COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

26 October 2020

T-PD(2020)04Rev

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

Digital Identities

by

Pat Walshe

Directorate General of Human Rights and Rule of Law

Table of Contents

A digital identity and the ability to prove who we are brings significant benefits and protections in multiple contexts. However, digital identity may also have negative consequences from discrimination and marginalisation to unwarranted surveillance, to a person's loss of control over their identity or the presentation of their identity by others. There is an unprecedented drive to create an 'identity for all' in the form of 'digital IDs' that raises serious questions of identity by whom for whom, and on whose terms? It raises questions of human agency of those whom digital ID systems are meant to serve, in their shaping of how they are presented to the world and what this means for their lived experiences[1] and their human rights.

1. Introduction

There is no universal single definition of 'digital identity' and it has multiple meanings across the private and public sectors. It may generally be considered as a set of electronically processed attributes that uniquely distinguish and represent an entity – whether a person or digital device for example - in given contexts. Borne out of the concept of identity and access management – controlling access to computers and electronic assets - a digital identity does not mean, and nor does it need to be a real-world identity.

However, policy agendas and initiatives among governments, international organisations and the private sector have fostered the conceptualisation and development of 'digital identity' as a digitised representation of a person's legal identity – as a national 'digital ID'. This reconceptualisation is given momentum by the emergence of commercial advocacy and the commodification of 'digital identity' as a 'fundamental human right'.[2]

'Digital identity' as reconceptualised is advocated as a digitised and legally recognised identity (a 'digital ID') and has in many cases become a prerequisite to access basic services and rights in many countries. Such 'digital IDs' are increasingly underpinned by biometric technologies that "*read characteristics of people's bodies and physical behaviours with the aim of fixing identities, or authenticating or sorting them, based on pre-determined categories and logics*." [3] Biometric identity technologies make individuals machine readable, assigning them an identity status that determines their inclusion or exclusion from the services and benefits digital identity schemes are meant to provide. Research conducted for this report, reveals that while 'digital identity' technology and even legislation may not necessarily have intent they may nonetheless facilitate the profiling, surveillance and exclusion of individuals and the groups they are meant to serve.[4]

This report discusses 'digital identity' developments and the benefits and risks of a reconceptualised national 'digital ID', and of the importance of ensuring appropriate legal frameworks and safeguards for human rights. The report draws on case studies and legal challenges that highlight the importance of ensuring 'digital identity' schemes (that by intent or otherwise, become *de facto* national identity schemes) reflect a legitimate aim and are inclusive, and that by default prioritise human rights in their design, implementation and operation. This is especially relevant considering arguments that a "*globally unique identifier could seem the answer for according a person official digital existence in the Information Society.*"[5] Research also stresses the importance of ensuring that approaches to 'Digital ID'

[1] Footnote 6

[2] Mastercard joins ID2020 Alliance https://mastercardcontentexchange.com/newsroom/press-releases/2020/may/mastercard-joins-id2020-alliance/

[3] Martin and Whitley (2013), *Fixing identity? Biometrics and the tensions of material practices* http://personal.lse.ac.uk/whitley/allpubs/MCS2013.pdf

[4] The court struck down the the National Identification and Registration Act that mandated the collection of biometric information on the entire Jamaican population and its storage in a centralised database. *Robinson – v- The Attorney General of Jamaica* https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

[5] UNESCO, (2007), Information for all Programme, *Ethical implications of emerging technologies: a survey* *http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/ethical-implications-of-emerging-technologies-a-survey/*

reflect the lived experiences of, and effects on, those that digital ID systems are meant to benefit, but who may "*face the biggest risks in relation to digital ID infrastructure, policies and protocols*."[6]

A key question remains identity for whom? Evidence shows that digital identity schemes – public and private - may mutually reinforce one another, linking identifiers or creating unique national global identifiers that leave little room for humans to flourish free of surveillance and the fear of surveillance for example. It raises the consideration of '*privacy as flourishing*'[7] and the right of individuals to be free to pursue personal development and fulfilment of their personality pursuant to Article 8 of the European Convention of Human Rights and case law.[8] Digital ID systems and the datafication of human bodies and behaviour may leave little space for human flourishing.

2. What is 'Digital identity'?

Around the world, individuals fortunate enough to have access to a smartphone, tablet or computer and to broadband internet connections, engage daily in multiple online contexts. These online contexts involve individuals in presenting a 'digital identity' to uniquely represent themselves; from communicating on social media platforms, to shopping online, to watching online streaming 'TV' or listening to online streaming music. In online contexts, a person's digital identity may simply be their 'online persona' [9] that may be created by individuals or given to them as they establish relationships with online services. A persona may take the form of a personal email address or social media profile name for example or an identifier on a prepaid debit card or of a device. An individual may have multiple personas and determine which identity to present in different online contexts. Combined with a means of authentication such as a password or a personal identification number (PIN), these 'digital identities' are often good enough to have confidence that a person is who they say they are when engaged in specific contexts online, for example logging into a social media account. These 'digital identities' may not be and are not necessarily required to be a verified real-world identity of an individual and as such they help provide some level of privacy protection and control to individuals over their real-world identities online.

Some online contexts, however, require greater levels of assurance about the identity of individuals, such as online financial services, to ensure greater trust in those individuals transacting online and to safeguard against harmful consequences for individuals. Online financial services organisations may also be subject to legal obligations to verify the identities of individuals for the purposes of 'know your customer' (KYC) and anti-money laundering (AML) regulations.[10] Increasingly, digital identity is also viewed as "*being of strategic importance to the future of digital services*,"[11] and vital to underpinning of the digital economy[12] and to its effective functioning and value creation.[13] These developments have helped

6 The Engine Room, (2020) Understanding the lived effects of digital ID: A multi-country report https://digitalid.theengineroom.org/assets/pdfs/200123_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive.pdf

[7] Bart van der Sloot, JIPITEC, (2014) Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data? https://www.ivir.nl/publicaties/download/1558.pdf

[8] European Court of Human Rights, (2019) Guide on Article of the European Convention on Human Rights https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

[9] National Institute of Standards and Technology (NIST) (2017), *Digital Identity Guidelines* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[10] FATF (2020), *Guidance on Digital Identity*, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

[11] Nyst et al, Consult Hyperion, (2016) *Digital Identity: Issue Analysis* https://chyp.com/wp-content/uploads/2020/06/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf

[12] UK Government Digital Service, (2019), *The Future of Digital Identity' https://gds.blog.gov.uk/2019/03/25/the-future-of-digital-identity/*

[13] GSMA (2014), *Mobile Identity - Unlocking the Potential of the Digital Economy* https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf

engender a digital identity industry,[14] and encouraged policy calls for the creation of a digital identity ecosystem[15] and the creation of digital identity markets to support the digital economy.[16]

While there is no universal single definition of 'digital identity' and it has multiple meanings across the private and public sectors, and in simple terms, it may be considered a way for organisations to verify that someone is who they claim to be in an online transaction. The World Bank considers digital identity as "*a set of electronically captured and stored attributes and credentials that can uniquely identify a person*." The UK government considers a digital identity as a trusted way for a citizen or consumer to prove "*one or more attributes about themselves .. and the linkage of those attributes to that same person as a uniquely identifiable individual.*"[17] In a joint paper the World Bank, the GSMA and the Secure Identity Alliance define digital identity as "*a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions*," and that may comprise biographic attributes such as name, age, gender, address or biometric data such as fingerprints or iris scans.[18] Of importance is that the National Institute of Standards and Technology (NIST) argues that while a "*digital identity is always unique in the context of a digital service*" there is not necessarily always a need to uniquely identify an individual in all digital transactional contexts and that "*accessing a digital service does not mean that an individual's real-life identity is known*," or needs to be known.[19]

While a 'digital identity' does not have to equate to a real-life identity, we increasingly see international organisations, industry sectors and governments define and promote 'digital identity' as a proxy for 'legal identity'. This report is concerned with this aspect of 'digital identity' – in other words, the digitisation of legal identity as a national digital identity represented as a digital ID.

2.1 The digitisation of legal identity

The digitisation of legal identity and its transformation to a national 'digital identity' has its origins in the interpretation of human rights instruments and international development efforts. Article 6 of the Universal Declaration of Human Rights (UDHR)[20] and Article 16 of the International Covenant on Civil and Political Rights[21] state that everyone has the right to recognition as a person before the law. These articles inform the United Nations legal identity agenda[22] and the UN Sustainable Development Goal (UN-SDG) 16.9 that calls for the provision of "*legal identity for all, including birth registration*" by 2030.[23] While the UN-SDG 16.9 does not define legal identity, the United Nations Legal Identity Expert Group defines legal identity as "*the basic characteristics of an individual's identity. e.g. name, sex, place and*

[14] Digital Identity Solutions Market worth $30.5 billion by 2024 https://www.marketsandmarkets.com/PressReleases/digital-identity-solutions.asp
[15] techUK, (2019) *The case for digital IDs: A techUK white paper* https://www.techuk.org/images/documents/digital_id_FINAL_WEBSITE.pdf
[16] Gov.UK, (2019), Minister confirms government ambition on digital identity https://www.gov.uk/government/news/minister-confirms-government-ambition-on-digital-identity
[17] DCMS, (2019) Digital Identity: Call for Evidence https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818801/Digital_Identity_-_Call_for_Evidence.pdf
[18] World Bank Group, GSMA, Secure Identity Alliance, (2016) Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf
[19] Footnote 1
[20] https://www.un.org/en/universal-declaration-human-rights/
[21] https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[22] https://unstats.un.org/legal-identity-agenda/
[23] https://sustainabledevelopment.un.org/sdg16

date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth."[24]

