DIGITAL IDS:
A PATHWAY TO INCLUSION OR A BARRIER TO ACCESS?

1. History of identification of persons

Over time, societies have developed different methods of identifying individuals, influenced by cultural norms, security requirements, and technological advancements. From ancient markings and community-based identification methods to National Identification cards and biometric ID systems, identification systems have developed.
The introduction of national ID systems, which exist in many countries, has enabled governments to 'effectively' manage populations, distribute' services, and 'increase' security.

In ancient civilizations, identity was conveyed through various markers that evolved over time and differed by region. In ancient Egypt , names were crucial, symbolizing life and securing immortality, with added identifiers such as origins and genealogy becoming prominent later . Seals authenticated documents in Greco-Roman Egypt , while other African societies used oral traditions, family ties, and physical markers. In Greece , identification included one's name, paternal and tribal affiliations, or ethnic origins, particularly distinguishing free citizens from slaves. In Rome , the three-part Roman name system detailed citizenship, family, and origin, reflecting social complexity. Ancient China used names and hometowns for taxes and military duties, relying on written records to enforce rules, with seals enhancing trade reliability. In medieval England and France , surnames established noble identity and control, linking families to estates, while commoners adopted occupational or geographic names for legal and social differentiation.

.

In the 19th century, colonial governments formalized identification systems for control, tax collection, labor organization, and migration tracking. Civil registers recorded citizens' details, improving governance and fiscal efficiency. The early 20th century saw the emergence of passports , which became essential for controlling movement across borders. Industrialization introduced fingerprinting in colonial India, which later spread to Europe and North America, and photography enabled mugshots to link faces to identities . During the World Wars, national ID systems expanded to manage resources and control movement.

Today, biometric IDs are common globally, with systems like South Africa's, India's Aadhaar, Kenya's Huduma Namba, and Nigeria's ID system, each with a unique identifier tied to biometric data that is designed to enhance security and streamline access to government services.

2. General Principles that Govern Digital I.Ds

Digital identity systems are massive databases that collect, store, and track sensitive info about people's identity and actions. They use technology to establish and prove your identity, often by collecting and linking your sensitive personal information, and to track you. This data can include your biometrics, health records, travel, and purchases. There are very few data protections against sharing this information with corporations and police.

Despite the fact that digital I.Ds are a slowly growing phenomena on a worldwide scale, international bodies and countries have generally come to a consensus regarding the main principles that govern the use of digital I.Ds. This segment shall explore the different principles that have come to be recognized in the use of digital I.Ds.

2.1. Universality and Accessibility.
The Digital I.D system of any country ought to take into consideration all individuals without discrimination on the basis of race, age, sex
2.2. In regard to governance, there ought to be data privacy and security safeguards through comprehensive laws.
2.2.1. In the first instance, there ought to be a legal framework governing the use of digital I.Ds in any given jurisdiction. As a matter of rule of law, actions by a state are required to be backed by laws if they are to be considered legal/rightful. Legal parameters should be in place to guide state officials in the relevant agencies on what to do, how to do it and what ought to be avoided.
2.2.2. The processes of collection and storage of data about any individual by any state agency must be regulated in order to safeguard one's right to privacy and ensure that whatever limitation or breach is within whatever is acceptable and demonstrably justifiable in a free and democratic society.

2.2.3. There should be clear institutional mandates set out in the legal framework. As earlier stated, there should be a law stipulating what should be done by the relevant authority and what it should avoid.

Secondly, to avoid conflict of interest, there should be two agencies; one to deal with the storage of individuals' data, and the second one to act as a regulator which licenses other bodies that intend to authenticate the data and also offer redress in instances where violations occur.

