Strathmore University
Centre for Intellectual Property and Information Technology Law

Internews
Local voices. Global change.

SERIES ON DIGITAL IDENTITY AND BIOMETRICS

Topic 3: Data Protection in Digital Identity (ID)

Greater Internet Freedom

Centre for Intellectual Property and Information Technology Law (CIPIT)
Strathmore University

August 2023

Data Protection in Digital Identity (ID)

Author: The Centre for Intellectual Property and Information Technology Law (CIPIT).

Acknowledgements: We would like to express our gratitude to the Centre for Intellectual Property and Information Technology Law (CIPIT) acknowledging, Florence Ogonjo, Joshua Kitili, Lilian Olivia Orero, Doreen Aoko Abiero, Josephine Kaaniru, and Dan Allan Kipkoech who prepared this learning material. The CIPIT team authored this material in close consultation with the Greater Internet Freedom team at Internews, including Sigi Waigumo Mwanzia, Digital Rights Advisor, and Olga Kyryliuk, Technical Advisor on Internet Governance and Digital Rights.

Copy-Edited by: Internews.

Design & Layout by: CIPIT.

Strathmore University
Centre for Intellectual Property and Information Technology Law

Internews
Local voices. Global change.

About CIPIT	About GIF
The Centre for Intellectual Property and Information Technology Law (CIPIT) is an evidence-based research and training Centre based at Strathmore University, Nairobi, Kenya. CIPIT was established in 2012 and focuses on studying, creating, and sharing knowledge on the development of intellectual property and information technology utilizing diverse methodological approaches to inform debates on ICT applications and regulation.	**The Greater Internet Freedom Project (GIF) is a three-year, consortium-based, global program implemented by Internews and the GIF consortium across 39 countries. GIF places regional and local organizations at the forefront of the fight to preserve an open, reliable, secure, and interoperable Internet – and, by extension, protects the citizens, civic actors, journalists, and human rights defenders who rely on it to realize fundamental freedoms.**

Table of Contents

Introduction

The CIPIT and the GIF have developed exploratory material relevant to pertinent digital identity and biometrics topics. The 'Data Protection and Digital Identity' topic briefly explores how data protection intersects with digital identity.

A digital ID is a virtual form of identity containing data that uniquely describes a person or thing but also contains information about a subject's relationships to other entities.[1] There has been a surge in the global adoption of digital ID across GIF countries. There are several countries that have issued digital IDs including Estonia, India, Vietnam, Brazil, Greece, Antigua and Barbuda, Bahamas, Barbados, Belize, Grenada and St. Kitts and Nevis and the UK.[2] Estonia is seen to be a frontrunner in the digital ID space and it has progressed by allowing citizens to store and manage their official documents through a digital wallet.[3] India runs its digital identification through the Aadhaar digital ID program, which began in 2009.[4]

The Place of Data Protection in Digital ID

Digital ID systems use biometrics or biometric identifiers to integrate the relevant information that is unique to each data subject. Biometrics is a term used to describe unique and measurable human biological and behavioral characteristics that can be used for identification, such as retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry, or the automated methods of recognizing an individual based on those characteristics.[5]

Data protection is interconnected with digital ID systems particularly in terms of privacy of the data subjects and the protection of personal data. The World Bank notes that the protection of people's data by design and by default is required to build inclusive and trusted digital ID systems.[6]

The 'murky conceptual waters' between what is public and what is private have caused significant modifications in the idea of privacy in the digital age.[7] This is particularly true in the context of profiling, when advanced technologies are systematically undermining people's autonomy and privacy. Although he does so from a technological standpoint, Hilderbrandt defines profiling as the process of 'discovering' patterns in data in databases that can be used to identify or represent a human or nonhuman subject (individual or group), and/or the application of profiles (sets of correlated data) to individuate and represent an individual subject or to identify as a member of a group (which can be an existing community or a 'discovered category').[8]

The General Data Protection Regulation (GDPR) provides a clearer definition of profiling and refers it to any automated processing of personal information involving the evaluation of specific personal characteristics relating to a natural person, including the analysis or prediction of characteristics such as that person's performance at work, financial status, health, individual tastes, pursuits, dependability, behavior, location, or movements.[9] In order to profile the conduct of the users of an internet-based resource, profiling has emerged as a new field that combines data mining and statistics.[10]

The Internet of Things (IoT) has made the problem of profiling worse because it allows for the combination and analysis of seemingly irrelevant data produced by IoT devices to produce useful user profiles.[11] This kind of indiscriminate profiling erodes privacy and liberty, and is an attack on an individual's core identity.