Civil Registration and Vital Statistics authorities and systems are a crucial means of conferring a legal identity to individuals from cradle to grave, and to ensuring individuals can secure access to welfare services and to their human rights.[25] Countries are increasingly facing multiple pressures to digitise and strengthen their CRVS systems and link them to national identity in efforts to enhance their role as a "*foundational registry at the center of an ID ecosystem*."[26] The Centre of Excellence for Civil Registration and Vital Statistics Systems has, for example, proposed that CRVS systems "*should stand as a foundation for a broader identity ecosystem upon which information other identification credentials are issued*,"[27] and that national ID systems should be linked with CRVS systems "*either by integrating the two systems in an organic way, or by creating two functionally distinct but interoperable systems."*[28] The World Bank argues that "*robust CRVS systems linked to identity management systems and tailored to local contexts form the foundation of all sectors and pillars of the economy and contribute to the sustainable development goals to end poverty, and ensure prosperity for all*."[29] We also see further evidence of policy approaches to strengthen the role of CRVS systems in national identity systems reflected in the work of the Center of Excellence on Digital Identity, Trade and Economy established by the United Nations Economic Commission for Africa. A key area of work of the Center is to support the harmonisation of civil registration and digital ID systems and the "*implementation of a comprehensive strategy for Digital ID, Trade and Economy for Africa*."[30]

The non-governmental organisation, Privacy International, has highlighted a broad range of digital identity initiatives given impetus by the UN-SDG 16.9 that go beyond creating systems for birth registration.[31] Multiple policy and industry agendas and initiatives are creating strategic imperatives to digitise legal identity and create 'digital' legal identities through "*digital identity (digital ID) systems*."[32] The language and allure of legal identity as a 'Digital ID' in support of social protection – including financial inclusion - growth of the digital economy, and even security, is a powerful argument for many governments, and the pressures to enable legal identity in the form of a 'digital identity' and digital identity management systems are great. For example, in a paper on ID4Africa, the United Nations asserts "*legal identity is a fundamental human right*," in the context of developing "*ID ecosystems around digital identity in the service of development, humanitarian action, security & facilitation*."[33] In its digital transformation strategy for 2020 -2030, the African Union also draws on UN-SDG 16.9 and calls for "*99.9% of people in Africa to have a digital legal identity as part of a civil registration process by 2030*" asserting also that Africa has a 'leapfrogging' opportunity to adopt digitised

[24] United Nations Strategy for Legal Identity for All, (2019) *Concept note developed by the United Nations Legal Identity Expert Group* https://unstats.un.org/legal-identity-agenda/documents/UN-Strategy-for-LIA.pdf

[25] UN Statistics Division, (2019) *Handbook on civil registration, vital statistics and identity management systems: Communication for development https://unstats.un.org/legal-identity-agenda/documents/Final-CRVS-Handbook.pdf*

[26] Secure Identity Alliance, (2015) *Civil Registry Consolidation Through Digital Identity Management* https://secureidentityalliance.org/publications-docman/public/7-15-12-17-civil-registry-consolidation-digital-identity-sia-final/file

[27] Centre of Excellence for CRVS Systems, (2019) *Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems* https://crvssystems.ca/IDcompendium

[28] Centre of Excellence for CRVS Systems, (2019) *Linking National ID and CRVS Systems: An Imperative for Inclusive Development* https://crvssystems.ca/sites/default/files/inline-files/CRVS_Gender_2.3_ID_e.pdf

[29] World Bank, (2017) *Strengthening CRVS and national ID* http://documents.worldbank.org/curated/en/306621510673094647/pdf/AUS16865-revised-public.pdf

[30] https://www.uneca.org/dite-africa/pages/what-way-forward-implementingor-strengthening-dite-africa

[31] Privacy International, (2018) The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights? https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk

[32] World Bank Development Report 2016, Spotlight 4, *Enabling Digital Development: Digital Identity* http://documents.worldbank.org/curated/en/896971468194972881/310436360_20160263021000/additional/102725-PUB-Replacement-PUBLIC.pdf

[33] UN Legal Identity Agenda - ID4Africa 2019 Toolkit: Legal Identity for All https://unstats.un.org/legal-identity-agenda/documents/UN%20LIA%20ID4Africa%20Digital%20Toolkit-final.pdf

solutions as driving force for "*innovative, inclusive and sustainable growth*."[34] Likewise, on the imperatives for digital economy, the European Union-African Union Digital Economy Task Force asserts that "*the majority of citizens in Africa lack government-issued identification, locking them out of access to critical public & private services*,"[35] and emphasises the "*opportunity for value creation through digital ID*" especially in cross-border contexts.[36]

In a 2007 report, UNESCO has suggested that a "*a globally unique identifier could seem the answer for according a person official digital existence in the Information Society*,"[37] to support stability in financial services and measures to combat cyber-attacks for example. However, the report also warns that such a globally unique identifier could end anonymity.

The emergence of ever more intrusive digital identity technologies and identity platform capabilities under pinning efforts to digitise legal identity, is leading to the commodification of 'legal identity' as perceived under the UDHR and global development efforts. For example, the narrative of digital identity companies has started to refer to a 'legal identity' as a "*fundamental human right*," as some imperative flowing from the UN-SDG 16.9. Worryingly, 'identity' is also promoted as an "*easily available commodity*" for which a "*new ecosystem of different applications naturally emerges*."[38] In other developments, Mastercard recently joined the identity partnership ID2020 and asserted its belief that "*digital identity is a fundamental human right.*"[39] The commodification of legal identity as a 'digital identity' across private and public spheres of life and the creation of digital identification systems that seek to give effect to a 'right to identity', raise multiple considerations. Digital identity systems are rapidly evolving and increasingly incorporating biometrics such as fingerprints and iris scans or digital behavioural attributes[40] as a means of creating and verifying a 'digital identity.[41]

"The expansion of digital identity, e-governance, and biometrics technology has rapidly increased interest and investment in identity systems by governments, development partners, and private sector actors."[42]

2.2 Biometrics and digital identity: informational bodies

Biometrics is generally defined as an automated means of recognising individuals based on their physical or behavioural characteristics. Biometrics technologies are variously seen as providing the "*means by which human beings can be uniquely identified,*" as an embodied

[34] African Union, (2020) *The Digital Transformation Strategy for Africa (2020 -2030)* https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

[35] Robert Viola, Director General of DG Connect, European Commission, (2020) *Putting the Digital Economy at the heart of EU-Africa cooperation* https://ec.europa.eu/digital-single-market/en/news/africa-europe-alliance-european-commission-and-african-union-commission-welcome-digital-economy

[36] World Bank and the Global Partnership for Financial Inclusion, (2018) *G20 Digital Identity Onboarding* *https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf*

[37] UNESCO, (2007), Information for all Programme, *Ethical implications of emerging technologies: a survey* *http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/ethical-implications-of-emerging-technologies-a-survey/*

38 Thales, Legal identity: A proxy for inclusion https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/legal-identity

[39] Mastercard joins ID2020 Alliance https://mastercardcontentexchange.com/newsroom/press-releases/2020/may/mastercard-joins-id2020-alliance/

[40] University of Exeter & Coelition, (2017) *Building Digital identities: The challenges, risks and opportunities of collecting behavioural attributes for new digital identity systems* http://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Buiding_Digital_Identities_with_Behavioural_Attributes.pdf

[41] Telefonica, (2016) *New paradigms of Digital Identity. Authentication and Authorization as a Service* https://www.wholesale.telefonica.com/en/information-centre/multimedia/new-paradigms-of-digital-identity-authentication-and-authorization-as-a-service/

42 Centre of Excellence for CRVS Systems 'Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems' http://www.data4sdgs.org/sites/default/files/2020-01/CRVS_Compendium_e_WEB_0.pdf

person, translating unique attributes of a physical identity to a digital identity, a 'digital ID'.[43] Problematically viewed as seeking to create "*one universal truth about the body as identity*,"[44] and as some "*objective and verifiable source of truth about our identities*."[45] By seeking to transform "*the body's surfaces and characteristics into digital codes and ciphers to be 'read' by a machine*,"[46] biometric technology "*changes irrevocably the relation between body and identity*."[47] It also changes the relationship of power between the state and the citizen. A machine-readable biometric identity automatically determines an individual's status that may result in them being excluded from participating in and benefiting from access to opportunities and services that biometric based digital identity system is intended to provide.