2.2.4. Related to the above is the need for accountability mechanisms. There must be civil and criminal accountability mechanisms in place to offer redress in instances where violations or breaches occur. A duty of care is imposed upon any agency that deals in the collection, authentication and storage of data pertaining to individuals. Should such information be used for other purposes other than those for which it was collected, and without the informed consent of the concerned individual, aspects of violation of one's right to privacy and breach of data privacy arise. Secondly, in instances where the information processed about a particular individual is erroneous, there ought to be mechanisms for correction of the inaccurate data. Lastly, accountability requires that an access log in a portal is created so that individuals can track who has accessed their data and for what reason.

2.3. By virtue of their design, the digital I.Ds ought to be secure and have accuracy in the information collected regarding one's identity.
2.3.1. The digital I.Ds should be made in a way the system ensures protection of one's personal information and data privacy is concerned. The system should be one that is not easily prone to breaches/hacks that lead to mission creep; that is third parties accessing and using information for a different purpose other than that which it is meant for.
2.3.2. States are also mandated to plan for financial sustainability of digital I.D programs without limiting aspects of accessibility by users.
2.3.3. The design of the digital I.D system ought to ensure that an interoperable platform is created to allow for ease of access and efficiency across different state agencies.

3. Uganda's Identification System

The Uganda National ID, also known as 'Ndaga Muntu', is issued by the National Identification and Registration Authority (NIRA) and provides a unique identification number (NIN) to Ugandan citizens and permanent residents. The ID includes personal details and biometric data like fingerprints and facial recognition. Introduced in 2014, it is essential for accessing services such as banking, healthcare, voting, and applying for passports. The Uganda ID aims to enhance public service delivery, improve national security, and facilitate government planning, though challenges remain with registration efficiency and accessibility in remote areas.

The Uganda National ID system is a crucial feature of the country's identity management. The system, which introduced mass registration in 2015 under the Registration of Persons Act, is managed by the National Identification and Registration Authority (NIRA), which is responsible for overseeing the registration process, issuing National Identity Cards (NIDs), and maintaining a central National Identification Register.

Before the National ID system was introduced in 2014, multiple government agencies, including the Uganda Registration Services Bureau and the Directorate of Citizenship and Immigration Control, managed various aspects of personal data. Following the launch of the new system in 2014, the first mass registration drive took place, creating a unified process for citizen identification. The Registration of Persons Act in 2015 then officially transferred full control of the registration process and issuance of ID cards to NIRA.

A significant development in Uganda's National ID system is the planned introduction of iris biometrics. In August 2022, NIRA announced plans to upgrade the current national identity card to include additional biometric details such as blood type, palm print, and eye scan information. This system aims to change current National Identity Cards to high-tech ones with a chip that can identify people's eyes and recognizes their DNA. This proposed advancement has since re-awakened the legitimate concerns around adoption of digital IDs in Uganda.

4. Implications of the Uganda National ID system

The Uganda National ID system has offered several benefits that support the country's development and governance as follows:

4.1. A centralized and biometric-based identification system has provided the government with a reliable means to track, identify, and manage potential security threats. This enhanced security helps to reduce identity fraud, effectively combat crime, and curb terrorist activities, thereby strengthening national security.

4.2. By providing citizens with a streamlined identification process, the National ID has enabled fairly easier access to essential government services such as healthcare, education, and social welfare programs. This is aimed at improving service delivery and greater inclusion in society.

4.3. The Uganda National ID system paved the way for increased financial inclusion, enabling more Ugandans to access formal banking services. This has led to increased opportunities for savings, credit, and other financial products, fostering more opportunities particularly in regions that were previously underserved by traditional banking systems.

4.4. The Uganda National ID card not only serves as a tool for citizen identification but also as a valid travel document for Ugandans within the East African Community. This allows for easy and seamless movement within the region, promoting regional integration and trade.

4.5. A standardized ID has allowed for voter registration and participation to become more secure, helping reduce issues like voter impersonation during elections.