Principles of Data Protection that are Applicable to Digital ID Systems

Data protection is crucial when it comes to handling digital IDs as they contain sensitive personal information. The key principles of data protection stemming from the GDPR that should be applicable to Digital ID systems include:

1. **Lawfulness, Fairness, and Transparency:** Digital ID systems should be implemented in accordance with applicable data protection laws and regulations. Users must be informed about the purpose of collecting their data, how it will be used, and any third parties involved in processing the information.
2. **Purpose Limitation:** Personal data collected for Digital ID purposes should only be used for specific and legitimate purposes. Data should not be processed in a way that is incompatible with these stated purposes.
3. **Data Minimization:** Only the minimum amount of personal data necessary for the Digital ID system's intended purpose should be collected and processed. Unnecessary data should be avoided to minimize risks.
4. **Accuracy:** Personal data used in Digital IDs should be accurate and kept up to date. Adequate measures should be in place to ensure the data remains accurate, and users should have the ability to correct any inaccuracies.
5. **Storage Limitation:** Personal data should not be retained for longer than necessary for the purpose for which it was collected. Once the data is no longer needed, it should be securely deleted or anonymized.
6. **Integrity and Confidentiality:** Strong security measures must be in place to protect the confidentiality and integrity of the data. This includes encryption, access controls, and protection against unauthorized access, loss, or destruction.

7. **Accountability:** The entity responsible for the Digital ID system should be accountable for complying with data protection regulations. This includes maintaining records of data processing activities and conducting privacy impact assessments.
8. **User's Rights:** Users should have clear and easily accessible information about their rights concerning their personal data. These rights may include the right to access, rectify, erase, and restrict the processing of their data.
9. **Consent:** When processing personal data for Digital ID purposes, user consent should be obtained when required by law. Consent should be freely given, specific, informed, and unambiguous.
10. **Data Breach Notification:** In the event of a data breach that may affect the security of the Digital ID system, affected users and relevant authorities should be notified promptly.
11. **Cross-Border Data Transfers:** If personal data is transferred across borders, appropriate safeguards must be in place to protect the data, in accordance with relevant data protection regulations.

Implementing these principles helps to build trust among users and ensures that their personal data is handled responsibly and securely within the context of a Digital ID system. Additionally, compliance with data protection laws reduces the risk of potential legal and reputational consequences for the organizations involved.

Important Note on Biometric Data

There are some features that are innate to biometric data and hence necessitate its protection:

1. It is unique to the individual. Biometric data, such as fingerprints, facial scans, and voiceprints, is unique to each individual. This means that it

cannot be easily changed or replaced, making it a valuable target for identity thieves.

2. It cannot be changed. Unlike passwords, which can be changed if they are compromised, biometric data cannot be changed. This means that if your biometric data is stolen, you will be at risk of identity theft for the rest of your life.
3. Potential uses and abuses of biometric data are not fully known. As biometric technology becomes more sophisticated, it is possible that it will be used for malicious purposes, such as tracking individuals or denying them access to services. It is important to protect biometric data now, before it can be used for these purposes.

Source: Illinois Biometric Information Privacy Act (BIPA) of 2008, 740 ILCS 14.

Indeed, biometric data is highly sensitive and unique, making it crucial to safeguard it from unauthorized access and misuse. The right to be incognito, or anonymous, is a fundamental aspect of privacy, as emphasized by Warren and Brandeis in their 1890 law review article “The Right to Privacy.”[12]

In the digital age, with the prevalence of social media and advanced data aggregation technologies, the concerns raised by Warren and Brandeis have become even more relevant to the general public. The aggregation of seemingly innocuous pieces of public information can create a detailed and invasive profile, compromising individuals' privacy and potentially affecting their pursuit of happiness.

The use of biometric data by both government and private sectors, such as fusion centers, can further exacerbate these privacy issues. The advanced data-mining tools and facial-recognition software utilized by fusion centers enable the compilation of vast dossiers on individuals, raising concerns about anonymity and control over personal information.

In conclusion, protecting biometric data and the right to privacy is of utmost importance in today's society, considering the vast amount of personal information that can be easily collected, aggregated, and shared. Legislation and measures to safeguard this information are essential to preserve individual privacy, prevent unauthorized use, and ensure that people can exercise their right to be incognito in an increasingly interconnected world.

Challenges and Security Risks

Although digital IDs have contributed to significant progress in the age of digital revolution, there are a myriad of challenges and risks that have cropped up. Notably, issues around data protection have been raised in many countries. In

Kenya for instance, privacy and exclusion issues were raised by civil society organizations resulting in the abandonment of the National Integrated Identity Management System otherwise known as Huduma Namba- a form of digital identification system[13]. This highlighted the need for proper systems and data protection measures to ensure that the information of data subjects was properly stored and safeguarded.