In 2007 Wickins argued that the "*the whole point of a biometrics system is exclusion—those who do not have the correct identifiers are excluded from access to whatever is protected by it*."[48] This highlights the need to consider at the social, political and the design level, the exclusionary nature of biometric technology and the underlying assumptions that the body is an objective source of truth of identity that can generally be reproduced and rendered machine readable at all times for all people and groups. This is an important consideration in the context of national digital identity schemes that rely on biometrics for identity verification and that may cause a range of harms. For example, such schemes may lead to the exclusion of individuals and groups. Some may fear that biometric identity systems may be used against them and so refuse to enrol and in so doing not gain access to the protections or services such schemes are meant to provide.[49] Some individuals may be excluded because they are unable to enrol their biometrics or subsequently verify their biometric identifiers. For example, it may be impossible to enrol an individual's fingerprints or verify fingerprints as a unique biometric identifier due to skin disease,[50] or because their fingerprints are too worn for example.[51] Anomalies with a person's iris, or eye disease[52] or eye surgery, or even age, may impact on the successful enrolment and subsequent use of an iris as a unique biometric identifier and as a means to verify biometric identity.[53]

Technology and design choices, and the politics of these choices can have significant implications for individuals and inadequately consider and put at risk their human rights, especially when a person's body and behaviour does not fit a predetermined notion of identity. In a 2011 'resolution', the Council of Europe raised concerns that the broad scope of biometrics technology and its rapid development and use for multiple purposes may put key human rights at risk.[54] The resolution cautioned that a country's legislation may not

[43] UNESCO, (2007), Information for all Programme, *Ethical implications of emerging technologies: a survey* *http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/ethical-implications-of-emerging-technologies-a-survey/*

[44] Rao and Greenleaf, (2013), *Subverting ID from above and below: The uncertain shaping of India's new instrument of e-governance* *https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/India_ID*

[45] Martin and Whitley, (2013), *Fixing identity? Biometrics and the tensions of material practices* http://personal.lse.ac.uk/whitley/allpubs/MCS2013.pdf

[46] Irma van der Ploeg, (1999) *The Illegal body: 'Eurodac' and the Politics of biometric identification* *https://link.springer.com/article/10.1023/A:1010064613240*

[47] Article 29 Data Protection Working Party. (2012) *Opinion 3/2012 on developments in Biometric Technologies* *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf*

[48] Wickins, (2007) *The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification* http://newton.ee.auth.gr/biometrics/images/docs/ethics.pdf

[49] Hindustan Times, (2019) *Assam to introduce biometric tracking for suspected illegal immigrants* https://www.hindustantimes.com/india-news/assam-to-introduce-biometric-tracking-for-suspected-illegal-immigrants/story-WPXUBWRm4EPapkiTktxQTP.html and Data & Society, (2019) *Digital Identity in the Migration & Refugee Context: Italy Case Study* https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf

[50] Drahansky et al, (2012) *Influence of Skin Diseases on Fingerprint Recognition* https://www.hindawi.com/journals/bmri/2012/626148/

[51] The global mobile trade association, the GSMA, reports that in Kenya, in a social protection programme, the elderly and those engaged in manual labour, were unable to provide proof of identity (called 'proof of life' in the programme) as their fingerprints were no longer readable by the biometric scanner. GSMA, (2020) *Opportunities for Improving Digital Identification in Social Cash Transfers* https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/04/SCT_Report_R_WebSingles.pdf

[52] Aslam et al, (2009) *Iris recognition in the presence of ocular disease* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2659699/

[53] See, The Wire (2017) *Unable to Verify Fingerprints or Iris, Aadhaar Denies Leprosy Patients Basic Services* https://thewire.in/government/unable-verify-fingerprints-iris-aadhaar-denies-leprosy-patients-basic-services

[54] Council of Europe, Resolutions 1797 (2011) The need for a global consideration of the human rights implications of biometrics

appropriately reflect the technology and the need to safeguard human rights in its use, and called for member state countries to revise their data protection laws without delay. The resolution further called for parties to promote proportionality in the adoption of biometric technologies and for the assessment of "*potential risks resulting from the use of biometrics for human rights and fundamental freedoms*." Of note is that in 2018, the UN High Commissioner for Human Rights, likewise cautioned that the "*creation of mass databases of biometric data raises significant human rights concerns*," and that it is worrisome that states appear to be adopting such measures without adequate legal and procedural safeguards in place.[55] Since the resolution was adopted, the modernised Council of Europe Convention 108+ (108+)[56] and at the EU level, the EU General Data Protection (GDPR) Regulation and the Law Enforcement Directive (LED)[57] now consider 'biometric data' as a special category of data requiring a higher level of protection in order to safeguard individuals against adverse effects of its use.

To date, approximately 142 countries have adopted data protection laws.[58] However, not all of those laws expressly provide for the regulation of biometric data. Neither have all of the 142 countries with national data protection laws established supervisory authorities to ensure the effective implementation of such laws or to help "*provide for effective remedies for individuals in case of violations of their human rights and fundamental freedoms.*"[59] World Bank data reveals that approximately 168 countries have established 'National ID' schemes, and of those schemes, approximately 159 are classed as a 'digitised ID system', and approximately 103 of those schemes collect biometrics in the form of fingerprints or iris scans.[60] This raises the question as to whether appropriate human rights-based data protection laws and legal safeguards are in place among all countries that are adopting biometric based national digital identity schemes for example. This especially important given that "*with the cost of biometric technology decreasing rapidly and global corporations and donors such as the World Bank promoting the use of biometrics in developing countries, more and more countries* [are] *enrolling their entire population in biometric programmes.*"[61]

Of note is the temporary seven month ban in August 2019 by the Moroccan data protection authority (le Commission Nationale de contrôle de la protection des Données à caractère Personnel) (the CNDP) on the use of facial recognition. Reflecting growing case law on digital identity and dimensions of privacy the CNDP argued that "Information technology is at the service of the citizen and is evolving within the framework of international cooperation. It must not affect identity, rights and collective or individual human freedoms. It should not be used as a means of disclose secrets of citizens' privacy."[62]

---

http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17968&lang=en

[55] *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights (August 2018)* https://undocs.org/A/HRC/39/29

[56] In paragraph 58 of the Explanatory Report to 108+, biometric data is considered "*data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual, is also considered sensitive when it is precisely used to uniquely identify*." https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[57] See the European Commission information site *'Data Protection in the EU'* for information on, and links to the General Data Protection Regulation and Data Protection Law Enforcement Directive https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[58] Greenleaf & Cottier, January 2020, '2020 ends a decade of 62 new data privacy laws' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611

[59] Council of Europe Resolution 1797 (2011)

[60] World Bank, (2018) *Identification For Development (ID4D) Global Dataset* https://id4d.worldbank.org/global-dataset

[61] Kloppenburg and Ploeg, (2018) *Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences* https://www.tandfonline.com/doi/full/10.1080/09505431.2018.1519534

[62] CNPD, Délibération n° D-194-2019 du 30/08/2019 relative à un moratoire sur la reconnaissance faciale https://www.cndp.ma/images/deliberations/deliberation-n-D-194-2019-30-08-2019.pdf

Also, of note is the withdrawal of a biometric identity card proposal and bill in Tunisia in 2018. These developments point to increased scrutiny of the proportionality and necessity of biometric identity systems and their impact on fundamental human rights and freedoms.[63]

For the reasons set out above, the processing of personal data and biometric data in digital ID systems should be expressly regulated in domestic legislation that clearly considers from the outset the impact on, and risks to, the human rights of individuals and that adopts appropriate safeguards.

3. Digital Identity scenarios

3.1 National identity schemes

More and more government are considering or are actively adopting centralised national digital identity schemes on the basis they are necessary to provide multiple benefits to the state and its citizens. These range from providing social protection measures, to giving access to public services, to achieving government efficiencies and accountability, to strengthening cross border trade, migration, and security and to supporting digital economy objectives. These schemes more often than not centre on creating a unique national identification number and a unique identity. A national digital identity includes not only demographic information such as a person's date of birth, full names and address, but increasingly their biometric fingerprints, iris and facial scans and may also include a person's ethnicity.

National identity schemes increasingly arise from pressures to create a 'legal identity for all under' the UN-SDG 16.9 or national and regional digital economy objectives. In their digital transformation strategy for Africa (2020-2030), the African Union (AU) argues that "*Digital ID forms a key mechanism for furthering the United Nations concept of 'legal identity for all*' and that a lack of legal identity makes it difficult for individuals to assert their human rights, including their citizenship. The AU further asserts that the "*rapid modernization and urbanization of African societies and the increasing sophistication of commercial transactions are increasing the need for legal identity. ID is required to obtain health services, tax certificates, travel documents, open bank accounts, exercise franchise, establish credit, etc.*"[64] A national digital ID is seen as the digitalisation of identity; as the unique identification of individuals and considered a 'vital component' of a digital economy. The allure of 'Digital ID' can seem too good an opportunity to miss for governments seeking to stimulate a digital economy. For example, the McKinsey Global Institute undertook analysis of Brazil, China, Ethiopia, India, Nigeria and recently reported that digital ID programs could increase GDP between 3 and 13 percent in 2030.[65] This a powerful goal for countries seeking to lift people out of poverty and to provide opportunities for all.

National identity schemes are envisaged as foundational ID systems that are population wide and that increasingly may seek to build on official civil registration systems (CRVS) including population registers. Civil registration is a critical event in a person's life and establishes their identity from birth, recording key details of the person (date, place of birth, name, parents' details) and that confers legal identity on that person. The CRVS is used to subsequently records an individual's key life events such as changes in name, marriage, divorce and death. A CRVS acts as the foundational means by which individuals are able to prove their identity and civil status to the state and its importance cannot be overstated. Increasing efforts are

[63] Access Now, (2018) Biometric ID vs. privacy: Tunisians win on privacy! But it's not over yet. https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet/

[64] African Union, (2020) *The Digital Transformation Strategy for Africa (2020 -2030)* https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

[65] McKinsey (April 2019), *Digital identification: A key to inclusive growth* https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx

being made to digitise civil registration systems from the point of capture of data at birth to strengthen the role of CRVS in identity management and the use of "*birth certificate unique identifiers***"** for national identity systems.[66] Digitising birth registrations is considered important to expanding its reach and benefits and has encouraged governments to adopt digital birth registration systems at birth, using mobile phone technology for example.[67] Increasingly, a CRVS is seen as constituting the backbone of a digital ID system[68] and their digitisation strengthens their role as a foundational element of a national digital ID system. What we see, is global policy[69] and technology merging to create a unique digital identity from cradle to grave.[70]

Recognising that measures to centralise national ID systems and to incorporate CRVS data and even digitising birth registrations, are well intentioned, they nonetheless carry a number of profound risks for individuals and communities. A major risk is that national digital ID systems may exclude and marginalise those unable to provide proof of legal identity by virtue that they are not registered in a civil registration system and cannot otherwise provide proof of 'legal identity'. Likewise, entirely digitised birth registration systems may exclude and deepen inequalities of already marginalised individuals and groups[71] who do not have access to digital infrastructures (even mobile phone based). These may deepen digital, social and economic divides and deny people access to health care, education, housing and other social protections and basic rights that depend on the ability of a person to present and national digital ID.

