

**THE REPUBLIC OF UGANDA**

**IN THE HIGH COURT OF UGANDA AT KAMPALA  
(CIVIL DIVISION)**

**MISCELLANEOUS CAUSE NO. \_\_\_\_\_ OF 2022**

- 1. INITIATIVE FOR SOCIAL AND ECONOMIC RIGHTS (ISER) LTD ..... APPLICANTS**
- 2. THE UNWANTED WITNESS (U) LIMITED**
- 3. THE WOMEN'S PROBONO INITIATIVE (U) LIMITED**
- 4. HEALTH EQUITY AND POLICY INITIATIVE LIMITED**

**VERSUS**

- 1. THE ATTORNEY GENERAL**
- 2. NATIONAL IDENTIFICATION REGISTRATION AUTHORITY (NIRA) ..... RESPONDENTS**

**AFFIDAVIT IN SUPPORT**

I, **Dr. Thomas Fisher**, of c/o ALP Advocates, Lotis Towers, 5<sup>th</sup> Floor, Plot 16 Mackinnon Road, P.O. Box 28611 Kampala, [info@alp-ea.com](mailto:info@alp-ea.com) do solemnly swear or (affirm) as hereunder;

1. THAT I am an adult British Citizen of sound mind, a Senior Research Officer with Privacy International, 62 Britton Street, London, EC1M 5UY, United Kingdom, a holder of a PhD from the Centre of African Studies at the University of Edinburgh and I swear this affidavit in that capacity.
2. THAT Privacy International ("PI") was established in 1990 as non-profit, non-governmental organisation based in London although its work is global.
3. THAT I have worked at PI since 2016 and led PI's work on identity systems, working with an interdisciplinary team of lawyers, technologists, and communication specialists at PI, with exclusion being a central theme of our work. I have conducted research into identity systems in Latin America, Asia and Africa.
4. THAT PI works at the intersection of modern technologies and rights. It exposes harms and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change.
5. THAT PI believes that privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built.
6. THAT within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

7. THAT PI has worked on issues relating to identification systems since its foundation, playing a notable and influential role in scrutinising the proposed ID system in the UK from 2002 until 2010 – which was ultimately scrapped after the government spent over £257 million and issued 15,000 cards. (See Alan Travis, “ID cards scheme to be scrapped within 100 days”, *The Guardian*, 27 May 2010. Available at: <https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards>).
8. THAT PI has taken its work on ID systems to the global stage. Among other work, PI has co-developed a global litigation guide for ID systems in partnership with the Harvard Law School’s International Human Rights Clinic. In all of its work, Privacy International draws from the expertise of partner civil society organisations around the globe in Africa, Latin America, Europe and Asia.
9. THAT as a result, PI is at the centre of a global network critically engaging with identity systems, and is a source of research, educational resources, and analysis. On numerous occasions PI has been called as an expert on identity and digital identity issues by the UK government, and entities such as the Council of Europe’s Committee of Convention 108, the United Nations Office of the High Commissioner for Human Rights (OHCHR) as well as the United Nations Special Rapporteurs on extreme poverty and human rights and on the promotion and protection of human rights and fundamental freedoms while countering terrorism.
10. THAT in April 2019, I submitted an expert affidavit on behalf of PI relating to Petition No. 56 of 2019 as consolidated with Petitions 58 & 59 of 2019 on the validity of the implementation of the National Integrated Identity Management System (NIIMS) in Kenya. My expertise was noted and recognised by the High Court of Kenya on several matters in its final judgment issued on 30 January 2020 (see *Nubian Rights Forum & Others v. The Hon. Attorney General*, Consolidated Petitions No. 56, 58 and 59 of 2019 [hereafter “Huduma Namba judgment”], para. 876.)
11. THAT I have supported the research conducted by our partner organisations around the globe.
12. THAT I am a member of the Privacy and Consumer Advisory Group (PCAG), advising the UK government on how to provide users with inclusive, trusted and secure means of accessing public services. (see <https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group>)
13. THAT I am also a member of the Privacy and Inclusion Advisory Forum (PIAF), advising the UK government on their development of a new single sign-on for accessing government services and how this can be inclusive across society.
14. THAT my expert evidence addresses some of the issues surrounding ID and exclusion, and how the UN, World Bank and other institutions recognise the risks of exclusion and discrimination from these systems.
15. THAT I will also explain the risks surrounding the use of biometrics in these systems and give examples from around the globe to illustrate risks surrounding the introduction of ID systems as well as to identify measures to mitigate these risks.

## **ID, Exclusion, and Discrimination**

16. THAT despite the discourse that often surrounds these systems as being ‘inclusive’, the challenge of the systems is that they lead to deeper exclusion of those who do not have access to these systems (see **Hanmer, L. and Daham, M., ‘Identification for Development: Its Potential for Empowering Women and Girls’, World Bank, 9 November 2015. Available at: <https://blogs.worldbank.org/voices/identification-development-its-potential-empowering-women-and-girls>; Pokharel, N. and Niroula, S., **How a Legal Identity Leads to a Better Life, Open Society Foundations, Voices, 22 January 2015. Available at: <https://www.opensocietyfoundations.org/voices/how-legal-identity-leads-better-life>**).**
17. THAT exclusion and discrimination have been a crucial theme that has emerged from my own research and investigation into ID systems, namely people not being able to access services that they are entitled to access (either by the state or private providers) because of either lacking the required ID documents or otherwise not being able to use them.
18. THAT a state can have a legitimate interest in ascertaining or verifying the identity of an individual. However, it does not follow from this that the state should require the possession of a singular form of ID document in order to meet that requirement; as this makes exclusion due to non-possession of a particular document arbitrary and unfair.
19. THAT when considering any use of a National ID system, it is important to understand the difference uses to which an identity system can be put. An ID system can be used to identify someone: that is, to answer the question, “who is this?”. An example of this use would be when the police stop an individual and are looking to find out the person’s identity. This is distinct from the use of an ID system to verify an identity; that is, to answer the question, “is this person who they claim to be?”. An example of this would be a person applying for social security, when they make a claim that they are a particular person and this claim needs to be verified through evidence.
20. THAT these two uses of ID are distinct, and are important to appreciate the differences between these. Any questions surrounding national ID must be seen in this context, and the different uses to which ID can be put.
21. THAT the Secretary General of the United Nations has drawn attention in particular to the risks of exclusion in his report on the role of new technologies for the realisation of economic, social and cultural rights:

“One major concern linked to comprehensive digital identification systems is that these systems can themselves be sources of exclusion, contrary to their purpose. Costly or difficult registration requirements, for example, may prevent poor and disadvantaged populations from fully participating in an identity system. Women in some regions face legal or customary barriers to obtaining official identification. A lack of Internet connectivity, needed for online authentication, also can contribute to exclusion. Older persons and members of some occupational groups performing mostly manual labour may have difficulties providing fingerprints that are clear enough for the purposes of the identify systems. Services that require authentication