Other issues raised with regards to digital identification systems on a global scale are access and governmental inefficiency. On matters of access, which can be linked to exclusion, mandatory digital ID cards mean that those without identification due to marginalization risk losing access to any social resources linked to the ID. Government inefficiency presents some of the biggest challenges when it comes to the implementation and citizen response to digital ID systems because of issues related to bureaucracy, corruption, lack of transparency, lack of public participation, and embezzlement of state funds that make the citizenry distrust the motives of the government even when rolling out digital IDs.[14]

Resources and Reading List

Basic Resources

A Blueprint for Digital Identity https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

Biometrics: A guide https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf.

Digital Identity Roadmap Guide https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/Digital_Identity_Roadmap_Guide-2018-E.pdf .

Digital Identity: The Essential Guide https://www.id4africa.com/main/files/Digital_Identity_The_Essential_Guide.pdf.

ePrivacy Regulation on Privacy and Electronic Communications (PECR).

Global Biometrics Guide https://us.eversheds-sutherland.com/portalresource/Global_Biometrics_Guide_2022.pdf.

Guidance on Digital Identity https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf.coredownload.pdf.

Guidelines on National Digital Identity https://rm.coe.int/prems-010823-gbr-2051-national-digital-identity-final-web-2762-4423-83/1680aa6b24.

National Digital Identity Programmes: What's Next? https://www.accessnow.org/wp-content/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf.

Policy Model for Digital Identity and Electronic Know Your Customer (E-KYC) https://www.afi-global.org/wp-content/uploads/2021/09/AFI_GSP_digital-ID_eKYC_PM.pdf.

The Emerging Era of Digital Identities: Challenges and Opportunities for the G20 (policy brief) https://www.adb.org/sites/default/files/publication/822681/adbi-brief-emerging-era-digital-identities-challenges-and-opportunities-g20.pdf.

Legislations

European Union

General Data Protection Regulation (GDPR)

Irish Data Protection Act 2018 (which replaced the Data Protection Act 1988)

Belgium's Protection of Natural Persons with regard to the Processing of Personal Data Act, 2018 ('the GDPR Implementing Law') (unofficial translation)

In Germany, the GDPR mainly governs data protection. The law is supplemented by the Federal Data Protection Act of 30 June 2017 (implementing the GDPR) ('BDSG')

In France, the French Act No. 2018-493 of 20 June 2018 ('the Amendment Law') (available in French only) incorporates the GDPR provisions in the existing Act on Information Technology, Data Files and Civil Liberties ('the 1978 Act') (only available in French), which governs the protection of personal data.

Italy implemented the GDPR by amending the Personal Data Protection Code, Containing Provisions to Adapt the National Legislation to General Data Protection Regulation (Regulation (EU) 2016/679) ('the Code'). The Code repealed sections that conflict with the GDPR.

Spain implemented the GDPR with its Protection of Personal Data and Guarantee of Digital Rights ('the LOPDGDD')

Malta Data Protection Act 2001

The United Kingdom

The UK GDPR (New)

The General Data Protection Regulation (EU) 2016/679) ('GDPR') applied in the UK until 1 January 2021, when the UK adopted the EU GDPR as domestic law with some changes to work effectively in the UK context, now referred to as the 'UK GDPR'.

Americas

United States

Sector-specific data protection laws

California Privacy Act, 2020 (CPRA) (New)

California Consumer Privacy Act (CCPA) (Law soon to be replaced by CCRA)

Illinois Biometric Information Privacy Act (BIPA) of 2008, 740 ILCS 14

Senate Bill for the New York Privacy Act (New) (reintroduced in the State Senate in January 2022)

Assembly Bill for the New York Privacy Act (New) (reintroduced in the State Assembly in January 2022)

Colorado Privacy Act ('CPA') (New) (The CPA will come into effect on 1 July 2023)

Virginia Consumer Data Protection Act (CDPA) (New) (The CDPA will come into force on 1 January 2023)

Draft Consumer Privacy Bill of Rights Act (CPBORA) (still not in force and probably won't be signed into law)

The EU-US Privacy Shield

Canada

Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA)

British Columbia: Personal Information Protection Act, SBC 2003 c 63 ('BC PIPA')

Alberta: Personal Information Protection Act, SA 2003 c P-6.5 ('AB PIPA')

Quebec: Act respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1 ('Quebec Private Sector Act')

Latin America and the Caribbean

Argentinian Personal Data Protection Act

Brazilian General Data Protection Law (in Portuguese)

Bermuda Personal Information Protection Act (PIPA)

Chile's Law No. 19.628 on the Protection of Private Life 1999 (in Spanish)

Uruguay's Law No. 18.331 on the Protection of Personal Data and the Habeas Data Action 2008 (in Spanish)