A lack of proof of 'legal identity' or bodies that are not compliant with technologically constrained biometric systems, and so that are not readily 'machine readable', may deny representation before the law or participation in the services national identity schemes are meant to support. It is crucial that national identity systems duly consider and design for human realities & human rights in order to mitigate risks such as exclusion, discrimination or infringements of privacy and personal identity. Many countries implementing or strengthening national identity systems are signatories to international human rights instruments that require them to respect, fulfil and protect fundamental rights such as the right to private life and the right to recognition as a person before the law and that such rights apply without discrimination on grounds of a person's race, colour, language, religion, national or social origin[72]. Any interference with such rights must have a clear legal basis in law and "*pursue a legitimate aim [and be] necessary and proportionate to that aim.*"[73]

A failure to make people the focus of design and build in human rights at a policy, legal and technical level has led to digital ID schemes being struck down or curtailed by restrictions on their use. The imperative to adopt a 'by design approach' to human rights is found in data protection instruments such as the Council of Europe Convention 108+. In the first instance, Article 1 of 108+ clearly sets that its purpose is to "*protect every individual, whatever his or*

---

[66] World Bank and World Health Organisation, (2014) *Global Civil Registration and Vital Statistics: Scaling up Investment Plan 2015-2024* *https://www.worldbank.org/content/dam/Worldbank/document/HDN/Health/CRVS%20Scaling-up%20plan%20final%205-28-14web.pdf*

[67] GSMA, (2017) *Innovations in Mobile Birth Registration: Insights from Tanzania and Pakistan* https://www.gsma.com/mobilefordevelopment/programme/digital-identity/innovations-in-mobile-birth-registration-insights-from-tanzania-and-pakistan/

[68] World Bank, (2015) Identification for Development (ID4D) Integration Approach

[69] United Nations, (2019) Introduction of the United Nations Legal Identity Agenda: a holistic approach to civil registration, vital statistics and identity management: Report of the Secretary-General https://digitallibrary.un.org/record/3841896

[70] GSMA, (2018) Roadmap for Digital Birth Registration: Identity for every child through the power of mobile https://www.gsma.com/mobilefordevelopment/resources/roadmap-for-digital-birth-registration-identity-for-every-child-through-the-power-of-mobile/ "*As an official and permanent recording of a child's identity, birth registration can help bestow access to a number of vital services, including healthcare and immunisations, education and social protections*."

[71] Plan International, *Identifying and addressing risks to children in digitised birth registration systems: a step-by-step guide* https://www.ohchr.org/Documents/Issues/Children/BirthRegistrationMarginalized/PlanInternationalGeneva_4.pdf

[72] Article 14 of the European Convention Human Rights https://www.echr.coe.int/Documents/Convention_ENG.pdf ; Article 7 of the Universal Declaration of Human Rights https://www.un.org/en/universal-declaration-human-rights/; Article 26 of the International Covenant of Civil and Political Rights https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

[73] Beduschi, A, (2019) Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3419039

her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy." Article 10 of 108+ further requires that controllers and where applicable processors shall, "*prior to the commencement*" of data processing, "*examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects*" and "*shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms*."[74] Similarly, the objective of the EU General Data Protection Regulation (GDPR) is to protect the "*fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*."[75] The GDPR also requires organisations to consider the risks to rights and freedoms of individuals posed by the processing of personal data and to adopt a data protection by design and default approach.

Examples of cases that have been struck down or curtailed by the courts on the basis of human rights considerations include:

3.1.1 Kenya and national digital ID - Huduma Namba ruling

Kenya has had a national identity card (national ID Card) in place since the 1980s and that, as in many countries, serves as a functional identity that is necessary or otherwise required to access services across the public and private sectors. Even seeking access to an office or government building can require proof of identity in the form of an identity card or passport. However, a "*the continuing colonial practice of recognising 42 tribes as indigenous to Kenya over other ethnic groups has made it difficult for some to apply for national IDs, including Somalis, Nubians, Shona, Maasais, Tesos and Arabs*."[76] A national ID card has long been required to obtain a mobile phone, to vote and to access most state services in Kenya.[77] Without a national ID card people are further marginalised and discriminated against in society.

In 2019, the government of Kenya sought to create a national 'digital ID' to address concerns over existing multiple but disjointed identity systems. It sought to create a single source of truth about a person's identity by establishing the National Integrated Identity Management System (NIIMS). The objective of NIIMS is to "*create and operate a national population register as a single source of information about Kenyan citizens and foreigners resident in the country*."[78] In addition to requiring the mandatory registration of a range of demographic data, NIIMS also required the collection of biometrics (including the DNA) from individuals and the GPS location of their homes. Once registered in NIIMS, individuals would be issued a unique identification number known as "Huduma Namba".[79] As proposed, registering with NIIMS was mandatory, and required to access key public services.

Lacking genuine public consultation, Huduma Namba failed at the policy, legal and technology level to address and prevent the discrimination and marginalisation that the national ID card historically created. In February 2019, Huduma Namba was subject a legal challenge on the grounds that it violated constitutional rights to privacy, equality and non-discrimination.[80] The case was heard in the Kenya High Court in April 2019. While permitting the continued

[74] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
[75] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504
[76] Caribou Digital, (2019) *Kenya's Identity Ecosystem* https://www.cariboudigital.net/wp-content/uploads/2019/10/Kenyas-Identity-Ecosystem.pdf
[77] ibid
[78] Justice Initiative, (2020) Kenya's National Integrated Identity Management Scheme (NIIMS) https://www.justiceinitiative.org/publications/kenyas-national-integrated-identity-management-scheme-niims
[79] National Government Communications Centre, (2019) Brochure NIIMS https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf
[80] Namati, (2019) *Case Filed to Stop New Digital ID Register in* Kenya https://namati.org/news-stories/case-filed-stop-new-digital-id-system-kenya/

collection of biometric data, and pending a later ruling, the court ruled that registration was no longer mandatory and that people could not be denied access to public services for failing to register their identities in Huduma Namba. The court also halted the requirement that people must register their DNA and the GPS location of their homes.[81] However, despite the success of this ruling, Huduma Namba still carried the risk that it would deepen the marginalisation of, and discrimination against, individuals and communities.

A second hearing was held in September 2019 in the Kenya High Court. In January 2020,[82] the Court issued its ruling and halted the implementation of Huduma Namba, finding that:

- "*biometric and personal data in NIIMS should only be processed if there is an appropriate legal framework in which sufficient safeguards are built in to protect fundamental rights*"
- the implementation of NIIMS may only proceed on the "*condition that an appropriate and comprehensive regulatory framework on the implementation of NIIMS that is compliant with the applicable constitutional requirements identified in this judgment is first enacted."*
- "the *collection of DNA and GPS co-ordinates for purposes of identification is intrusive and unnecessary"*

The Huduma Namba case[83] illustrates the over-reach of national digital ID systems and a failure to evaluate and reflect human rights in the policy, legal, technology and governance requirements of such systems. It raises the question yet again of identity by whom for whom and the need to ensure digital identity systems are inclusive and built on respect for and the safeguarding of, human rights and fundamental freedoms.

3.1.2 Jamaica and national digital ID

In a 2019 ruling the Jamaica Supreme Court declared "*unconstitutional, null, void and of no legal effect*" the National Identification and Registration Act (NIRA).[84] NIRA established a National Identification System (NIDS) that mandated the collection of biometric information on the entire Jamaican population and its storage in a centralised database, giving each person a unique national identification number.

The court argued that "*The mandatory nature of the requirement as well as the breadth of its scope, and the absence of a right to opt out, are not justified or justifiable in a free and democratic society*." The court also redefined the legal concept of privacy in Jamaica. On considering various international case law on national identity and privacy, the Court argued that "*privacy, as now understood, has at least three aspects: privacy of the person; informational privacy, and privacy of choice. These aspects of privacy arise not because they are conferred by the state but are possessed by all persons simply by being human*."

The ruling provides clarity on the application of exceptions to, and the inference with, human rights. The court analysed in detail what may be considered proportionate and necessary in a democratic society to achieve the legitimate aim of the state in implementing a national digital ID system as proposed. The analysis of proportionality and the 'ingredients of proportionality' provides valuable guidance for parties seeking to implement national digital ID systems. For example, in identifying the necessary ingredient of proportionality, the Supreme court of Jamaica argued that a measure interfering with a right must be "*carefully designed to achieve*

[81] Privacy International, (2019) Civil society achieves change, but risks still remain in Kenya's new biometric ID system https://privacyinternational.org/news-analysis/2774/civil-society-achieves-change-risks-still-remain-kenyas-new-biometric-id-system
[82] http://kenyalaw.org/caselaw/cases/view/189189/
[83] Nubian Rights Forum and Others v Attorney General
[84] Robinson – v- The Attorney General of Jamaica https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

the objective in question." It should "*should impair as little as possible the right or freedom in question*." But that even if "*an objective is of sufficient importance, and the first two elements of the proportionality test are satisfied, it is still possible that, because of the severity of the deleterious effects of a measure on individuals or groups, the measure will not be justified by the purposes it is intended to serve*." The ruling demonstrates as in the case of Huduma Namba, the importance evaluating the impact of digital ID systems on human rights, including discrimination and marginalisation. It assists in interpreting the application of Article 11 (Exceptions and Restrictions) and Article 10 (Additional Obligations) of Convention 108+.

