance with people's rights.

- In an environment where data privacy law is absent, NEC ensures delivery to its customers while meeting societal expectations applicable throughout the world by:

    - Staying up to speed on what different groups are recommending on similar issues;

    - Sharing best practice guidance resources with customers, and getting their opinions on those resources;

    - Talking to the people who would be affected by the use of the technology concerning how they feel about the technology, and;

    - Adopting strategies to build public trust in the context of various deployments.

2.5. The centrality of biometric data in 'linking' digital identities across government systems, and 'control' of biometric data.

Context Setting by UNDP

- Birth registration or birth certification is the gold standard of legal identity. Every person in the world is entitled to it and should have it from birth. As previously mentioned, the government may opt to introduce purely digital ID schemes such as core National Identity Registers, national population registers, and National ID Card schemes. They should be linked with the core birth registration system for several fundamental reasons. These types of schemes may also be referred to as, Foundational Identity Registers. If, for example, an individual does not have a birth certificate, or their birth was never registered, or it was registered but the certificate was never issued, or it was issued but was lost or stolen, or the individual destroyed their own document out of fear of being identified as a member of a vulnerable population, or the state records were destroyed. In such a context when there is no record of a birth certificate and the individual enrolls in a core digital identity scheme or core National Population Register scheme, that becomes the foundational identity register. The identity with which one can assert one's public and human rights as a citizen, resident, foreigner, or refugee, for example.

- Questions were raised in the case where two competing foundational identities exist as a result of an existing digital identity register; either in the form of a plastic or digital identity credential with a different name or gender than what was recorded in the birth register. In this instance:

    - Which of them has legal primacy?;

    - Which of them is the core identity of a deceased person? Is it the one on the birth certificate or on the digital identity credential?

- Regardless of other identity variables, biometrics provides a means to connect foundational identities in such a way that name and gender become less important. It is an absolute way of tracing an individual from birth all the way through life. Since biometrics will predominantly influence use of functional identities in the private sector then it could be inferred that names, gender and other core identity variables will have less importance within foundational identity systems.

- In addition, private technology companies have designed technology identity systems that allow for zero knowledge proofs, etc. Unfortunately, a few countries do not uphold the right to privacy. Hence, questions considered an invasion of privacy are still asked, and people are required to prove and hand over their personal identity data that is irrelevant to the function that an individual wishes to perform. Presenting documents to prove a bona fide marriage to a private sector entity such as a hotel is an example.

Highlighted Remarks from Panelists and Discussants

The key outcomes were discussed in the following order:

a) Irina Stoica, Laxton Group

- Names and gender are labels therefore, actual identity is more than a set of data that defines a person.

- However, there is no general rule regarding use of biometrics to define foundational identity. This may only be applicable to a number of countries while for other countries the birth certificate or paper based identity card is used to define identity as regulated by their own policy frameworks and identities infrastructure.

b) Simon Reed, IrisGuard UK Ltd

- Biometrics will play a more significant part in providing that absolute proof of life without the requirement for other items. Going forward, the world will change slightly to allow individuals to federate their own identities. The birth certificate may contain biometric data, which is capable of storing a complete set of information that an individual chooses to use as their identity. In addition, in order to provide the required services, a service provider may accept or decline the said certificate. As a result, putting power back to the individual, and this can occur across a wide range of demographics, cultures, and countries.

- George Orwell's fictional vision of the future introduces the concept of chips implanted at birth, which could be explored as a form of universal identity. Although it could be argued that this is already happening by default because the vast majority of the world's population owns mobile phones with embedded chips.

- Further discussions are required regarding managing identities and their legal implication on issues such as:

    - Who is paying the taxes?;

    - Where to pay taxes?;

    - Who pays taxes for one to exist within a country and have access to health services?

c) Gabrielle Shea, NEC Corporation

- Biometrics are important identity features; however, there is no single, generic credential that is entirely satisfactory on its own for the diverse needs of societies around the world. Depending on the unique context of each use-case, different forms of biometric and non-biometric identity verification and authentication could be offered.