- at the point of delivery create problems for older persons or persons with disabilities who may not be able to travel. Difficulties also arise when the name and gender in identity documentation are not properly reflected in the identity system, exposing people with non-binary gender identity to particular risks. Lastly, exclusion can also result from a particular group being given identity documents that are different from those of others.” (Exhibit TF1, Available from [https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session43/Documents/A\\_HRC\\_43\\_29.pdf](https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf) para 33)
22. THAT the Secretary General of the United Nations concluded: “not being able to prove one’s identity can severely inhibit, and even effectively block, access to essential services, including housing, social security, banking, health care and telecommunications (Available from [https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session43/Documents/A\\_HRC\\_43\\_29.pdf](https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf) para 30)
  23. THAT while judicial consideration of the differentiated impacts of ID-related exclusion on specific communities is incipient, the fact that they exist has already been recognised.
  24. THAT in Kenya, the High Court identified that there may be a segment of the population who ran the risk of exclusion, highlighting “a need for a clear regulatory framework that addresses the possibility of exclusion in NIIMS. Such a framework will need to regulate the manner in which those without access to identity documents or with poor biometrics will be enrolled in NIIMS”. (see *Huduma Namba Judgment*, para. 1012)
  25. THAT when ID is made a requirement to access public services, it becomes relevant to the fulfilment of a State’s obligations in relation to economic, social and cultural rights under the International Covenant for Economic, Social and Cultural Rights (ICESCR). When a State Party to the ICESCR such as Uganda takes action which furthers or impedes access to social protection and, as applicable, healthcare, the right to social security and the right to health (Articles 9 and 12 respectively) are engaged. Each of these rights has multiple dimensions which, among others, encompass notions of availability and accessibility. These, in turn, require States to ensure that the rights are effectively respected, protected and fulfilled. (Committee on Economic, Social and Cultural Rights, General Comment No. 14: The Right to the Highest Attainable Standard of Health, para.12. Available at: [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/Download.aspx?symbolno=E%2fC.12%2f2000%2f4&Lang=en](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=E%2fC.12%2f2000%2f4&Lang=en))
  26. THAT the potential for ID systems to have exclusionary effect has been highlighted by the UN Secretary General. In a report addressed to the Human Rights Council, he noted that “not being able to prove one’s identity can severely inhibit, and even effectively block, access to essential services, including housing, social security, banking, health care and telecommunications”. (available at [https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A\\_HRC\\_43\\_29.pdf](https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf))
  27. THAT where specific groups cannot effectively access ID systems, concerns of discrimination may arise.
  28. THAT the ICESCR, in its Article 2, imposes an obligation on State parties to guarantee the rights contained therein “without discrimination of any kind as to race, colour, sex,

language, religion, political or other opinion, national or social origin, property, birth or other status”.

29. THAT the ICESCR does not explicitly mention age-based discrimination against the elderly. However, it is understood by the UN Committee on Economic and Social Rights (CESCR) that this not a deliberate omission in its General Comment on non-discrimination, the CESCR explicitly identified “age” as one of the relevant protected characteristics to be read into Article 2.
30. THAT further, in each of its General Comments addressing the right to social security and the right to health, the CESCR has explicitly identified older persons as a key group with particular needs and challenges, and whose enjoyment of rights warrants a specific approach.

### **Recognition of the risks of exclusion due to ID in the humanitarian and development community**

31. THAT a key driver of digital identity systems has been that they would lead to empowerment and inclusion including social and financial inclusion. But whilst motivated by aspirations for inclusivity and openness, the way digital identity systems have been designed and implemented result in different forms of discrimination and exclusion. This has been also acknowledged by leading proponents of digital identity systems.
32. THAT the document “Principles on Identification for Sustainable Development: Toward the Digital Age” is a set of principles about the development and deployment of ID endorsed by over 20 organisations including the African Development Bank, ID4Africa, the UNHCR, UNDP, United Nations Economic Commission for Africa, and the World Bank Group. The document has recently been revised by these endorsing organisations, from which it can be surmised that it is indicative of the current state of the art thinking amongst the international development and humanitarian community. **(Exhibit TF9, Available at <https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf>)**
33. THAT the document notes in its preamble, “Vulnerable and marginalized groups are often the least likely to have proof of their identity, but also the most in need of the protection and services linked to identification. People who are unable to obtain or easily use identification are therefore at greater risk of being left behind when strict identification requirements must be met to access services.”
34. THAT the Principles also include the Inclusion by Design Principle: “Identification systems should prioritize the needs and address the concerns of marginalized and vulnerable groups who are most at risk of being excluded and who are the most in need of the protections and benefits identification can provide. This requires working with communities to proactively identify legal, procedural, social, and economic barriers faced by particular groups, risks and impacts specific to these groups, and adopting appropriate technologies and mitigation measures to ensure that new or updated identification systems do not reinforce or deepen existing inequalities.”

35. THAT it is therefore clear that there is a recognition across the international human rights, development and humanitarian communities that identification systems come with the risk of exclusion.
36. THAT the risks and issues surrounding identity systems were a key concern in the UN Special Rapporteur (UNSR) on Extreme Poverty and Human Rights 2019 report on the digital welfare state. In his report, the UNSR highlighted some key issues associated with identity verification systems including “political backlash to concerns over privacy, security and cybersecurity” as well as equality, non-discrimination and public participation. (Available at <https://www.ohchr.org/en/documents/thematic-reports/digital-welfare-states-and-human-rights-report-special-rapporteur>).

#### **Individuals and communities at risk of exclusion**

37. THAT it has been well-documented that there are individuals and communities who are at a higher risk of being excluded. A report by the UN Secretary General highlighted groups commonly vulnerable to exclusion from ID systems, noting the legal and practical obstacles for the poor and disadvantaged, women, older persons, members of some occupational groups, people with disabilities, and people whose name and gender were not properly reflected in the ID system. (See UN Secretary General, *The role of new technologies for the realization of economic, social and cultural rights*, para. 33.)
38. THAT furthermore, courts in various jurisdictions including in Jamaica, Kenya and India have explored in their judgements on how identity systems can lead to discrimination between different groups of persons, particularly in the absence of a strong legal framework, they may also disproportionately impact the rights of marginalised and vulnerable people, compounding and multiplying factors of exclusion and they can lead to the perpetuation of pre-existing inequalities and injustices. (available at <https://privacyinternational.org/report/4159/guide-litigating-identity-systems-impact-identity-systems-rights-other-privacy>)
39. THAT the World Bank’s major ID4D-Findex survey of 2017 revealed that, The World Bank’s major ID4D-Findex survey of 2017 revealed that, in low income countries those in lower income quartiles are less likely to have an ID. Specifically, 43% of the poorest 20% do not have an ID, as opposed to the 25% of the richest 20%. (Exhibit TF4, available at <https://documents1.worldbank.org/curated/en/953621531854471275/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-Insights-from-the-ID4D-Findex-Survey.pdf>).
40. Women are particularly affected, with 44% of women in low income countries lacking an ID, as opposed to 28% of men. The World Bank argues that the unequal access to identification limits women’s economic opportunities. (available at <https://blogs.worldbank.org/developmenttalk/importance-womens-equal-access-identification-times-global-crisis>)
41. These systems also affect migrant populations. The way ID systems are deployed around the world means that migrant populations may not be able to register for such documentation and therefore be excluded from accessing the services tied to the provision of this particular form of identity. (available at <https://antheppress.com/legal-identity-race-and-belonging-in-the-dominican-republic-hb>;

### Exclusion of those with ID

42. THAT the issue of exclusion, when it comes to ID, is not only an issue of whether an individual is able to get the necessary ID card or not: an individual can have an ID card but still suffer from exclusion. This could be, for example, when an ID document has inaccurate information, and it is not easily corrected by the individual concerned.
43. THAT an example of groups that may have access to ID documents, but can face major obstacles in making use of these documents, is intersex, non-binary and transgender persons. PI conducted research on trans people, i.e. people who do not identify with the gender marker they were assigned at birth in 2021. As this research on trans people in the Philippines, Argentina and France reveals, this is a group that faces particular issues because their ID documents do not reflect how they present their gender identity. As a result of this, they face difficulties accessing social services, in particular healthcare. (See exhibit TF7, available at <https://privacyinternational.org/long-read/4372/my-id-my-identity-impact-id-systems-transgender-people-argentina-france-and>)

### Biometrics and Exclusion

44. THAT biometrics is the “measurement of unique and distinctive physical, biological and behavioural characteristics used to confirm the identity of individuals”. (see Privacy International (2013) *Biometrics: Friend or Foe of Privacy?*” available at [https://privacyinternational.org/sites/default/files/2017-11/Biometrics Friend or foe.pdf](https://privacyinternational.org/sites/default/files/2017-11/Biometrics%20Friend%20or%20foe.pdf), page 5)
45. THAT modalities can include fingerprints, iris, facial photographs, vein patterns, etc. Key features of the physical body are extracted and stored as an electronic template, that is then stored – usually in either a centralised database, or in a smartcard. This template can be used to authenticate the identity of an individual – this is a 1-1 match of the individual against the stored template, to answer the question, “Is this x?” Biometrics can also be used to identify an individual – this is a 1-many match, to answer the question “Who is this?”
46. THAT the issues surrounding biometrics that have been identified as raising serious human rights concerns. In 2018, the United Nations High Commissioner for Human Rights issued a Report on the right to privacy in the digital age which highlights significant human rights concerns with the creation of mass databases of biometric data:

“Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person’s life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual’s rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is worrisome that some States are embarking on vast biometric data-base projects without having adequate

legal and procedural safeguards in place.” (Available at <https://undocs.org/A/HRC/39/29>)

### Biometrics and identity systems

47. THAT identity systems rely on the collection and storage of biometric data for a variety of purposes. They can be used during the registration process for ‘deduplication’, i.e. the attempt to make sure that all the people registered are unique. The data gathered during system registration, to be compared with biometric data collected at the point of a given transaction requiring identity system verification. (available at <https://privacyinternational.org/long-read/3067/have-biometric-id-system-coming-your-way-key-questions-ask-and-arguments-make>)
48. THAT the risks of discrimination and exclusion associated with the use of biometric digital identity systems have been highlighted by courts in various jurisdiction. For example, as recognised by the Kenyan High Court in relation to the potential changing of biometrics over time and authentication failures or the dissenting judgement of the Indian Supreme Court referring to error rates in biometric systems being particularly high for the young, the aged, disabled persons, as well as persons suffering from health problems.
49. THAT another challenge is that biometrics can potentially be used to identify an individual for their entire lifetime. This means that caution has to be shown in the face of changing regimes or political contexts, and also the changes in technology. The technology surrounding biometrics is continually evolving, which places new pressures and risks on biometric systems. For example, it is possible to clone a fingerprint from a photograph, using commercially-available software. (Available from <https://www.bbc.co.uk/news/technology-30623611>)
50. THAT the use of a centralised database for biometrics compounds concerns as noted in the report of the UN High Commissioner for Human Rights quoted in **paragraph 42 above**. In considering the fundamental rights implications of storing biometric data in identity documents and residents cards, the European Union Agency for Fundamental Rights (“FRA”) found: “The creation of national dactyloscopic [fingerprint biometric] databases of all identity and residence cards holders would constitute a grave interference with the right to respect for private and family life (Article 7 of the Charter [European Union Charter of Fundamental Rights]) and with the right to protection of personal data (Article 8 of the Charter).” (See *Fundamental rights implications of storing biometric data in identity documents and residence cards*: page 14. Available from [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf)).
51. THAT the FRA also found: “The establishment of a central national database would also increase the risk of abuse for using the data for other purposes than those originally intended. Due to its scale and the sensitive nature of the data which would be stored, the consequences of any data breach could seriously harm a potentially very large number of individuals. If such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights.” (See *European Union Agency for Fundamental Rights (2018) Fundamental rights implications of storing biometric data in identity documents and residence cards*: page 14. Available from



[https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf).

52. THAT these broader human rights concerns, beyond the issues surrounding exclusion, are important to consider when understanding the issues surrounding biometrics and exclusion. The concerns and fears of individuals towards these systems are genuine.
53. THAT an issue is that biometrics are essentially probabilistic. Other means of authenticating the individual are deterministic: for example, when a PIN is entered, there is either a match with the stored PIN or there is not. However, biometrics are different. As the UK's National Cyber Security Centre puts it, "[...] no two captures of biometric data will produce truly 'identical' results. So, a biometric system must make an estimation as to whether two biometric samples come from the same individual." Thus, a biometric system is not making a definitive decision on whether an individual is who he or she claims to be, but rather a probabilistic one. This means that some are going to be excluded from what they are entitled to, or falsely accepted as somebody they are not, as a result.

### **Biometric failures**

54. THAT one of the most common forms of biometrics are fingerprints, but this raises issues. As the Secretary General noted above, "Older persons and members of some occupational groups performing mostly manual labour may have difficulties providing fingerprints that are clear enough for the purposes of the identify systems." (see **paragraph 19 above**).
55. THAT as adults age, the quality of the fingerprint declines. Research for the European Commission found that, after the age of 70, "The quality degradation of the fingerprints for this part of the population is quite significant." Fingerprint quality declines linearly from the ages of 65-90. Similarly, manual labourers can have worn fingerprints. (See **European Commission (2016) *Evaluation of the implementation of Regulation (EC) No 767/2008 of the European Parliament and Council*: page 105. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0328&from=EN%20page%20207>**)
56. THAT in the book *When Biometrics Fail*, there are many examples presented of people unable to make use of biometrics because of disabilities, age, or other causes of biometric failure. The author concludes: "these technologies do not operate with the mechanical objectivity claimed for them."
57. THAT the recognition of these risks has prompted calls for the regulation of the use of biometric identity systems such as those issued by the UN Human Rights Council which has called upon States "to take appropriate measures to ensure that digital or biometric identity programmes are designed, implemented and operated with appropriate legal and technical safeguards in place and in full compliance with human rights law".

### **Concerns specific to the healthcare setting**

58. THAT in guidance provided by the United Nations Development Program (UNDP) on the use of digital technologies in the healthcare setting, they note: "For people without an officially recognized legal identity (ID) document, accessing basic services, including HIV and health service, can be a major barrier." In particular, the risk of exclusion is

present for groups that are already marginalised. *“they also pose the risk of excluding already marginalized populations, such as people living with HIV and key populations in criminalized settings, if proper safeguards are not in place to mitigate these risks.”*

(Exhibit TF 10 Available from <https://www.undp.org/sites/g/files/zskgke326/files/2021-07/UNDP-Guidance-on-the-rights-based-and-ethical-use-of-digital-technologies-in-HIV-and-health-programmes-2-EN.pdf>).

### Exposing individual and groups

59. THAT a notion of the long-term benefits of digital ID often brings in an idea of “visibility”, and whilst some see ‘visibility’ as an unquestioned good, the benefits must be contextualised and the harms and dangers of being ‘visible’ must be recognised. In the case of access to healthcare, the use of biometrics to authenticate the identities of people in the healthcare system can bring about its own exclusions. According to the UNDP, “The use of biometrics, however, can pose significant rights-related risks, since it facilitates the identification of individuals, potentially exposing them to rights violations, especially when individuals belong to stigmatized, marginalized or criminalized groups.” (Available from <https://www.undp.org/sites/g/files/zskgke326/files/2021-07/UNDP-Guidance-on-the-rights-based-and-ethical-use-of-digital-technologies-in-HIV-and-health-programmes-2-EN.pdf>)
60. THAT in Kenya in 2015-2017, the health authorities - alongside the Global Fund to Fight AIDS, TB and Malaria, and with the support of UNAIDS - planned to conduct a study of those with HIV and key populations. This study made use of biometrics in this research. However, the presence of the biometrics for this study prompted an outcry from people with HIV and key population. The concern was multifaceted: firstly, there was a fear of function creep, i.e. that the biometric data collected from this study would be used for other purposes, such as by the police to facilitate arrests. Secondly, there was a fear that data breaches could expose stigmatising information. In the face of protests and objections from the affected population, the planned use of biometrics was dropped. (Available from <https://www.kelinkkenya.org/wp-content/uploads/2018/07/“Everyone-said-no”.pdf>)
61. THAT when health care provision is linked to a biometric system, it raises the fear of stigmatisation and discrimination, particularly for those who have stigmatising conditions. There have been press reports that people in India with HIV/AIDS have not sought treatment because of the fear of linking this treatment to their Aadhaar card.
62. THAT these examples demonstrate that it is essential that the use identification systems, including biometric data, in healthcare be treated with the appropriate caution.

### Global examples of ID systems

63. THAT in examining examples of ID systems around the world, particular consideration should be given to the very different contexts in which they exist. The nature of the ID systems, rates of birth registration, and in particular what other forms of ID other than a national ID might be available to people, vary greatly.

64. THAT the following selected examples show that exclusion is a persistent area of concern with the deployment of ID systems around the world, with people having difficulty accessing essential government services due to not having the required identity documents.