Although the National ID system has registered some progressive milestones to Ugandans, it has also faced criticism and challenges with negative aspects including:

4.6. A major criticism of the National ID system is the exclusion of vulnerable groups, particularly the elderly, rural populations, and individuals without formal documentation. Many Ugandans struggle to obtain National IDs due to a lack of birth certificates or other required documents, leading to delays in accessing essential services. The mandatory requirement of the ID for accessing public services, employment, financial transactions, and healthcare further intensifies the marginalization of these groups. Infact, more than 15 million Ugandans remain at risk of being excluded from accessing essential public services and entitlements as they lack national digital identity cards. Citizens who do not have the national ID cards are denied access to services such as Uganda's Senior Citizens' Grants, National Health System, School capitation grants, property acquisition, access to land title deeds and assets registration, National Social Security Fund's social security benefits delivery, driving permits, SIM card registration, bank account opening, passport acquisition and voter registration. As noted by Katelyn Cioffi in Human Rights Gateway or Gatekeeper: Digital IDs on Trial in Uganda (July 24, 2023), immediate remedies are urgently needed for individuals excluded from public services due to the ID system.

4.7. The National ID system has sparked concerns over the privacy and security of biometric data collected by NIRA. Citizens' privacy is at risk due to the lack of transparency in data sharing among various Ministries, Departments, and Agencies within the government heightening worries about data protection and potential misuse. Citizens worry that their personal information, such as fingerprints and facial recognition data, could be misused or fall into the wrong hands, potentially leading to identity theft or unauthorized surveillance. This has been a significant concern for many Ugandans and remains a challenge for the system. The authority's failure to conduct a Data Impact Assessment and establish a privacy policy poses significant risks to the privacy rights of Ugandan citizens. These deficiencies contravene Uganda's data protection laws, leaving personal information vulnerable to misuse and breaches. Addressing these issues is vital to safeguarding individual privacy and fostering public trust in the national ID system. The concerns surrounding data privacy in Uganda's National ID system are further amplified by the introduction of advanced biometric measures in the New Generation National ID Project. This increased technological sophistication can improve system accuracy and efficiency, but without robust human rights safeguards, it may lead to serious abuses. There is need for enhanced privacy protections and greater transparency from NIRA is paramount, as highlighted in "A Call for Inclusivity, Trust, and Accountability in Reforming Uganda's National ID System."

4.8. In addition to privacy concerns, allegations of political manipulation have been raised about Uganda's National ID system, particularly in the context of elections. During the 2016 and 2021 general elections, some opposition members alleged that delays in issuing IDs in certain regions were a deliberate strategy to exclude voters.

4.9. The National ID system in Uganda has been plagued by the notable high cost and access issues that affect impoverished populations. Individuals in remote districts often endure long treks to reach registration centers, only to encounter further obstacles such as system failures, staffing shortages, and technical problems that hinder the registration process and deprive citizens of essential benefits associated with National IDs. In rural areas, where internet connectivity and infrastructure are limited, these problems are further aggravated. Reports indicate frequent incidents where biometric machines fail to capture fingerprints properly, resulting in failed registrations.

4.10. The process for replacing lost or damaged National IDs has been a subject of criticism. Many individuals who have lost their IDs have reported long waiting periods for replacements, which often meant being unable to access essential services during this time. This situation has caused significant difficulties, especially for those who rely on their IDs for banking, accessing social welfare, or other government services. The slow and cumbersome process for replacing lost or damaged IDs has further frustrated citizens.

4.11. For some Ugandans, the lack of a National ID or difficulties with registration have resulted in challenges in enrolling in schools. There have been instances where students have been denied admission to universities or unable to apply for government scholarships due to the absence of a valid National ID. This has negatively affected young people's ability to pursue higher education and access professional opportunities. The exclusion of vulnerable groups from education is a serious concern, as it can create long-term consequences and aggravate existing inequalities in the country.

4.12. The Registration of Persons Act 2015, which mandates the National ID system in Uganda, raises significant challenges by virtue of its compulsory nature. Under this Act, citizens who fail to register with NIRA face severe penalties, including fines up to UGX 2,400,000 or imprisonment for up to five years. This imposes a punitive approach that extremely affects vulnerable populations. The resulting barriers to essential services, such as healthcare, social protection, banking, and SIM cards, infringe upon citizens' fundamental rights and restrict their participation in the economy.