Paraguay's Law No. 1682 which Regulates Private Information 2001 (in Spanish)

Peru's Law No. 29.733 on the Protection of Personal Data 2011 (in Spanish)

Ecuador's Organic Law on the Protection of Personal Data (in Spanish)

Africa

Kenya Data Protection Act No. 24 of 2019

South Africa Protection of Personal Information Act (POPI Act) Key Insights

Mauritian Data Protection Act 2017, which replaces the Data Protection Act 2004

Various Data Protection Laws of Africa

Australia and New Zealand

Australian Privacy Act

New Zealand Privacy Act

Asia

China's Personal Information Protection Law ('PIPL')

Indian Personal Data Protection Bill 2018

The APEC Privacy Framework and the OECD Privacy Framework

Japan Act on the Protection of Personal Information (APPI)

Japan passed the Amended Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2020). The 2020 Amendments will come into force on 1 April 2022.

The Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013 as amended) ('the My Number Act')

Hong Kong Personal Data (Privacy) Ordinance.

Singapore Personal Data Protection Act 2012 (PDPA)

Middle East

Bahrain's Personal Data Protection Law

Israeli Protection of Privacy Law 2014

UAE's Federal Law on Protection of Personal Data

Websites and Blogs

Biometric Update.com 'A handful of nations distributing new digital ID documents,' https://www.biometricupdate.com/202207/a-handful-of-nations-distributing-new-digital-id-documents

Center for Human Rights and Global Justice, 'Putting Profit Before Welfare: A Closer Look at India's Digital Identification System,' https://chrgj.org/2022/11/29/putting-profit-before-welfare-a-closer-look-at-indias-digital-identification-system/

e-Estonia, 'e-Identity,' https://e-estonia.com/solutions/e-identity/id-card/

Gov.UK, 'Enabling the use of digital identities in the UK,' https://www.gov.uk/guidance/digital-identity

Jennifer Gustavson, 'Digital Identity (Digital ID): The Complete Guide' (3 March 2022) https://www.notarize.com/blog/digital-identity-digital-id-the-complete-guide

Massimo Attoresi, 'Digital Identity and data protection: current developments and future trends,' https://edps.europa.eu/press-publications/press-news/blog/digital-identity-and-data-protection-current-developments-and_en

Research ICT Africa, 'Digital Identity in Kenya' https://researchictafrica.net/wp/wp-content/uploads/2021/11/Kenya_1.11.21.pdf

Security Magazine, 'Encryption bridges gap between data protection & digital identity' https://www.securitymagazine.com/articles/99222-encryption-bridges-gap-between-data-protection-and-digital-identity

Reports

Privacy & Data Protection in ID Systems Concept Note- https://www.id4africa.com/2023/workshops/W4.pdf

Report on Identifying Key Enablers on Digital Identity <https://web.kominfo.go.id/sites/default/files/Report%20on%20Identifying%20Key%20Enablers%20on%20Digital%20Identity.pdf

Books

A People's Guide to Tech and The Engine Room, *A Digital ID Handbook: Strategies for Navigating Electronic Identification Systems* (2022)

Maryline Laurent and Samia Bouzefrane (eds), *Digital Identity Management* (Elsevier 2015)

Windley, Phillip J.. *Learning Digital Identity*. United States: (O'Reilly Media, 2023)

Journals

Clark, Julia; Daly, Conrad. 2019. Digital ID and the Data Protection Challenge: Practitioner's Note. © World Bank, Washington, DC.

References

[1] Phillip J. Windley (2023). Learning Digital Identity.

[2] Biometric Update (2022). A handful of nations distributing new digital ID documents.

[3] e-Estonia, *e-Identity*.

[4] Center for Human Rights and Global Justice (2022). Putting Profit Before Welfare: A Closer Look at India's Digital Identification System.

[5] Michael P. Daly et al., (2018). Biometrics Litigation: An Evolving Landscape.

[6] World Bank (2021). Good digital ID needs great data protection.

[7] Gary T Marx (2001). Murky Conceptual Waters: The Public and the Private.

[8] Mireille Hildebrandt and Serge Gutwirth (eds) (2008). Profiling the European Citizen: Cross-disciplinary perspectives.

[9] GDPR, Art 4(1).

[10] Jean-Marc Dinant (2009). The Concepts of Identity and Identifiablity: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society?

[11] Sarah Eskens (2016). Profiling the European Consumer in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?

[12] Samuel D. Warren & Louis D. Brandeis (1890). The Right to Privacy.

[13] Research ICT Africa (2021). Digital Identity in Kenya.

[14] A People's Guide to Tech & The Engine Room (2022). A Digital ID Handbook: Strategies for Navigating Electronic Identification Systems.