### Argentina

65. THAT research in Argentina by Chudnovsky and Peeters into the Argentina's National Identity Document (Documento Nacional de Identidad, or "DNI") reveals the challenges and administrative burdens in place for many in obtaining this essential ID document. These are classed as learning costs (a lack of information, or misinformation, about the application procedure); psychological costs (for example, issues of shame and inadequacy around working with bureaucrats); and compliance costs (the costs of time and money, for example, in travelling to get the necessary documents). **(Exhibit TF2, Available from <https://journals.sagepub.com/doi/abs/10.1177/0020852320984541>)**
66. THAT exclusion from the DNI creates, in the words of Chudnovsky and Peeters, a "cascade of exclusion", as the exclusion from the ID system also leads to exclusion from social security and benefits. In particular, they highlight the case of the Universal Child Allowance (Asignacion Universal por Hijo (AUH)), a payment given to people who are not in formal employment and have a child under 18 resident in Argentina, for which both the eligible parent and child are required to hold a DNI. In this case, exclusion from the national ID scheme also involves exclusion from social protection.

### Chile

67. THAT exclusion can impact individuals who are entitled to but not able to get an identification card or number. PI conducted research in Chile, where a single identity number is used for a very broad range of purposes in the public and private spheres. It is required to access state health care, to sign some contracts, and is used as a 'loyalty card' in some shops. PI conducted research, in particular with migrants who were entitled to but not able to get a card, often – as they saw it – because of the pressure that the bureaucracy was under. The research found that as a result these individuals experienced difficulties in accessing state healthcare, change jobs, move house, or even getting married. (See "Privacy International (2018) Exclusion and identity: Life without ID **(Exhibit TF3, available from: <https://privacyinternational.org/feature/2544/exclusion-and-identity-life-without-id>)**)

### Pakistan

68. THAT in Pakistan, the national ID – the Computerised National Identity Card (CNIC) – was held, in 2017, by 96 million out of a population of 210 million citizens. Holding a CNIC is a requirement to access Pakistan's largest social security scheme, the Benazir Income Support Programme (BISP). One of the largest social security schemes in the world, this provides cash transfers to around 4.7 million households in Pakistan. Alongside the eligibility criteria, receiving these funds requires a Computerised National Identity Card (CNIC), Pakistan's national ID card. **(Available from**

<https://www.opml.co.uk/files/Publications/A2241-maintains/making-bisp-shock-responsive-14062021.pdf?noredirect=1> page 10)

69. THAT the challenges of instituting ID as a compulsory requirement to receive benefits were highlighted in research conducted for the UK's Department for International Development. The researchers found: "Possession of a CNIC is required to verify IDs and is essential. It is, however, also an access barrier to the most vulnerable who are more likely not to have a CNIC". Particularly when considering the use of BISP in the case of responses to shock or disaster relief, the research found: "CNIC possession is likely to remain a core eligibility criterion to access any type of disaster relief but, at least at the moment, this criterion is likely to exclude those who need support the most... The biggest hurdle to rapidly accessing relief is the CNIC."

### **Republic of Ireland**

70. THAT in the Republic of Ireland, the Public Services Card (PSC) is a biometric identity document that is needed for people to claim social benefits in Ireland.
71. THAT in June 2020, the Special Rapporteur on Extreme Poverty and Human Rights wrote to the Irish government about the PSC. He argued that "I am concerned that this unwieldy process, spread out over more than two decades, and of the lack of flexibility and consultation that has been one of its hallmarks, is that low income individuals and otherwise marginalised communities, must now contend with formidable barriers to accessing their human right to social protection in Ireland." (**Exhibit TF8, Available from <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25176>**)

### **Examples where risk of exclusion mitigated**

72. THAT rather than accepting only a national ID card as proof of identity, a broader range of documentary evidence can be accepted, including other forms of state-issued ID, non-state ID from educational institutions, and letters and other documentation from central and local government, educational institutions, and the private sector. Crucially, a system of vouching is often a key way of reaching those who lack these documents, in which another trusted individual can vouch for the identity of someone that they know.

### **United Kingdom**

73. THAT the United Kingdom does not have a single National Identity Card or similar system. There was an attempt by government to introduce such a system in the mid-2000s, but in 2010 the biometric database was deleted and the project scrapped. In order to facilitate people accessing services online (a requirement for social protection), the government took a federated approach to identity, under the name Verify. Verify is underpinned by a set of Identity Assurance Principles. (**Exhibit TF11**).
74. THAT while not having a national ID card, the UK has two main forms of government-issued photo ID, the passport and the driving licence. However, it is clear that these alone

are not sufficient to allow everybody to prove their identity. The 2011 census revealed that 17% of the population of England and Wales did not have either a UK or a non-UK passport. Another possible form of identification is the driving license. According to the National Travel Survey, in 2020 80% of the population aged above 17 in England had a full driving licence. But within that there is a range: for example, 92% of men aged 50-59 have a full driving licence, whereas only 68% of women aged over 70 have the document.

75. THAT therefore relying only on these two forms of ID would exclude a significant number of people. An approach was taken that would allow a wider variety of ways in which people can assure their identity.
76. THAT crucial concept here is Levels of Assurance. This is the degree of confidence that the person is who they claim to be. Depending on what service the individual is looking to access, the required Level of Assurance can vary. To meet the required level of assurance of the individual's identity claim, the individual submits two or more pieces of identity evidence. The types of documents that constitute identity evidence is very broad. A full list is available in Appendix A of GPG 45. This is a broad range of potential pieces of identity evidence, from a variety of sources including local and national government, financial organisations, utility providers, and educational institutions. **(Exhibit TF5)**.
77. THAT the Verify system is to be replaced with two current government initiatives: a trust framework for businesses looking to verify identities, and a Single-Sign on for Government to verify the identity of those accessing government services. While still under development, I have been consulted on the developments in my role in PCAG and PIAF, and those building the systems are certainly avoiding the development of any centralised database and maintain the same ethos of inclusivity as present under Verify.

### Canada

78. THAT another example of alternative forms of ID being accepted in interactions with the government comes from Canada.
79. THAT in Canadian federal elections, voters at the polling station have to prove their identity and address. This can be through a government-issued ID document containing the voter's name, address and photograph; or through two additional methods. First, the voter can provide two pieces of evidence from a long list of sources that include various proofs of identity government, private sector, financial sector, utilities and educational institutions. Many of these do not have a photograph, but must include the voters' name. Finally, a vouching system is in place, where another person who knows the voter can vouch in writing for their identity. **(See exhibit TF6)**
80. THAT I now attach and mark the following documents that I refer to and rely on in my foregoing expert evidence:

TF1: Secretary General of the United Nations, *Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights*, Feb-Mar 2020

TF2: Chudnovsky, M and Peeters, R *A cascade of exclusion: administrative burdens and access to citizenship in the case of Argentina's National Identity Document 2021*

- TF3: Privacy International *Exclusion and identity: life without ID* 2018  
 TF4: ID4D, *Global ID Coverage, Barriers, and Use by the Numbers: Insights from the ID4D-Findex Survey*  
 TF5: GDS, *Good Practice Guide 45: Identity Proofing and Verification of an Individual* 2017  
 TF6: Elections Canada *ID to Vote*  
 TF7: Privacy International, *My ID, my identity? The impact of ID systems on transgender people in Argentina, France and the Philippines* 2021  
 TF8: The Special Rapporteur on extreme poverty and human rights, *Report on the Digital Welfare State*, 2019  
 TF9: World Bank, *Principles on Identification for Sustainable Development* 2021  
 TF10: UNDP, *Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes*, 2021  
 TF11: Whitley, E. *Trusted digital identity provision: GOV.UK Verify's federated approach* 2018

81. THAT I make this affidavit truthfully to provide the foregoing expert evidence in relation to the Petition by the Initiative for Social and Economic Rights and Unwanted Witness, and for no other or improper purpose.
82. THAT whatever I have stated herein is true to the best of my knowledge and belief.