Of note, and in the absence of national policy or regulatory considerations of human rights in digital identity systems, the Centre for Internet and Society (CIS) has developed an evaluation framework for the governance of digital identity systems.[85] The framework has the potential to help identify implications of national digital ID systems to privacy, surveillance, marginalisation and discrimination. CIS has already applied the framework to a case study of Huduma Namba.[86] Such approaches may be helpful in developing best practice in a human rights by design approach to digital ID systems.

Also of note is the publication by the international NGO, Privacy International, of a 'Guide to Litigating Digital Identity Systems'.[87] The guide reflects a range of case law on legal challenges to digital identity systems and their negative impacts on human rights. It is intended that the guide can support communities and civil society in their actions to ensure digital identity systems respect human rights and fundamental freedoms, including the necessity and proportionality of digital identity systems.

The legal challenges discussed above, and the pro-active engagement of civil society demonstrate the need to consider the development of a human rights impact assessment methodology (HRIA) for national digital ID systems. A HRIA can help ensure that human rights are appropriately considered in the development of policy and integrated into identity technologies and the management of identity systems. A HRIA approach can especially help ensure the identification and mitigation of risks and harms to those "*who may be most vulnerable, marginalized or discriminated against*."[88]

3.2 Digital identity and mandatory SIM card registration

Billions of people around the world use a mobile phone and mobile networks to make calls, send texts and use the mobile internet. To do this they need a mobile SIM card (known as a subscriber identity module 'SIM'). Without a SIM (or an eSIM)[89] an individual cannot use their mobile phone to make calls, send text messages or access the internet on a mobile operator's network (MNO). A SIM card is used by MNOs to authenticate subscribers and control their access to mobile networks and services. As discussed below, the SIM card has significant implications for the digital identity and human rights of billions of people around the world.

A SIM card has two key identifiers. An IMSI - international subscriber identity module – that is a unique electronic identifier stored in the SIM card and that maps to a mobile phone number

[85] See https://cis-india.org/internet-governance/blog/governing-id-a-framework-for-evaluation-of-digital-identity
[86] The Centre for Internet & Society, (2020) Governing ID: Kenya's Huduma Namba Programme https://cis-india.org/internet-governance/digital-id-kenya-case-study
[87] Privacy International, (2020) https://privacyinternational.org/report/4156/guide-litigating-identity-systems-introduction
[88] Götzmann, (2019), The Danish Institute for Human Rights, *Handbook on Human Rights Impact Assessment* https://www.researchgate.net/institution/The_Danish_Institute_for_Human_Rights
[89] https://www.gsma.com/esim/

and identifies and authenticates the SIM to the mobile network. The second identifier is called an ICCID – integrated circuit card identifier – and is generally printed on the outside of a SIM Card. The ICCID is a globally unique serial number that is the identifier of the SIM card itself. The ICCID also contains the mobile network operator's account identification number for a subscriber and helps ensure a subscriber is billed for the services they consume.

SIM card identifiers, along with a unique electronic identifier of the mobile phone[90] are generally recorded by mobile network operators when people make or receive calls creating a detailed record of an individual's behaviour and their social networks by reference to key digital identifiers.[91] These unique mobile identifiers and account and service related attributes[92] are increasingly used in creating and binding digital identities – including biometrically - to individuals. In many countries a mobile digital identity is linked and bound to a legal identity and to a national identity number and that may lay the foundations for surveillance with profound implications for human rights. The use of these identifiers as digital identities is beyond the control of individuals.

People face a range of socio-economic and political pressures to adopt mobile phones and services, that may make them necessary or essential (especially during times of crisis), and that digital economy policy and initiatives seek to encourage. In 2007, speaking at the Connect Africa Summit in Kigali, President Paul Kagame said that "*In just ten years, what was once an object of luxury and privilege, the mobile phone has become a basic necessity in urban and rural Africa*."[93] Research among consumers in the UK found they considered mobile and internet services essential for a range of purposes.[94] For some groups, such as refugees, a mobile phone may be considered as important as food and water,[95] and a tool of protection and a lifeline, [96] and 'essential'.[97]

According to the global mobile trade association, the GMSA, there are currently 5.2 billion unique mobile subscribers across the world.[98] That's 5.2 billion mobile SIM cards with multiple unique digital identities that in many cases may be linked by law to national or functional identifiers such as a national identity card number or a passport number.[99] Increasingly in many countries, in order to obtain a mobile SIM an individual is required by law to provide proof of, and to register their legal identity, which may include their unique national identity number. SIM registration law may also require individuals to register their biometrics – including facial scans[100] - simply to obtain a mobile phone. This regulatory policy lays the foundation for monitoring and mass surveillance across different dimensions of mobile activity tied to a digital mobile identity such as mobile money services for example.

---

[90] Known as an international mobile equipment identity (IMEI). IMEIs are issued by and maintained in a global database by the GSMA https://imeidb.gsma.com/imei/index# See also, GSMA IMEI Services https://www.gsma.com/services/gsma-imei/

[91] Wikipedia, Call Detail Record, https://en.wikipedia.org/wiki/Call_detail_record

[92] GSMA, (2018), Data attributes as the new digital identity currency https://www.gsma.com/identity/wp-content/uploads/2018/03/Data-Attributes-as-the-New-Digital-Identity-Currency-deck-FINAL.pdf

[93] The New Times, (2007) ICT no longer luxury for Africans – Kagame https://www.newtimes.co.rw/section/read/1640

[94] OFCOM, (2014) Mobile and internet services now 'essential' to consumers https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2014/essential-comms-services

[95] The Conversation, 2019, *For young refugees, a mobile phone can be as important as food and water when arriving in a new country* https://theconversation.com/for-young-refugees-a-mobile-phone-can-be-as-important-as-food-and-water-when-arriving-in-a-new-country-122077

[96] UNHCR, (2016) *CONNECTING REFUGEES: How Internet and Mobile Connectivity can Improve Refugee Well-Being and Transform Humanitarian Action* https://www.unhcr.org/uk/news/latest/2016/9/57d7d4478/mobile-connectivity-lifeline-refugees-report-finds.html

97 Latonero et al, Data & Society, (2019) Digital Identity in the Migration & Refugee Context: Italy Case Study https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf

[98] GSMA Intelligence https://www.gsmaintelligence.com/data/

[99] The figure of 5.2 billon may not represent a unique individual but a unique activated SIM card. An individual may possess and use more than one SIM card.

[100] Radio Free Asia, (2019) *Chinese Telecoms Companies Confirm Mandatory Facial Recognition For New Numbers* https://www.rfa.org/english/news/china/facial-recognition-12052019162028.html

3.3 Mobile SIM Card registration, mobile money and transactional privacy

According to the GSMA, as of January 2020, **approximately 155 countries** have adopted mandatory SIM registration laws that prevent people obtaining a mobile SIM card and accessing mobile services unless they can provide proof of state-issued legal identity. In the first instance this creates a significant barrier to those who may lack legally recognised proof of identity, exacerbating inequalities and discrimination and denying people access to mobile services, including public services. In the absence of laws that objectively set out the necessity and proportionality of SIM registration measures and absent appropriate legal protections, including data protection laws that reflect Convention 108+, SIM registration may interfere with the right to privacy of communications, the right to identity and personal development and the right to communicate anonymously (as an aspect of the right to freedom of expression).[101] SIM registration forces individuals into digital identity surveillance across multiple dimensions of their mobile connected activities.

Adding political pressure to ensure compliance with SIM registration law, and so restricting space for privacy and other fundamental rights, some governments have ordered mobile operators to disconnect service to the SIM cards of individuals who fail to register a prescribed legal identity recognised by the state.[102] These disconnection orders can deny service to many millions of people, disenfranchising them further from the digital economy, and public services that may require a mobile phone, and also from their right to freedom of expression[103] for example. In some countries, regulatory bodies have also imposed heavy fines on mobile operators for failing to meet government mandated SIM requirements.[104] For those lacking the necessary proof of state recognised legal identity to obtain a SIM card, it may force them to rely on black market SIM cards and criminalise them for doing so. In a ruling of the Supreme Court of Jamaica the presiding judges warn of the "*ultimate coercive power of the state being enlisted to ensure compliance*" with identity measures[105] – as is happening in the realm of national mandatory SIM card registration.

Martin (2019) discusses how mobile money platforms, that play a crucial role across Africa in facilitating loans, payments and cash transfers, leverage SIM registration identity data to support Know Your Customer (KYC) and Customer Due Diligence Checks (CDD). Mobile SIM registration and device identity data and transaction data combine to facilitate the surveillance of users of mobile money services.[106] It's a hidden surveillance that may be carried out by financial institutions or by mobile operators that provide financial services themselves under a mobile money licence. These developments narrow the opportunities for individuals to be free of the gaze of governments and private entities to enjoy a right to transactional privacy.