3. Summary Conclusion of the Roundtable

The shared responses to the questions below were as follows:

1) Emrys Schoemaker, Caribou Digital

a) There are numerous constituents among private sector solution providers. Customers include states and other consumers who purchase their technology. Furthermore, they have made commitments to users in terms of privacy and data protection principles, among other things. Recognizing that there will inevitably be times when purchasing technology necessitates access to or use of data that users may choose not to provide; where and how will private sector solution providers address this?

Respondent: Vikas Malhotra, WOPLLI Technologies

Private solution providers should never grant anyone (including their customers) access to data that individuals have chosen not to provide. If an incident occurs in which things are awry between the two parties because of upholding ethical standards, the service provider should be willing to walk away from such business.

b) The move to greater user control over personal data by using Zero Knowledge Proof and Data Tokenization techniques is a welcome direction. However, technology providers who advocate for greater control deal with individuals who are reluctant to take control of their personal data?

Respondent: Vikas Malhotra, WOPLLI Technologies

Companies choose to build technology and innovate based on their core values. The companies will then have the opportunity to deal with customers and people who share a similar inclination and direction toward innovation. It could be inferred that alignment of goals in terms of providing data privacy techniques aimed at building a better social value context attracts the right set of people willing to take control of their personal data. It is also a matter of providing individuals with the choice to control their data, which they do not currently have. It is not a matter of reluctance, but rather of a lack of control.

2) John ErikSetsaas, Signicat AS

a) How can approaches like data guardians and data trust, for example, be established to resolve some of the emerging issues?

Respondent: Dan Bachenheimer, Accenture

The International Civil Aviation Organization (ICAO), for example, has introduced biometric passports/e-passports/digital passports as a strategy to improve global border management and security. The achievements made possible by digital signing could be attributed to an underlying trust ecosystem. Almost 200 member states meet regularly to decide what information will be shared and how it will be protected. Furthermore, a few countries have a visa waiver program because they trust certain countries' passport issuance processes. Because biometrics are already probabilistic, matching biometric information when it is encrypted is extremely difficult. Although there are emerging matching techniques that use encrypted or hashed biometrics (to improve privacy), Type I (false rejects) and Type II (false matches) errors should be expected to increase.

3) Frank Hersey, Biometric Update

a) What is the appropriateness of marketing digital identity solutions in a competitive space?

Respondent: Eva Mowbray, IrisGuard UK Ltd

Digital identity solution providers appeal to a diverse audience. As a result, the messaging that is distributed must resonate with a variety of roles within each of these organizations. Whether it is an internal business analyst looking to improve the efficiency of the process, a vendor assessing the system and its security, or the operational teams who are ultimately responsible for running it in the field. Moving forward, collaboration among the various segments prior to and after system installation should be considered. By combining the story, the impact, and the benefits, a complete picture of the entire solution is presented.

Aside from the questions, the following insights/recommendations were shared:

1) Irina Stoica, Laxton Group

- Digitality has become a self-service platform where unsecured devices and networks are used to register subjects. Therefore, securing identities starts with a program. Every element of the entire identity enrolment and verification process, whether for fundamental or functional identity use, must be secure. must be secure. This is how a combination of two different faces, for example, can easily pass any type of facial recognition.

- Interoperability issues remain widespread and unresolved around the world. To begin, there is a need to standardize at least what the minimum identity entails.

2) Eva Mowbray, IrisGuard UK Ltd

- Based on the use of collected data, the terms foundational identity and functional identity could be defined. Furthermore, data should be collected with the intent of using it, not just for the sake of collecting it.

- The humanitarian sector is interested in populations who have lost their identity, with a focus on verified onboarding. As a result, biometrics are crucial in this context, because good information in, equals good information out.

3) Makoto Noda, NEC Corporation

Furthermore, digital ID systems must be interoperable with other systems such as civil registries and sub data providers, as well as allow for the plug-and-play functionality of various components. This will avert the risk of the vendor lock while increasing data portability across systems.

4) Nahid Iftekhar, CodeMarshal IT System Ltd

Solutions for how service providers can easily deploy biometric-based identification and biometric-based onboarding into their services should be provided.