SWORN at LONDON, ENGLAND this 14<sup>TH</sup> day of APRIL 2022.

by the said **Dr. Thomas Fisher**



DEPONENT

BEFORE ME



A NOTARY PUBLIC

Notary Public London, England (Katia E. Fallow)

**Drawn and Filed by:**

M/s ALP Advocates,  
 Lotis Towers, 5th Floor,  
 Plot 16 Mackinnon Road,  
 P.O Box 28611,  
 Kampala, Uganda.  
 Email: [Info@alp-ea.com](mailto:Info@alp-ea.com)



Human  
 Forty-  
 24 Feb  
 Agend  
 Annu  
 for H  
 High  
 Prom  
 politi  
 inclu

---

# Advance Edited Version

Distr.: General  
4 March 2020

Original: English

---

## Human Rights Council

### Forty-third session

24 February–20 March 2020

Agenda items 2 and 3

### Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General

Promotion and protection of all human rights, civil  
political, economic, social and cultural rights,  
including the right to development

## Question of the realization of economic, social and cultural rights in all countries: the role of new technologies for the realization of economic, social and cultural rights

### Report of the Secretary-General\*

#### *Summary*

The present report is submitted pursuant to Human Rights Council resolution 40/12, in which the Council requested the Secretary-General to prepare an annual report on the question of the realization in all countries of economic, social and cultural rights, with a special focus on the role of new technologies for the realization of economic, social and cultural rights.

In the report, the Secretary-General identifies the opportunities and potential held by new technologies for the realization of economic, social and cultural rights and other related human rights, and for the human rights-based implementation of the 2030 Agenda for Sustainable Development. He also identifies risks associated with technological changes in exacerbating gaps and inequalities, and highlights particular challenges that they pose for the realization of economic, social and cultural rights. He considers the value of the normative framework of human rights in terms of providing guidance for States and other stakeholders in harnessing new technologies and mitigating risks in a more effective and inclusive manner. The report concludes with recommendations for related action by Member States, private companies and other stakeholders.

---

\* The document was submitted late to the conference services without the explanation required under paragraph 8 of General Assembly resolution 53/208 B.

## I. Introduction

1. New technologies, including digital technologies, have enormous potential and profound implications for the realization of economic, social and cultural rights, as well as all other human rights, and for the transformative changes envisioned by the world leaders in the 2030 Agenda for Sustainable Development.<sup>1</sup> New technologies can rapidly expand the quality of and access to many essential services and products for the realization of economic, social and cultural rights. At the same time, they involve significant risks in potentially exacerbating existing gaps and inequalities and creating new ones. Furthermore, the benefits of new technologies are not currently distributed equally across and within countries. Some digital technologies often have unanticipated adverse consequences. Digital divides and technology gaps exist between and within countries, between men and women, between generations and across social groups. Many of these gaps correspond to differences in infrastructure, access and capacities, as well as to deeply entrenched discrimination and inequalities.

2. There is a significant risk that new technologies could further exacerbate and entrench existing inequality and patterns of discrimination, leaving those who do not have access to technologies even further behind. The people most heavily affected by these risks are likely to be at the margins of society. As stated by the Secretary-General's independent High-level Panel on Digital Cooperation, in its 2019 report, "[a]s any new technology is developed, we should ask how it might inadvertently create new ways of violating rights – especially of people who are already often marginalized or discriminated against".<sup>2</sup>

3. The focus of the present report, submitted pursuant to Human Rights Council resolution 40/12, is the role of new technologies for the realization of economic, social and cultural rights. In the report, the Secretary-General highlights the value of a human rights-based approach to harnessing the potential of new technologies while addressing potential risks, an approach that views people as individual holders of rights, empowers them and promotes a legal and institutional environment to enforce their rights and to seek redress for any human rights violations and abuses. The report concludes with recommendations to States and other stakeholders to guide them towards ensuring better human rights outcomes when designing, developing and deploying new technologies.

## II. Impact of new technologies on key economic, social and cultural rights

4. With its central commitment to leave no one behind, the 2030 Agenda has given important political impetus to the realization of economic, social and cultural rights and efforts to address inequality. If harnessed and distributed equitably, new technologies could greatly facilitate the realization of economic, social and cultural rights, and help ensure that their key elements of availability, affordability, accessibility and quality are achieved.

5. New technologies open opportunities for "leapfrogging" – bypassing intermediate stages of technology through which countries have historically passed during the

---

<sup>1</sup> There is no universally agreed definition of "new technologies", which are often interchangeably referred to as "frontier technologies" or "emerging technologies". The Organization for Economic Cooperation and Development (OECD) has mapped some of the most commonly identified new technologies into four quadrants that represent broad technological areas: digital technologies (such as artificial intelligence, big data analytics, the Internet of things, robotics and blockchain); biotechnologies (such as stem cell technology and health monitoring technology); advanced materials (such as nanomaterials); and energy and environment (such as drones, microsatellites, electric vehicles and biofuels) (see OECD, *OECD Science, Technology and Innovation Outlook 2016* (Paris, 2016)). Given the multitude of new technologies, the present report focuses on a selective set of digital and other new technologies that have significant relevance to economic, social and cultural rights.

<sup>2</sup> High-level Panel on Digital Cooperation, "The age of digital interdependence: report of the UN Secretary-General's High-level Panel on Digital Cooperation", June 2019, p. 17.



development process – which can accelerate the pace of the progressive realization of economic, social and cultural rights. For example, the availability of cheaper mobile communication technologies has enabled some developing countries, notably in Africa, to skip the development of analogue landline infrastructure and move directly to digital mobile telecommunications, enabling people living in rural areas to access a range of information and services.<sup>3</sup>

6. New technologies can also support States' efforts to promote the right to participation and access to information and to improve the efficiency and effectiveness of public decision-making, with a view to maximizing the use of available resources for the realization of economic, social and cultural rights. For example, during a typhoid outbreak in Uganda in 2015, the Ministry of Health used data visualization and interactive mapping techniques to support the early response to the disease outbreak. By providing the ability to explore real-time data at multiple levels of detail, authorities were able to plan resource allocation effectively, including for medical supplies, medical personnel and training.<sup>4</sup> In short, these technologies hold great potential for advancing the collective good of humanity.

7. At the same time, new technologies also pose significant risks, including with respect to the protection of human rights, that are often unintended by-products of scientific and technological advancement. Algorithms often reflect and reproduce existing biases. Social media can easily be misused to spread hatred. The collection and processing of a large amount of personal data without due consideration for the right to privacy has significant implications for the enjoyment of rights more generally.

8. Given the cross-cutting benefits and risks of new technologies for all human rights as highlighted above, the focus of the following sections is on the potential impact of new technologies on several key economic, social and cultural rights, as well as the potential of digital identification and financial technology for promoting greater inclusion.

## A. Right to education

9. Education is both a human right in itself and an indispensable means of realizing other human rights (E/C.12/1999/10, para. 1). Education is key for lifting people out of poverty, empowering women, safeguarding children and protecting the environment. Education and learning are critical in preparing countries and their people for changes resulting from the accelerated development and spread of technological innovations, in order to maximize their benefits while minimizing the potential risks.

10. New technologies have greatly expanded access to education and learning opportunities, making it easier for teachers to create instructional materials and enabling new ways for people to learn and work together. Online education materials and courses, digitized textbooks and e-learning modules are revolutionizing the provision of education, including for those with disabilities. Open online courses provide an alternative path to higher education. At the same time, this transformation is placing new demands on people in terms of the knowledge and skills that they need to acquire throughout their lives.

11. Advancement in new technologies brings challenges in terms of availability and accessibility of the right to education, particularly for poor and the most marginalized people. Access to educational content and opportunities disseminated by digital means requires physical infrastructure and economic means. People living in urban areas generally enjoy better and cheaper access to electricity, broadband Internet connection and economic means to acquire devices such as computers, tablets and smartphones, while those in remote rural areas are often relegated to using relatively outdated technologies.

<sup>3</sup> *Technology and Innovation Report 2018: Harnessing Frontier Technologies for Sustainable Development* (United Nations publication, Sales No. E.18.II.D.3), pp. 84–85.

<sup>4</sup> United Nations, Global Pulse, “Data visualisation and interactive mapping to support response to disease outbreak”, Global Pulse Project Series, No. 20, 2015.