---

[101] See for example, Breyer v. Germany (2020) European Court of Human Rights on the mandatory registration of SIM cards https://hudoc.echr.coe.int/eng-press#{"itemid":["003-6624862-8792771"]} Of particular note is the dissenting opinion of Judge Ranzoni in this case (page 44) and who disagreed with the majority view of the court and argued that SIM registration was not proportionate to the legitimate aim pursued and so amounted to a violation of the Article 8 right to privacy. It is likely this matter will be revisited in the ECHR.

[102] For example, following instructions from the Tanzania Communications Regulatory Authority approximately 3 million SIM cards were disconnected as a result of people lacking a national identity card or passport required as part of the biometric SIM registration law. A further 15 million SIM cards are due for disconnection https://www.theeastafrican.co.ke/business/Tanzania-to-switch-off-sim-cards/2560-5437128-ws8o5nz/index.html In Myanmar millions may have their SIM cards deactivated unless they register a valid identity document by the 30 June 2020 https://www.mmtimes.com/news/millions-myanmar-risk-having-mobile-phones-cut-after-sim-registration-deadline.html Likewise in Ghana, the government intends to deactivate SIM cards not registered using the national identity card by June 2020 https://www.moc.gov.gh/meet-press-statement

[103] Article 19, (2020) *Tanzania: SIM card deactivation poses a significant threat to freedom of expression* https://www.article19.org/resources/tanzania-sim-card-deactivation-poses-a-significant-threat-to-freedom-of-expression/

[104] In Nigeria the mobile operator MTN was fined $5.2 billion reduced to $1.7 billion after legal challenges https://en.wikipedia.org/wiki/MTN_$5.2_billion_fine and in Tanzania, the Tanzania Communications Regulatory Authority imposed fines amounting to millions of Tanzanian shillings on six mobile network operators https://itweb.africa/content/DZQ587VPoxgqzXy2

[105] Footnote 2

[106] Martin, A (2019) *Mobile Money Platform Surveillance* https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12924

They raise questions of effective transparency[107] for users of the mobile money services and effective legal protections and oversight across multiple regulatory domains, especially given that some countries may lack effective data protection and privacy frameworks and independent regulatory oversight. Martin also raises a troubling concern that "*government bodies have taken a keen interest in more invasive forms of regulatory oversight by directly accessing mobile money platform data.*" While such interest may not be driven by security concerns but about concerns over tax revenues, the potential for function creep and abuse nonetheless remains absent of appropriate legal, regulatory and technical protections.

As discussed above, in approximately 155 countries possessing and being able to prove a legal identity is now a prerequisite for obtaining a SIM card. No proof of legal identity – no SIM card. SIM registration binds multiple SIM and device identifiers to a person's unique legal and national identifiers, and to the identifiers used by mobile money service providers to uniquely identify an individual, creating an 'economic identity'. It is argued that mobile money services "*require an economic identity*", defined as a "*a form of functional identity, as its purpose is to enable access to a specific set of services (such as access to credit, insurance and savings products)*.[108]

A shift from cash payments to digital payments, and a move to a 'payments as a platform model',[109] means that an 'economic identity' and the transactional surveillance that such models facilitate raise multiple questions of proportionality, necessity and appropriateness of linking multiple identities and the facilitation of surveillance. In Tanzania, under recent SIM Card Registration Regulations, if the names an individual presents for the reregistration of their SIM card, differ or result in mismatches with those held by the National Identification Authority, then a mobile operator can verify SIM card ownership based on verification of a customer's mobile money transactions – an 'economic identity'.[110] The shift to digital money transactions and to mobile money platforms also signifies a profound shift in digital identity and a user's control over such identities and their privacy as individuals and as members of their communities.[111]

Exacerbating the human rights concerns of national SIM registration schemes, some governments have proposed regional SIM registration platforms or frameworks on the basis of combatting crime. For example, the East African countries of Kenya, Rwanda, Uganda and South Sudan have discussed creating a harmonised SIM card registration framework.[112] In Southeast Asia, Thailand's telecommunications regulator has proposed that the country's national SIM registration scheme should be extended to Laos, Cambodia and Myanmar.[113] The East African Communications Organisation has established a working group to "develop a regulatory framework for implementing SIM card registration within EAC Member States."[114]

---

[107] Bowers et al, (2017) *Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services*. In a review of 54 mobile money apps, 44% had no privacy policy, and of those 33% were not "*written in the most common languages used within the country*" and "*50% do not identify to the user what data is used and collected*" https://www.usenix.org/system/files/conference/soups2017/soups2017-bowers.pdf

[108] GSMA, (2019) State of the Industry Report on Mobile Money https://www.gsma.com/sotir/wp-content/uploads/2020/03/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2019-Full-Report.pdf

[109] ibid

[110] See the Electronic and Postal Communications (Sim Card Registration) 2020 https://tanzlii.org/content/electronic-postal-communications-sim-card-registration-regulations2020 and https://aloysassociates.co.tz/2020/02/22/the-electronic-and-postal-communications-sim-card-registration-regulations-2020/

[111] While digital financial services may provide privacy from an immediate social and domestic gaze of cash payments, as discussed by Riley https://novafrica.org/wp-content/uploads/2019/05/Hiding_loans_in_the_household_using_mobile_money__Experimental_evidence_on_microenterprise_investment_in_Uganda-4.pdf and by Hamdan https://www.diw.de/documents/publikationen/73/diw_01.c.669402.de/diw_roundup_131_en.pdf digital financial services may engage hidden surveillance with implications not immediately obvious nor within an individual's control.

[112] The Exchange, (2015) *East African Countries Move Closer to Common Sim Registration* https://theexchange.africa/trending/east-africa-countries-move-closer-to-common-sim-card-registration/

[113] ITU News, (2016) *SIM registration: A new Thai model for regional collaboration* https://news.itu.int/sim-registration-a-new-thai-model-for-regional-collaboration/

[114] East Africa Communications Organisation. WG 1: ICTs Policy and Regulatory Frameworks Harmonization http://www.eaco.int/pages/working-groups

While national SIM registration raises multiple concerns about the linking of unique mobile identifiers to state issued legal identifiers at a state level, these concerns increase in the absence of agreed and compatible cross border data protection and privacy frameworks & rules regulating law enforcement access to and use of identity related data for example.

As discussed, digital IDs borne of mandatory SIM registration law, may be linked to national and other functional IDs, and that may lead a global unique ID. It makes observable most aspects of a person's life lived via their mobile devices. This digital ID policy and infrastructure leaves little space to be free of surveillance and for human flourishing. That national identity policy and law and/or compulsory linked identities may interfere with the right to privacy in a manner that erodes other freedoms is a point made in two supreme court rulings from India and Jamaica.

3.3.1 India – Linking Aadhaar, SIM registration, privacy and freedoms

"*instead of the State being transparent to the citizen, it is the citizen who is rendered transparent to the State*."[115]

In 2009 the Indian government began to implement the social protection Aadhaar programme with the objective of issuing a 'unique identification number' (UID) called 'Aadhaar' to all residents of India.[116] The Aadhaar programme created a centralised database linking a UID to a broad range of demographic data about a person and to their biometric information such as all ten fingerprints, two iris scans and a facial photograph.[117] India also has had mandatory SIM registration in place since approximately 2005. Mandatory SIM registration developed to require mobile operators to collect and record approximately 31 categories of personal, demographic, financial, account, SIM and device related data, in addition to biometric information such as fingerprints and iris scans. Mobile operators are required to submit the collected data to a government database.

In 2014, the Department of Telecommunications (DoT) issued instructions to all Indian mobile operators requiring them to collect and record a customer's unique 'Aadhaar' number as part of the mandatory SIM registration process.[118] In 2017, the DoT issued instructions to all mobile to reverify existing customers through an Aadhaar based eKYC process, and to verify new customers through the same Aadhaar process.[119] These instructions and requirements had the effect of linking multiple personal, mobile device and account identifiers and financial identifiers to what in all effects was a national identity system - Aadhaar. It could be argued that linking SIM registration and Aadhaar created a surveillance foundation unlawfully infringing on the fundamental right to privacy, deemed to be a constitutional right in a 2017 landmark ruling of the Supreme Court of India.[120] In the context of the importance of privacy to human flourishing raised in this report, and how perceptions of surveillance may influence people's behaviour and sense of self and identity, of note is the court's assertion that "*privacy is .. necessary in both its mental and physical aspects as an enabler of guaranteed freedoms*" and for the development of their personality.[121]

---

[115] [115] Supreme Court of India, (2018) *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.* Writ Petition (Civil) No 494 of 2012 https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[116] See https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html

[117] See https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html

[118] Department of Telecommunications, (2014) File No: 800-09/2010 VAS *Collecting Aadhaar numbers along with Customer Acquisition Form (CAF) of mobile telephone applications https://dot.gov.in/sites/default/files/doc.pdf*

[119] See https://dot.gov.in/sites/default/files/Re-verification%20instructions%2023.03.2017.pdf?download=1

[120] Supreme Court of India, (2017) Justice K S Puttaswamy (Retd) and ANR v. Union of India and ORS https://uidai.gov.in/images/Right_to_Privacy.pdf

[121] ibid

The Aadhaar programme has been subject to various legal challenges since 2012[122] on the grounds that it was unconstitutional, culminating in a Supreme Court ruling in 2018.[123] The Supreme court held that it was constitutional under the Aadhaar Act[124] to use a UID for the purposes of establishing the identity of a person entitled to receive social protection benefits such as cooking fuel or food grains for example. Importantly however, among other decisions, the court found that the mandatory linking of SIM registration identity with an Aadhaar unique identity lacked the "*backing of a law*" and failed "*to meet the requirement of proportionality*," and necessity. The court argued that "*the entire population cannot be subjected to intrusion into their private lives*" because of the "*misuse of SIM cards by a handful of persons*." The court found the government order to link Aadhaar identities to mobile subscriber identities to be an *"disproportionate and unreasonable state compulsion,"* and declared the order as unconstitutional and that it must stand invalidated.