While the Uganda National ID system represents a contemporary approach to identity management, its benefits are overshadowed by significant challenges, including exclusion of vulnerable groups, privacy concerns, and allegations of political manipulation. Addressing these challenges through urgent reforms, such as promoting inclusivity, safeguarding citizens' privacy, increasing transparency in the system, and recognition of alternative means of identification in access to public services is crucial to ensuring equitable access and maximizing the benefits of the National ID system for all Ugandans.

5. Digital IDs and the Privacy Question

Digital ID systems usually assign each individual a unique identifier that connects their biometric and personal details to that number. This identifier is tied to an "access key" or "credential," which is used to verify identity. This credential, which can be digital or physical, acts as a portable identity tracker. Digital credentials may be stored on a smartphone or linked to facial recognition, iris scans, or fingerprints, while physical credentials might include a card with a "smart chip" that monitors its usage or location.

Although digital IDs are marketed as safer than traditional paper-based systems, offering greater efficiency and convenience while facilitating access to banking and social services, it is crucial for governments to conduct a transparent cost-benefit analysis of these systems.

For starters, the risks tied to digital ID systems—such as identity theft, massive data breaches, and serious privacy issues—cannot be ignored. Many of these ID systems are launched without sufficient security or data protection regulations. In some cases, to ostensibly "reduce fraud," governments and companies are instead creating intrusive surveillance infrastructures with minimal regulation, which increases vulnerability to breaches and fraud. Digital ID programs gather vast amounts of personal and biometric data, sharing it with corporations and government bodies alike, which jeopardizes individual privacy and safety. This data sharing feeds both corporate tracking and law enforcement databases. For example, Mastercard, a major digital ID provider, has structured part of its business on data collection and expanded credit card use, claiming a commitment to privacy while often collecting and selling user data without consent. In 2018, the Electronic Privacy Information Center filed a complaint with the US Federal Trade Commission over Mastercard's undisclosed data-sharing partnership with Google, which affected its two billion cardholders.

Secondly, digital IDs and the automation of social services risk increasing exclusion from both social and financial support. Automating eligibility decisions can embed bias, leading to loss of access to crucial resources. When digital IDs become mandatory for accessing rights or services, exclusion deepens. While governments and companies often promote digital IDs linked to financial services to improve banking access, simply having a bank account does not guarantee financial stability. These "inclusion" programs are often run by fintech companies that lack the security and services banks provide. Instead, they push high-cost, low-value products to low-income individuals, entrenching economic inequality. Prepaid debit cards, for example, are marketed to the unbanked, yet carry high transaction fees, maintaining a tiered banking system that reinforces economic disparity.

Thirdly, the "convenience" promised by digital IDs comes at a high price. Even if these systems have good intentions, collecting vast personal and biometric data can lead to misuse, especially since it's difficult to ensure system security.

6. Best Practices in other Jurisdictions regarding the use of Digital I.Ds

In a bid to offer guidance on acceptable parameters pertaining to the use of digital I.Ds, different states have through their courts and other mechanisms ruled on what would be regarded as the legal or acceptable ways to act. These decisions and parameters have shaped what could be regarded as best practices regarding the use of digital I.Ds which shall be discussed below;

6.1. Generally, regarding the limitation of the right to privacy which takes centre stage in regard to digital I.Ds, the proportionality test is very key. In the South African case of S v. Makwanyane (1995) 3 SA 391 (CC), the Constitutional Court guided that violation of one's fundamental right such as the right to life, personal liberty (or in this case the right to privacy) should only be done in accordance with what is acceptable by law.