12. New technologies also risk exacerbating gender and other disparities. According to the latest estimates, the digital gender gap is rapidly growing in developing countries, especially in the least developed countries.<sup>5</sup> Gender disparities in access to and use of information and communications technology often reflect the discrimination faced by women in society more broadly, and have the effect of further limiting access to technologies and the opportunities presented by them (A/HRC/35/9, para. 17). Similarly, children with disabilities face several barriers in taking advantage of information and communications technology to better access more educational opportunities, as technologies and contents may need to be adapted for their use (A/HRC/32/37, para. 42).

13. Ensuring the quality of the learning experience in online education is another challenge, as the driver of content dissemination can overwhelm the need for learner engagement and interaction. According to the Special Rapporteur on the right to education, qualifications and certificates obtained through open online courses often do not go through adequate assessment processes. Furthermore, as open online courses are often delivered by or in partnership with the private sector, it is incumbent upon Governments to put in place appropriate policies and regulations to fully ensure the acceptability, adaptability and quality of education in line with their obligations (for example, *ibid.*, sections VI and XII).

14. Technology-based education should preferably supplement, rather than replace, a full learning experience based on proven face-to-face teaching and interaction (*ibid.*, para. 58). There is a need to ensure that the overall education system fully respects the right to education and that education itself is directed to the full development of the human personality and the sense of its dignity.<sup>6</sup>

## **B. Right to food**

15. New technologies are having multiple and complex implications for various dimensions of food security and the right to food. For example, biotechnology and genetic engineering, as well as techniques for improving soil fertility, irrigation technologies and targeted use of agrochemicals, can increase the availability of food. Post-harvest and agroprocessing technologies can address food accessibility, and biofortification can improve the nutritional quality of food. At the same time, the potential safety and ethical implications of these new technologies, including synthetic biology, artificial intelligence and tissue engineering, will require close examination from a human rights perspective.<sup>7</sup>

16. Droughts increasingly threaten access to water for food production and exacerbate hunger. However, new technologies offer the means to predict and mitigate the potential adverse effects of drought on food production. In a joint initiative, the United Nations Children's Fund and the European Union supported the Government of Ethiopia in using satellite remote sensing to identify groundwater sources, with information relayed to communities and pastoralists in drought-affected areas, assisting them in digging more accurate boreholes. This has led to a 92-per-cent success rate in drilling new water sources, reducing cost and improving accessibility.<sup>8</sup>

17. Information and communications technology can play an important role in empowering farmers and rural entrepreneurs with access to information about agricultural innovations, weather conditions, financial services and market prices, and connecting them with buyers. Mobile phones also have great potential for empowering smallholders and

---

<sup>5</sup> International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2019* (Geneva, 2019), pp. 3–4.

<sup>6</sup> International Covenant on Economic, Social and Cultural Rights, art. 13.

<sup>7</sup> United Nations Conference on Trade and Development, *The Role of Science, Technology and Innovation in Ensuring Food Security by 2030* (Geneva, 2017), pp. 21–22.

<sup>8</sup> *Sustainable Development Outlook 2019: Gathering Storms and Silver Linings* (United Nations publication, Sales No. E.20.II.A.1), p. 94.

promoting inclusiveness in the market, enabling them to sell their perishable produce more effectively and negotiate better prices.<sup>9</sup>

18. At the same time, trends towards digitization, the financialization of the food market and the commodification of food, accelerated by technological advancement, are profoundly reshaping food systems and having a significant impact on the right to food. Technology is at the heart of the industrial food system, which focuses on maximizing efficiency in food production at the lowest possible cost and relies heavily on chemical inputs, affecting nutritional quality and public and environmental health (A/71/282, paras. 22–23). As seeds and other plant genetic materials are being digitized and patented by global corporations, risks emerge that access to traditional knowledge and seeds developed in other ways, including by indigenous peoples, may be undermined. Digitization of land registration and land-related data with blockchain technology can bring significant benefits in enhanced transparency, efficiency and security. However, new technologies need to be introduced with care in order to avoid unintended consequences, including easier transformation of land interests into speculative financial assets and risks of dispossession of, in particular, rural communities from long-held land.<sup>10</sup>

### C. Right to health

19. New technologies, including digital technologies, play an important role in the realization of the right to health and universal health coverage for all. Information and communications technology can expand the availability and accessibility of quality health services. For example, in Ghana, mobile phone-based health information technology has helped community health workers in rural areas to receive needed advice online and to track information about patients.<sup>11</sup>

20. Artificial intelligence and big data are being used to develop new medicines, provide personalized treatment plans and improve the efficiency of care delivery. When new technologies are designed and implemented in an accountable manner, they offer the potential to transform health services, expand access to preventive, diagnostic and treatment services, provide health education and expand knowledge and research.

21. Despite the potential benefits, new technologies such as digitization in health care are not always necessary or appropriate in all circumstances or for all people. As technologies affect different people in different ways, the design and application of new technologies will need to take into account the particular conditions and needs of the persons concerned and the context in which technology is to be deployed, so as not to undermine applicable rights and infringe upon the persons' dignity.

22. For example, new technologies, including assistive devices, built-in environmental applications and robotics, are gaining traction as cost-effective and efficient solutions to the increased need for individualized support and long-term care for older persons in many of the countries facing the most advanced population ageing. Effectively designed robots could support care delivery in a safer, more responsible way, relieving pressures from overworked care staff. This could contribute considerably to reducing abuse, violence and maltreatment of older persons in care settings. Interactions with robots, such as social companion robots, could potentially be beneficial for the physical and emotional well-being of older persons (A/HRC/36/48, paras. 73 and 82).

23. At the same time, overreliance on technology entails the risks of dehumanizing care practice. Technologies may undermine the autonomy and independence of older persons,

<sup>9</sup> Food and Agriculture Organization of the United Nations, *The Future of Food and Agriculture: Trends and Challenges* (Rome, 2017), p. 54.

<sup>10</sup> See Global Network for the Right to Food and Nutrition, *Right to Food and Nutrition Watch: When Food Becomes Immaterial: Confronting the Digital Age*, September 2018.

<sup>11</sup> See the conference report of the Integrated National Information and Communications Technology for Health and Development Forum, August 2016. Available at [http://1millionhealthworkers.org/files/2016/09/ICT\\_REPORT.pdf](http://1millionhealthworkers.org/files/2016/09/ICT_REPORT.pdf).

and create new forms of segregation and neglect, with older persons abandoned in their private homes or deprived of human interactions. Attention must be paid to ensure that technologies designed to assist older persons do not stigmatize them as frail and needy, which would have a disempowering effect on them and perpetuate dependency and indignity. Electronic surveillance and monitoring technologies could result in unwanted supervision that could even take place without an older person's consent or conscious knowledge (ibid., para. 52).

24. The use of big data and artificial intelligence in the health context poses significant risks to patients' right to privacy regarding sensitive health data and other personal information. With the growth of consumer health technologies such as wearable technology and smartphone applications, the creation, processing, exchange and sale of vast amounts of health data have increased worldwide (A/71/368, para. 13). This trend accompanies the increased risk of inadvertent disclosure of sensitive health-related patient data from health-care institutions, but also of unwarranted sharing with third parties. A further concern is the ability of artificial intelligence to infer and predict health conditions that individuals have not voluntarily disclosed, which may result in the denial of health insurance. Policy frameworks for the right to health need to protect the right to privacy and security in the use of digital health technologies such as biometric identification. Suitable regulation is also needed to ensure the quality and safety of software products, devices and applications that not only are used in primary health care, but also may be directly marketed or otherwise available to individuals.<sup>12</sup>

#### **D. Right to an adequate standard of living**

25. Over half of the world's population today lives in urban areas, a number expected to rise to 68 per cent by 2050.<sup>13</sup> Cities are often the centre of innovations and new technologies, as they host universities, research institutions and major technology industries. Increasingly, many cities are harnessing the power of new technologies to address the challenges posed by urbanization, to design and manage the complex interactions of energy, transport, water and waste, and to advance the goals of the New Urban Agenda and of Sustainable Development Goal 11 on making cities inclusive, safe, resilient and sustainable.