The Supreme Court ruling emphasised that the "*mere existence of a legitimate state aim will not justify the means which are adopted*." The court argued that by "*making Aadhaar compulsory for other activities such as air travel, rail travel … there will be virtually no zone of activity left where the citizen is not under the gaze of the State. This will have a chilling effect on the citizen*." Privacy as an aspect of human flourishing.

The Supreme Court Aadhaar ruling illustrates the importance of adopting a human rights approach to the development of policy and technology and their application, ensuring measures are necessary and proportionate to legitimate aim pursued, and that mitigates risks to human rights. The court also recognised the importance of a robust regime for data protection also noting that the "*lack of regulatory frameworks, or the inadequacy of existing frameworks, has societal and ethical consequences and poses a constant risk that the concepts of privacy, liberty and other fundamental freedoms will be misunderstood, eroded or devalued*." The court further commented that "*Creating strong privacy protection laws and instilling safeguards may address or at the very least assuage some of the concerns associated with the Aadhaar scheme which severely impairs informational self-determination, individual privacy, dignity and autonomy*." Though a draft data protection bill[125] has been developed in India, there remains a need to establish a harmonised policy, legal and regulatory approach to digital ID that a mobile device mediates across different regulated services.

3.4 Digital Identity in humanitarian contexts – identity by whom for whom?

Humanitarian and development organisations are increasingly adopting identity management systems to help them achieve crucial programmatic goals, whether in providing social protection benefits to people in crisis or tracing the family of a refugee fleeing civil war. In their updated Handbook on Data Protection, the International Committee of the Red Cross (ICRC) acknowledges that such organisations "*do not always need to know someone's legal identity*"[126] to support beneficiaries. In a welcome approach and adopting long standing data protection principles of data minimisation and purposes limitation, the ICRC argues instead of beginning with the question "*who are you*?" organisations should begin by asking "*what do I need to know from that person to provide aid or assistance*?." This approach also seeks to ensure both the adopted identity system and the data used to populate the system and support beneficiaries, is proportionate, necessary and not excessive to achieve a clearly identified and

[122] See https://economictimes.indiatimes.com/news/politics-and-nation/chronology-of-aadhaar-case/articleshow/65965443.cms?from=mdr

[123] Supreme Court of India, (2018) *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.* Writ Petition (Civil) No 494 of 2012 https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[124] The Aadhaar programme was envisaged to give effect to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (amended in 2019 following the Supreme Court Case https://uidai.gov.in/images/news/Amendment_Act_2019.pdf)

[125] See https://www.medianama.com/2020/02/223-joint-parliamentary-committee-consultation-pdp-bill-2019/

[126] International Committee of the Red Cross, (2020) *Handbook on Data Protection in Humanitarian Action – Second Edition* https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html

legitimate aim, in keeping with data protection frameworks such as the modernised Convention 108+.[127]

But what identity system is appropriate and who does the identity system serve? There are in general two types of identity systems in use in the majority countries:[128]

- A 'functional identity' (functional ID) system that limits the process of identification, authentication and authorisation to a specific well-defined purpose and service. For example, a functional ID may be used to provide access to health care or welfare payment services or to provide a voter ID. Humanitarian organisations may create and issue a functional identity to provide beneficiaries access to key services.
- A foundational identity (foundational ID) system covers the whole population of a country and acts as a general-purpose ID system providing proof of official 'legal identity' that may be widely accepted for multiple purposes across public and private sector services.[129] Foundational ID systems may include national ID systems and civil registration systems and population registration systems, and that may in turn support functional identity systems.

In their handbook on data protection, the ICRC (2020) advises there are number of ongoing initiatives to develop digital ID systems as a form of foundational identity that can serve as a legally recognised identity providing access to mobile SIM cards, bank accounts or mobile money services. A key challenge in the humanitarian context is enabling access to legally recognised forms of identity that are often a prerequisite for obtaining a mobile SIM card or mobile money services for example. One of the most important and influential global humanitarian organisations, the United Nations High Commissioner for Refugees (UNCHR) has committed to supporting "*a legally recognized as well as a digital identity,*" for all refugees, returnees, asylum seekers, forcibly displaced and stateless persons. To this end the UNHCR also supports setting up separate refugee registration systems that governments can "*include into their national identity systems as this is a win-win for everybody*." [130]

The UNCHR has adopted a high-level data protection policy[131]setting out principles and rules to help protect the personal data and privacy of beneficiaries, and that is elaborated in more detailed data protection guidelines.[132] The guidelines reflect key concepts, definitions governance principles, and individual rights enumerated in European data protection frameworks such as the Council of Europe Convention 108 and the EU General Data Protection Regulation. While the guidelines do not contain any separate and specific section on 'identity' they nonetheless emphasise the need to protect the identity of persons of concern, through the use of pseudonymous identifiers for example. Though the guidelines do not expressly address 'identity' the UNHCR has developed separate guidance on registration and identity management[133] and which supports the use of the UNCHR Population Registration

[127] See for example Article 5 on the legitimacy of processing , and in particular the Paragraph 40 of Explanatory Report to Article 5.
[128] This report is limited to consideration of functional and foundational identity systems used by the majority of countries and does not discuss other emerging types of identity such as self-sovereign identity https://sovrin.org/faq/what-is-self-sovereign-identity/ Such forms of identity should be the subject of further consideration.
[129] Adapted from World Bank, (2019) ID4D Practioner's Guide http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf and Financial Action Task Force (2020) Guidance on Digital Identity http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

[130] UNCHR (2018), UNHCR Strategy on Digital Identity and Inclusion https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf
[131] UNCHR, (2018) POLICY on the Protection of Personal Data of Persons of Concern to UNHCR https://www.refworld.org/pdfid/55643c1d4.pdf
[132] UNHCR, (2018) Guidance on the protection of personal data of persons of concern to the UNHCR https://www.refworld.org/docid/5b360f4d4.html
[133] See https://www.unhcr.org/registration-guidance/

and Identity Management Eco-System (PRIMES).[134] The PRIMES system is also used to "*supports States through the joint use of the digital tools contained in [PRIMES], including its biometrics systems*."[135] While the UNHCR is to be commended for adopting both policy and guidance to ensure the protection of personal data and privacy of beneficiaries, research suggests there is a need to reconsider how these translate into meaningful privacy experiences on the ground for the communities identity system seek to serve.

In 2018, the UNHCR implemented a programme to establish "*a unified database for the purposes of protection, identity management, documentation, provision of assistance, population statistics and ultimately solutions for an estimated 900,000 refugees who have fled from Myanmar to Bangladesh in successive waves of forced displacement*."[136] The non-governmental organisation, The Engine Room, recently conducted research and published a study into a number of digital identity systems in use in Bangladesh, Ethiopia, Nigeria, Zimbabwe and Thailand.[137] The Engine Room identifies limitations to its research and that it sought to understand the 'lived experiences' of digital ID systems on individuals that they "*cannot necessarily extrapolate one person's experience to the norm – though there are times when every person interviewed experienced an aspect of a system the same way*." The report includes findings from research in the joint UNHCR and Government of Bangladesh identity verification system implemented to provide assistance to Rohingya refugees.[138] The verification process involved "*the collection of three types of biometric data – face photographs, 10 fingerprints and two iris scans – for individuals age 13 and above*," and that refugees being assigned identity 'smart' cards.[139]

The Engine Room study reports on how the process of identification among the Rohingya refugees resulted in multiple fears and concerns about the purpose of the digital ID system and about data use and privacy. Rohingya refugees falsely believed that accepting a digital identity card would lead to their repatriation to Myanmar and to circumstances that led to their fleeing the country. This resulted in refugees choosing not to register – trust needs to be a foundation of digital ID and organisations should consider what may negatively impact trust and address those factors. That requires community engagement and understanding which should be key requirement of digital identity approaches.

The Engine Room research also revealed that many people interviewed "*could not read at all, while others could not read English or Bengali*" which from a data protection perspective raises multiple questions and concerns. For example, transparency is a cornerstone of data protection laws around the world. Transparency is crucial to helping individuals understand not just how the use of their data will benefit them, but also any potential risks and the safeguards adopted to mitigate such risks. Transparency is also crucial to helping people understand the legal basis relied on to process their personal data, of the uses that will be made of their data, of rights and choices over such use and how to exercise rights and choices pursuant to international data protection frameworks and the UNHCR data protection policy.[140] Providing genuine transparency and facilitating understanding requires organisations to test the effectiveness of 'transparency' measures. EU data protection authorities advise that if organisations "*are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/notices/ policies etc., they can test these, for example,*

[134] UNHCR, (2017) Modernizing Registration and Identity Management in UNHCR: Introducing PRIMES https://www.unhcr.org/blogs/modernizing-registration-identity-management-unhcr/
[135] UNHCR, (2019) report *Displaced and Disconnected* https://www.unhcr.org/innovation/displaced-and-disconnected/
[136] See, *Joint Bangladesh/UNHCR verification of Rohingya refugees gets underway* https://www.unhcr.org/en-us/news/briefing/2018/7/5b3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html
[137] The Engine Room, (2020) Understanding the Lived Effects of Digital ID: A Multi-Country Study https://digitalid.theengineroom.org/assets/pdfs/200128_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive_Edit1.pdf
[138] Footnote 113
[139] Footnote 114
[140] It is important to consider that Bangladesh does not have a data protection act that may apply to the processing of personal data and so it is unclear how Rohingya refugees could exercise data protection concerns and rights in law.

through mechanisms such as user panels, readability testing."[141] The Engine Room further reports that "*Refugees displayed low levels of understanding about the purpose of the biometric component of the digital ID system and of the consequences of a potential data breach*." Accepting the urgent need to assist Rohingya refugees in their plight, and that efforts were apparently made via community leaders to improve transparency, the research provides various learnings and suggests the need to review measures to improve comprehension and understanding among vulnerable refugees and the legitimise the processing of personal data.