6.2. In India, the Supreme Court of India in the case of Justice K.S Puttaswamy & Ors v. Union of India; Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161; the question of private sector users was addressed. This matter came up after Facebook acquired Whatsapp in 2014 and a new data sharing policy was issued by Whatsapp which entailed the aspect of making individuals data available to other interested third parties. The court not only upheld the right to privacy as a fundamental human right in India, but also prohibited the use of digital I.Ds by private sector actors in ways that were allowing for 'commercial exploitation' of biometrics and personal data.

6.3. In the United Kingdom, sections 45 and 46 of the U.K Data Protection Act (1998) provide for the rights to access and rectify any errors in data that may have been captured in one's data. This is unlike Uganda's Registration of Persons Act which is silent on the same and imposes the responsibility of any error on the individual. For example, if an official of a state agency entered wrong data about an individual in regard to their I.D, currently, it is the individual who incurs the cost of making the corrections. Although NIRA has promised that corrections will be made at no cost in the forthcoming digital I.D program for the renewal of national I.Ds, there is no clear procedure on how this will be done.

6.4. The European Court in the case of Leander v. Sweden; ECHR 4 (1987) at para 48 held that the storage of data for unspecified reasons or without the informed consent of the concerned individual was tantamount to a violation of the right to privacy.

This case dealt with whether the state can use secret files to vet an individual for employment purposes and safeguard national security, whether an individual has a right to access such files and whether procedural safeguards were needed to protect an individual from abuse by the state in such instances. In this case, Leander, a Swedish citizen was a carpenter working at the Naval Museum. He applied to be employed as a permanent employee at the museum. A background check was conducted into his police files and the Commander in chief recommended that he was not suitable for permanent employment. Mr. Leander filed this case arguing that he ought to have access to such files and that there was a violation of his right to privacy since no informed consent was sought from him to maintain such secret files that were redundant and only used to his detriment when he sought employment. The grand chamber of the European Court agreed with Mr. Leander.

6.5. In the case of the case of Ammann v. Switzerland ECHR 88 (2000), the European Commission on Human Rights required Switzerland to enact laws that 'contain detailed and specific provisions on the gathering, recording and storage of information.' In this case, Mr. Ammann, a Swedish businessman dealing in depilatory electronics received a phone call from the Russian Embassy ordering for an electronic. The call was intercepted by the Swedish authorities and a card was developed earmarking Mr. Ammann as an individual taking part in espionage. The Commission found that this was in breach of Mr. Ammann's private life and that there was need for clear and specific laws to guide on how information pertaining to individuals could be collected by state agencies.

6.6. In Jamaica, the right of individuals to consent or reject the collection of biometric data was upheld by the Supreme Court in the case of Robinson, Julian v. The Attorney General of Jamaica (2019) JMFC. In this case, Julian Jay Robinson, a parliamentarian challenged the constitutionality of Jamaica's National Identification and Registration Act (NIRA). The Jamaican Supreme Court held that the forced gathering of biometric data violated people's right to liberty and amounted to bodily intrusion because it deprived them of their choice. Since there was no "strong justification" for the lack of an opt-out clause, Section 20's mandatory collection clause was ruled unconstitutional since it was not regarded as reasonable in a free and democratic society.

7. International Trends and shifting perspectives on Digital IDs

7.1.Digital IDs and Smart Cities

International trends in digital IDs are being integrated into smart city initiatives, with digital identity being used as the primary means for laying the ground work for smart cities and collectively, one global village. A smart city is a place where everything you do is tracked and managed by government including what you do at home. This is possible because most modern home appliances have internet connectivity and not just thermostats. In smart cities, the sharing of data is not limited to homes, but also businesses, citizens and other third parties.

According to Sustainable Development Goal (SDG) 11, the UN requires all its 193-member states to introduce smart cities by 2030.To support this initiative is SDG16.9 that identifies global legal identity as a development priority and requires the same for all by 2030.