26. Effective and accountable use of information and communications technology and digital technologies can help urban planners and residents to enhance equitable access to urban services and opportunities. Conscious and targeted efforts and a broader participatory process are necessary to ensure that new technologies support the better realization of economic, social and cultural rights, such as the rights to housing, water and sanitation, for the most disadvantaged people. Without such efforts, there is a risk that efforts related to smart cities may not necessarily be focused on improving the quality of urban life for all and providing better access to quality services, particularly for poor and the disadvantaged people.

27. The wave of recent technological advances, such as the digitization of land and property data, cloud computing and the emergence of digital platforms, are contributing to a process of financialization of housing that is happening at a much faster pace and is deeper in scope than previously. The social and cultural value of housing may also be undermined by technologies enabling private actors to transform housing and real estate markets into financial instruments and a commodity of choice for investment. Digital platforms facilitating short-term rentals have contributed to driving up rent to a level that is no longer affordable for many residents in some locations.<sup>14</sup> Some governmental authorities have

---

<sup>12</sup> World Health Organization, "Digital technologies: shaping the future of primary health care", 2018, p. 6.

<sup>13</sup> *World Urbanization Prospects: The 2018 Revision* (United Nations publication, Sales No. E.20.II.A.1), p. xix.

<sup>14</sup> Desiree Fields and Dallas Rogers, "Towards a critical housing studies research agenda on platform real estate", *Housing, Theory and Society*, 2019, p. 4.

started to counter these trends by taxing real estate acquisitions by external investors or introducing regulations with stricter controls on short-term rentals, in order to protect access to adequate housing for their residents.<sup>15</sup> However, as technologies and the platform economy evolve at a rapid pace, they have tended to reinforce existing patterns of social and spatial segregation, exclusion and dispossession of housing and land. Regulatory frameworks seeking to counteract such effects remain piecemeal in the absence of a comprehensive approach fully taking human rights into account.

## E. Right to work

28. The global wave of technology changes is having a profound impact on the future of jobs, posing both opportunities and challenges for the realization of the right to work, including the right to the enjoyment of just and favourable conditions of work. Automation and new technologies are creating new job opportunities, while eliminating others. Robots and automation can reduce or eliminate hazardous tasks and contribute to the right to safe working conditions. At the same time, many workers who are at risk of losing their jobs to automation and robotization may be forced to accept lower-skilled and lower-paying jobs. The changing nature of jobs requires new skill sets, particularly digital skills: digital technologies are used in all types of jobs, including in sectors previously less associated with such technologies, such as agriculture, health and construction.<sup>16</sup> When it comes to the impact of such technological changes on different age groups, an emerging challenge is the need for adaptation and the retraining and relocation of adults, particularly older persons, affected by technological shifts. Women are also at the risk of losing out in the workplace because of the digital gender gap, in terms of skills, participation in digitization processes and representation in the workforce and corporate leadership (A/HRC/35/9, para. 25).

29. New technologies are also creating a growing diversity of employment forms, including work done outside of an employer's premises, often at home, which may widen access to employment and bring additional benefits in, for example, social and environmental spheres. However, while digital service platforms may create new work opportunities and help stabilize informal work arrangements, many workers in the gig economy face greater precarity in their work situation. Employment arrangements of this sort are often temporary in nature and involve multiple employers, impeding or restricting employees' practical ability to exercise their right to freedom of association, including the right to form and join trade unions, as most workers on online platforms do not know each other and their working patterns and conditions vary greatly.<sup>17</sup>

## F. Inclusion through digital technology

30. Many new technological solutions have the potential to enhance the inclusion of marginalized people in development processes, positively affecting various human rights. For example, providing the means for identification is an important way to empower people to participate in social, economic, political and public life. Conversely, not being able to prove one's identity can severely inhibit, and even effectively block, access to essential services, including housing, social security, banking, health care and telecommunications. Lack of proof of identity can lead to people being wrongly deemed not to have any citizenship, thus leading to statelessness. From the perspective of governmental functions, identity systems can be an important tool for Governments to avoid duplication and fraud and facilitate planning and accurate targeting of resources.

<sup>15</sup> For example, in British Columbia, Canada, the Miscellaneous Statutes (Housing Priority Initiatives) Amendment Act (2016) imposed 20-per-cent tax for foreign buyers of residential properties in selected geographic areas.

<sup>16</sup> See European Commission, *ICT for Work: Digital Skills in the Workplace* (Brussels, 2016).

<sup>17</sup> European Agency for Safety and Health at Work, *Protecting Workers in Online Platform Economy: An Overview of Regulatory and Policy Developments in the EU* (Luxembourg, 2017), pp. 15–16.

31. In recent years, many States and international organizations have moved towards adopting comprehensive digital identity systems. Often, new digitized identity systems are accompanied by legal obligations to enrol; in other cases, enrolment is made a requirement for accessing services, including public services, social security and food aid. The World Bank, with its Identification for Development campaign, and other organizations have launched broad programmes to promote access to identity documents, with a strong focus on digital technologies. Such initiatives are often designed as a response to the target 16.9 of the Sustainable Development Goals, under which States have committed to providing legal identity for all, including birth registration.

32. While implementing such systems may help tackle many challenges, it is important to carefully consider their potential and actual impact on the enjoyment of human rights, both positive and negative.

33. One major concern linked to comprehensive digital identification systems is that these systems can themselves be sources of exclusion, contrary to their purpose. Costly or difficult registration requirements, for example, may prevent poor and disadvantaged populations from fully participating in an identity system. Women in some regions face legal or customary barriers to obtaining official identification. A lack of Internet connectivity, needed for online authentication, also can contribute to exclusion. Older persons and members of some occupational groups performing mostly manual labour may have difficulties providing fingerprints that are clear enough for the purposes of the identify systems. Services that require authentication at the point of delivery create problems for older persons or persons with disabilities who may not be able to travel. Difficulties also arise when the name and gender in identity documentation are not properly reflected in the identity system, exposing people with non-binary gender identity to particular risks. Lastly, exclusion can also result from a particular group being given identity documents that are different from those of others.<sup>18</sup>

34. Comprehensive identity systems can also have a significant impact on the right to privacy, which in turn may lead to adverse impacts on a broad range of human rights and sustainable development. Digitized identity systems face great challenges regarding the security of the personal data collected, stored, shared and otherwise processed. Databases with information on millions of people are highly sensitive and attractive targets for attacks by criminal actors. Data breaches of any kind can facilitate identity theft, the consequences of which can be dire for the individuals concerned (A/HRC/39/29, para. 14). If the data collected contains biometric information, which is inseparably linked to a particular person and that person's life, the harms of data breaches can be irreparable.

35. When not properly designed, implemented and run, digitized identity systems tend to collect, analyse, share, merge and otherwise process more data than may be strictly necessary for legitimate system purposes. The accessibility of personal data to a range of government entities (and possibly other actors) may pose certain risks. Integrated identity management systems can facilitate access to personal information across the Government and enable the linking of individual records across disparate data registers, potentially facilitating tracking and monitoring of individuals without sufficient legal justification in violation of the rights to privacy and to freedom of association.

36. The Human Rights Council has called upon States to take appropriate measures to ensure that digital or biometric identity programmes are designed, implemented and operated with appropriate legal and technical safeguards in place and in full compliance with international human rights law (Council resolution 42/15, para. 6 (m)). The World Bank has provided guidance for designing digital identity systems and implementing the required technical, legal and institutional framework, the key principles of which include universal coverage and accessibility, robust and secure design that protects privacy, and

---

<sup>18</sup> See, for example, Alan Gelb and Anna Diofasi Metz, *Identification Revolution: Can Digital ID Be Harnessed for Development?*, (Washington, D.C., Center for Global Development, 2018, pp. 127–134.

strong governance, including a legal and regulatory framework, clear institutional mandates and accountability and independent oversight.<sup>19</sup>

37. Financial inclusion is another area in which new technological solutions, such as financial technology or fintech, hold great promise for the greater socioeconomic participation of people. The significant reduction in transaction costs and expanded access precipitated by new technologies, including mobile networks, has made financial services affordable and accessible for many that were previously priced out or considered not creditworthy. As highlighted by the High-level Panel on Digital Cooperation in its report, “many more people [have] the ability to save and transact securely without needing cash, insure against risks, borrow to grow their businesses and reach new markets”.<sup>20</sup>

38. Upon closer scrutiny, however, new opportunities for digital financial inclusion are also a source of considerable human rights risks. Mobile money has been widely lauded as bringing financial services to marginalized people and remote regions, and lending platforms are credited with bringing instant digital loans to similarly remote users. At the same time, many of the claimed benefits of these technologies have been disputed, as concerns have arisen that highlight the need for consumer protection and oversight, including overindebtedness and abusive contract enforcement.<sup>21</sup>

39. Across the world, new business models enable people with no credit history or physical collateral to demonstrate their creditworthiness, by, for example, allowing lenders to access and model social media profile and phone location data, as well as online transaction and payment histories. These are innovative approaches to modelling credit risk, but as with digital identification, there are important questions to be addressed concerning data privacy, user consent and knowledge regarding the collection and use of data, and the absence of legal and other safeguards.