It is also uncertain what legitimate basis[142] the UNHCR relied on to enrol Rohingya refugees in the joint digital identity system of the UNHCR and the Government of Bangladesh. As the Engine Room points out in their research, the UNHCR data protection guidance[143] does not prescribe a legitimate basis that must be relied on but rather ambiguously leaves such decisions to the "*data controller, assisted by the data protection focal point."* The guidance states that while there is a 'principled need' to ensure an appropriate legitimate basis the 'practical relevance' of the processing will determine whether or not the processing requires the consent of individuals. However, and in a seeming contradiction, the guidance further states that "*given the vulnerability of most beneficiaries and the nature of humanitarian emergencies, many humanitarian organizations will not be in a position to rely on consent for most of their personal data processing.*" [144] This raises the question: what 'legitimate basis' did the UNCHR and the Government of Bangladesh rely on, and what did the Rohingya refugees believe was the legitimate basis? This is especially important given that Bangladesh does not have a data protection law to protect personal data and privacy, and that the UNHCR as an international organisation is not subject to the GDPR for example.

It is beyond this report to detail every finding of the study as it relates to the digital ID system deployed in Bangladesh by the UNHCR and the Government of Bangladesh. However, the study reveals the importance of developing a shared language on digital ID and on community involvement in the development of policy, design and implementation of digital ID systems. It highlights how a failure to engage can lead to negative perceptions and resistance to humanitarian assistance and to its success or failure. The study also highlights the multiple negative impacts of digital ID programmes on human dignity and autonomy to name but a few. The study should be required reading for policy makers and for all parties in the 'digital ID for humanitarian action' ecosystem. It should be used to inform the development of appropriate standards for personal data protection and privacy and associated human rights and freedoms to better reflect and protect 'lived experiences'.

The need to consider and engage communities and develop a human rights by design approach to digital ID in order to safeguard rights and freedoms is more pressing than ever given the assertion by the UNHCR that "*many States, particularly in Africa, are increasingly … considering including refugees in [national] foundational ID platforms*." The UNCHR further suggest that such foundational ID efforts should also consider how they can facilitate meeting the KYC requirements of national mandatory SIM Registration and other services such as mobile money. [145] Though in the Displaced and Disconnected report, the UNCHR does not outright question the continuing justification for mandatory SIM card registration, the UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, has reported that "*states should refrain from making the identification of users a*

[141] Article 29 Working Party, (2018) Guidelines on Transparency under Regulation 2016/679 www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[142] Article 5(2) of Convention 108+ requires organisations to ensure that the processing personal data is carried out on the basis of the free, specific, informed and unambiguous consent of an individual or some other legitimate basis laid down in law. Article 5(4) further requires that personal data be processed fairly and in a transparent manner; collected for explicit and specified purposes; are adequate, relevant and not excessive and not kept for longer than necessary.

[143] Footnote 109

[144] Footnote 109

[145] UNHCR, (2020) Displaced and Disconnected report https://www.unhcr.org/innovation/wp-content/uploads/2019/04/Displaced-Disconnected-WEB.pdf

condition for access to digital communications and online services and requiring SIM card registration for mobile users."[146]

In the Executive Summary to the Displaced and Disconnected report, the UNCHR expresses a keenness to engage with a broad range of actors such as governments, the mobile operators, financial service providers and humanitarian and development agencies. The summary does not make any reference to representatives of the beneficiary communities of or civil society non-governmental organisations. One hopes this is an oversight as such groups are essential to developing inclusive approaches and to addressing concerns discussed in this report about mandatory SIM registration and mobile money services for example.

4. Concluding thoughts and considerations for policy makers

As the report has highlighted 'digital ID' systems whether national digital identity systems or functional digital identity systems - including hybrid SIM card registration identity systems - may pose significant risks to the rights and freedoms of individuals. Legal challenges continue to highlight the unconstitutional nature of these digital identity schemes and the lack of adequate legal and governance frameworks to safeguard privacy and protect against risks of surveillance, marginalisation and discrimination. There is a danger that those who such schemes seek to serve are not the focus of policy, law and design but more some overarching national security objective in order to create a single source of truth about citizens.

While case law has very much examined national identity schemes in the context of constitutional and legal rights of citizens, we see the development of digital identity systems by international organisations such as the UNCHR. International organisations such as the UN, need to process and often transfer significant amounts of personal data, including special categories of personal data relating to ethnicity or biometrics of beneficiaries. Given their global influence in driving identity for all (under the UN-SDG 16.9) and their crucial role in providing humanitarian assistance, and given that it is argued data protection frameworks such as the GDPR do not apply to international organisations,[147] the UN should consider adopting and acceding to the Council of Europe Convention 108+.[148] While international data protection frameworks may inspire data protection policy and practice among international organisations, it is important that an organisation's obligations and individuals rights are clearly set out in law and that individuals have clear legally defined rights, protections and avenues of redress in law.

Digital ID systems cut across different regulated sectors and requires a harmonised policy, legal and governance approach to ensure consistency in the application of human rights to digital identity. This would appear to require capacity building between policy makers, regulators, government agencies, humanitarian and development agencies and civil society on the subject human rights and digital ID, to avoid digital ID being commodified as human

[146] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, 22 May 2015
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc
[147] Kuner, C, (2020), American Journal of International Law, *The GDPR and International Organizations*
https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-and-international-organizations/5EDB2AA87AB6BAF9C3731FF3CD0080A9/core-reader
[148] Greenleaf, G, (2017) *The UN should adopt Data Protection Convention 108 as a global treaty: submission on the 'right to privacy in a digital age' to the UN High Commission for Human Rights*
https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf

right. To avoid 'being human' simply meaning humans becoming machine readable bodies to be read, profiled and acted on, and being "treated as mere objects."[149]

As the Jamaica Supreme Court ruling stressed, rights "*are possessed by all persons simply by being human."* Digital ID schemes should consider their impact on 'being human' and the lived experiences they may create. This requires the development of best practice on designing for human rights in digital ID. It is recommended that the Council of Europe considers the development of:

- human rights impact assessment methodology for digital identity systems, including criteria on the necessity and proportionality of national digital identity systems
- guidelines that reflect the provisions of Convention 108+ and that support policy makers, industry, app developers and regulators in ensuring that national digital identity systems do not undermine human rights and fundamental freedoms and in particular the right to data protection and privacy, and that take a human rights by design approach. Such guidelines may exclude the use of persistent global unique identifiers for example, and address the requirements if functional versus national foundational identity systems. Any such guidance will need to reflect the mobile developments below.

There is more to be written on this subject as we see calls grow for international immunity passports and digital IDs during a time of COVID.[150] Given the central role that mobile devices play in peoples' lives and is likely to play in 'covid immunity passport' policy making, of note, is the patent application by Apple, for using a device for 'controlled identity credential release'. The patent application relates to the controlled release of identity credentials stored on a mobile device, such as driver's licenses, passports, and clearly argues that the "collection/sharing [of credentials] should occur only after receiving the consent of the users or other legitimate basis specified in applicable law."[151]

Importantly, the German Federal Office for Information Security (BSI) also recently announced that its national digital identity credentials (eID) will soon be able to be stored on a secure chip on Samsung mobile devices.[152] This development and the standards adopted can help inform mobile digital identity solutions (especially given that the eID is designed not use a global or persistent unique identifiers but pseudonyms and to prevent profiling by relying parties).[153]

---

[149] Council of Europe Convention 108+, Explanatory Notes, Page 16, Preamble, Section 10 "*the preamble expressly refers to the right to personal autonomy and the right to control one's personal data, which stems in particular from the right to privacy, as well as to the dignity of individuals. Human dignity requires that safeguards be put in place when processing personal data, in order for individuals not to be treated as mere objects.*"

[150] The Guardian (2020) Surveillance a price worth paying to beat coronavirus, says Blair thinktank https://www.theguardian.com/world/2020/apr/24/surveillance-a-price-worth-paying-to-beat-coronavirus-says-blair-thinktank

[151] United States Patent Application *20200320188 (October 8 2020),* controlled identity credential release' *http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220200320188%22.PGNR.&OS=DN/20200320188&RS=DN/20200320188*

[152] SecureIDNews, 07 October 2020, German national digital ID is going mobile https://www.secureidnews.com/news-item/german-national-digital-id-is-going-mobile/ and Samsung Newsroom, 23 July 2020, Samsung, BSI, Bundesdruckerei and Telekom Security Partner to Bring National ID to Your Smartphone https://news.samsung.com/global/samsung-bsi-bundesdruckerei-and-telekom-security-partner-to-bring-national-id-to-your-smartphone

[153] Federal Office for Information Security, (2017) Overview of the German eID system https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_01_Whitepaper_final.pdf?version=1&modificationDate=1499172188962&api=v2