By implementing digital ID systems, cities are being set up to facilitate seamless interactions with various services, such as public transportation, healthcare, and housing, using a single, verifiable identity. As smart cities emerge, diverse technologies, with interoperable systems are being developed for access of multiple services through a single ID. With this integration data collection and management would allow city planners to analyze residents' behaviors and preferences for a more predictive and centred management system of the people. The data collectors are able to detect, predict, and of course, even control the behaviors of the general population.

The World Economic Forum plays a central role in advancing smart city initiatives through the G20 Global Smart Cities Alliance. According to a WEF report on reimagining the digital ID, it has been indicated that there is need for a global digital ID given that it can be difficult or impossible for people without an official ID to participate in society.

Accordingly, the G20 Global Smart Cities Alliance has developed model policies and networks over the past decade aimed at fostering the implementation of smart city policies .In November 2020, the World Economic Forum announced that it had selected 36 cities across 22 countries and six continents to pioneer a new global policy roadmap for smart cities developed by the G20 Global Smart Cities Alliance. This pilot study was rolled out as a means of examining how best the WEF can govern smart cities. Subsequently, the WEF announced plans to start developing smart cities in Japan, India and Latin America. Questions have been raised about the organization's authority to lead such global projects.

The findings from this pilot initiative have sparked debate due to limited assurances around government accountability, cybersecurity measures, data transparency, privacy standards or opt-out provisions for citizens. As a matter of fact, United Nations Education, Scientific and Cultural Organisation (UNESCO) has classified Society 5.0 (Japan's smart city innovation) as a far more reaching concept than the 4th Industrial revolution. In this report , UNESCO details the vision of this innovation as being one that aims to completely revolutionalise the Japanese way of life by blurring the frontier between cyber space and physical space.

It is worth noting that some of the strongest opposition to WEF's digital ID and smart city initiatives has come from organizations that typically align with WEF's goals. Concerns about data privacy, transparency, and control have raised questions over whether digital ID systems are a step toward widespread surveillance and control within smart cities. This criticism suggests that digital IDs might serve as a pathway to broader monitoring and governance mechanisms under smart city management.

7.2. Digital IDs and Centralized Bank Digital Currency

A foundational element for national digital currencies is digital identity. As countries explore digital versions of their traditional currencies, there's a growing convergence between Central Bank Digital Currencies (CBDCs) and digital identification systems. This blending raises significant concerns about individual privacy and personal freedoms.

CBDCs, which are digital counterparts of a nation's currency regulated by the central bank, have become a focal point in modern financial discussions. To maximize their functionality, reliable user authentication is essential for maintaining financial integrity and preventing illicit activities. Digital ID systems are seen as vital to this, providing each person with a unique digital identity and thus supporting the CBDC framework.

However, combining CBDCs with digital IDs introduces serious privacy risks. A centralized ledger that tracks every transaction could open the door to heightened state surveillance, where each individual's financial actions are easily traceable, endangering financial privacy. Additionally, centralized systems can be vulnerable to cyber threats, which, if compromised, could expose both financial and personal data, leading to identity theft and fraud. While CBDCs aim to promote financial inclusion, there's a paradox: individuals lacking digital IDs may be excluded from this emerging financial system. The integrated power of CBDCs and digital IDs could allow governments extensive control over citizens' finances, raising concerns about the potential use of financial data for monitoring dissent, influencing political opposition, or even subtly impacting electoral processes.

Accordingly, the G20 Global Smart Cities Alliance has developed model policies and networks over the past decade aimed at fostering the implementation of smart city policies .In November 2020, the World Economic Forum announced that it had selected 36 cities across 22 countries and six continents to pioneer a new global policy roadmap for smart cities developed by the G20 Global Smart Cities Alliance. This pilot study was rolled out as a means of examining how best the WEF can govern smart cities. Subsequently, the WEF announced plans to start developing smart cities in Japan, India and Latin America. Questions have been raised about the organization's authority to lead such global projects.

The findings from this pilot initiative have sparked debate due to limited assurances around government accountability, cybersecurity measures, data transparency, privacy standards or opt-out provisions for citizens. As a matter of fact, United Nations Education, Scientific and Cultural Organisation (UNESCO) has classified Society 5.0 (Japan's smart city innovation) as a far more reaching concept than the 4th Industrial revolution. In this report , UNESCO details the vision of this innovation as being one that aims to completely revolutionalise the Japanese way of life by blurring the frontier between cyber space and physical space.

It is worth noting that some of the strongest opposition to WEF's digital ID and smart city initiatives has come from organizations that typically align with WEF's goals. Concerns about data privacy, transparency, and control have raised questions over whether digital ID systems are a step toward widespread surveillance and control within smart cities. This criticism suggests that digital IDs might serve as a pathway to broader monitoring and governance mechanisms under smart city management.

8. Strategies for closing Identified Gaps in ID systems

8.1.Set Clear Guidelines for Data Collection and Use
Governments should define strict limits on data acquisition, retention, and usage, making sure to collect only essential biographic information. Establishing these boundaries can prevent data overreach, protect individual privacy, and build public trust by clarifying exactly how and why data is gathered and stored.

8.2. Explore Decentralized Identity Solutions
Shifting towards decentralized identity models can empower individuals to control their personal data directly, reducing dependence on centralized databases. This approach not only enhances privacy by limiting data concentration but also fosters a more user-centric system where individuals decide if or how their data is accessed and shared.

8.3. Implement Advanced Security Protocols and Conduct Regular Audits
Security should be a top priority, with governments employing the latest cybersecurity measures and conducting frequent audits to maintain data integrity and privacy. Investing in cutting-edge technologies like encryption, biometric protections, and multi-factor authentication will help safeguard sensitive data within digital ID frameworks.

8.4. Foster Public Involvement and Transparent Dialogue
Engaging the public in discussions about digital identity systems is crucial to developing solutions that align with democratic principles. Inclusive dialogues can address citizen concerns, increase transparency, and ensure the digital identity framework resonates with community values and the broader social fabric.

Conclusion
The discourse on digital IDs transcends finance and service delivery. It beckons us to envisage the kind of society we aspire to in this digital epoch. As we tread this uncharted territory, our guiding light should be a commitment to melding digital innovation with the timeless principles of Godliness, privacy, and personal freedom.

References

Arlette David, "Identification in Ancient Egypt from the Old Kingdom to the End of the New Kingdom (2650-1100 BCE'', 2014

Mark Depauw, "Elements of Identification in Egypt, 800 BC–AD 300'', pp. 75-102, 2014

Katelijn Vandorpe, "Seals and Stamps as Identifiers in Daily Life in Greco-Roman Egypt",2004

Michele Faraguna, "Citizens, Non-Citizens, and Slaves: Identification Methods in Classical Greece'', 2014, pp. 165-183

Eva Jakab, "Methoden der Identifikation in lateinischen Tabulae'', 2014, pp. 209-231

Mark Edward Lewis, "The Early Chinese Empires: Qin and Han'', 2007

David Crouch, "The Birth of Nobility: Constructing Aristocracy in England and France'', pp. 900–1300

Soomro, Anam, ''People, Paper and Power: The Birth of the Passport in International Law. Routledge'', 2018

https://science.howstuffworks.com/fingerprinting.htm accessed on 24th October 2024

Nyst, Carly, Steve Pannifer, Edgar Whitley, and Paul Makin, "Digital Identity: Issue Analysis", 2016

https://www3.weforum.org/docs/WEF_Reimagining_Digital_ID_2023.pdf accessed on 25th October 2024

https://www.weforum.org/press/2020/11/in-the-face-of-extraordinary-challenges-36-pioneer-cities-chart-a-course-towards-a-more-ethical-and-responsible-future/ accessed on 25th October 2024

https://www.unesco.org/en/articles/japan-pushing-ahead-society-50-overcome-chronic-social-challenges accessed on 25th October 2024