### III. Human rights-based responses to new technologies

40. In order to fully reap the benefits of the technological progress under way while minimizing the potential for harm, the development and deployment of new technologies needs to be rooted in strong human rights foundations.<sup>22</sup> As agreed by States and monitored by national, regional and international mechanisms, international human rights law provides a key guiding framework for societies in shaping their responses to the challenges of an ever-changing technological environment. Human rights law sets out substantive and procedural rights, which, if violated, constitute harms that need to be prevented, mitigated or remedied. It imposes corresponding duties on States to respect, promote and protect human rights, and provides a framework for businesses to fulfil their responsibilities to do likewise.<sup>23</sup>

41. Both Governments and technology companies should ensure that the development and application of new technologies does not pose risks to the enjoyment of human rights. A human rights-based approach entails the application of a number of core principles, including equality and non-discrimination, participation, and accountability, which are also at the heart of the Sustainable Development Goals. In addition, new technologies raise the

<sup>19</sup> World Bank, “Principles on identification for sustainable development: towards the digital age”, February 2018.

<sup>20</sup> High-level Panel on Digital Cooperation, “The age of digital interdependence”, p. 9.

<sup>21</sup> See, for example, Center for Financial Inclusion, “Making digital credit truly responsible”, 25 September 2019.

<sup>22</sup> See Human Rights Council resolution 42/15, in which the Council recognized the need to apply international human rights law in the design, development, deployment, evaluation and regulation of individual profiling, automated decision-making and machine learning technologies, and acknowledged that international human rights law should be taken into account in the design, development and deployment of new and emerging technologies, such as artificial intelligence.

<sup>23</sup> Lorna McGregor, Daragh Murray and Vivian Ng, “International human rights law as a framework for algorithmic accountability”, *International & Comparative Law Quarterly*, vol. 68, No. 2 (April 2019), pp. 309–343.

importance of fully considering relevant rules concerning the legality, legitimacy, necessity and proportionality of restrictions on human rights. The following sections highlight examples in the application of these key principles.

## **A. Reinforcing equality and non-discrimination in new technologies**

### **Bridging the digital divide**

42. The need to bridge the digital divide, which hampers access to technologies and its benefits, is recognized in the 2030 Agenda (General Assembly resolution 70/1, para. 15) and in several resolutions of the Human Rights Council. In its resolution 38/7, for example, the Human Rights Council called upon all States to bridge the digital divides, including the gender digital divide, and to enhance the use of information and communications technology, in order to promote the full enjoyment of human rights for all.

43. Assessing and addressing the digital divide requires attention not only to physical access to technologies and devices, but also to the different types of technology, the quality of access and the distributional equity of access. For example, while developing countries are gaining cheaper access to mobile technologies and the use of mobile phones has spread rapidly in most parts of the world, technology gaps are widening with regard to more advanced areas of technology, such as bandwidth availability.<sup>24</sup> The gender digital divide also persists, reflecting existing patterns of gender inequality and discrimination. Disaggregated data is needed to analyse and monitor the differentiated impacts of technologies in order to ensure equality and non-discrimination.

### **Addressing bias in algorithms**

44. While many dimensions of economic, social and cultural rights are to be realized progressively, States have an immediate obligation to ensure equality and non-discrimination in law and practice. There is an urgent need to address the causes and impact of unintended bias and discrimination resulting from certain algorithmic and automated decision-making based on artificial intelligence and other technologies. Many algorithms tend to reinforce existing biases and prejudices, thereby exacerbating discrimination and social exclusion. Data-driven tools often encode human prejudice and biases, with a disproportionate impact on women and minority and vulnerable groups that are the subjects of those prejudices and biases.<sup>25</sup>

## **B. Legality, legitimacy, necessity and proportionality**

45. Unless carefully regulated, the use of new technologies, in particular digital technologies, can easily lead to inappropriate restrictions on human rights. For example, big data and artificial intelligence, as well as digital identity systems, frequently depend on the collection and processing of data, often including massive amounts of personal data. This may amount to violations and abuses of the right to privacy when undertaken without the informed free consent of affected persons. Other rights often affected by the deployment of new technologies relating to economic, social and cultural rights include the right to freedom of opinion and expression, the rights to freedom of association and of peaceful assembly, and the right to an effective remedy. Restrictions on these and other rights must conform to the principles of legality, legitimacy, necessity and proportionality.<sup>26</sup> Limitations on a right, where permissible, must be necessary for reaching a legitimate aim

<sup>24</sup> *Human Development Report 2019 – Beyond Income, Beyond Averages, Beyond Today: Inequalities in Human Development in the 21st Century* (United Nations publication, Sales No. E.20.III.B.1), p. 201.

<sup>25</sup> High-level Panel on Digital Cooperation, “The age of digital interdependence”, pp. 17–18; World Economic Forum, Global Future Council on Human Rights, “How to prevent discriminatory outcomes in machine learning”, white paper, March 2018.

<sup>26</sup> The Special Rapporteur on extreme poverty and human rights has pointed out that too many digital welfare state initiatives are characterized by a lack of attention to the importance of ensuring legality (A/74/493, para. 42).



and must be in proportion to that aim. According to the Human Rights Committee, restrictions must be the least intrusive option available,<sup>27</sup> and must not be applied or invoked in a manner that would impair the essence of a right.<sup>28</sup> They need to be prescribed by publicly available law that clearly specifies the circumstances under which a restriction may occur.<sup>29</sup>

46. In the light of the foregoing, an assessment of the necessity and proportionality of the implementation of a biometric identity system would consider the intrusiveness of taking biometric information, the heightened safety risks linked to biometric databases and the risks of abuse of such databases, such as for monitoring of political opponents or for other purposes beyond the scope and purposes of the original implementation. Based on this, the assessment would investigate whether the purposes of the biometric system justified the means sought to achieve them, and whether less intrusive ways for verifying people's identity could achieve those ends. Where biometric systems are deployed, less intrusive approaches should be made available to those who choose to opt out of such systems whenever feasible.

### C. Empowering rights holders

47. The development, diffusion and adoption of new technologies consistent with international obligations can be enhanced by effective and meaningful participation of rights holders. Towards that end, States should create opportunities for rights holders, particularly those most affected or likely to suffer adverse consequences, to effectively participate and contribute to the development process, and facilitate targeted adoption of new technologies. Through participation and inclusive consultation, States can determine what technologies would be most appropriate and effective as they pursue balanced and integrated sustainable development with economic efficiency, environmental sustainability, inclusion and equity.

48. Access to new technologies needs to be accompanied by measures to promote and protect economic, social and cultural rights, with a specific emphasis on poor and marginalized people to empower them and build their capacity to take full advantage of those technologies. Enhanced opportunities for jobs, access to education, health and other public services, infrastructure, and social protection systems are critical for such empowerment, as are adjustments to laws, policies and social norms that discriminate against poor people and other social groups. Investing in physical infrastructure such as computers, broadband networks and markets, strengthening endogenous capacities for innovation and adaptation of relevant technologies, and developing institutional and regulatory frameworks are essential to maximizing the sustainable development impact of new technologies (E/2018/50, p. 8).

49. Investing in the right to social protection in particular will be critical to ensuring that people can harness the benefits of economic and technological change, and mitigate the risks and uncertainties arising from it, in order to protect and fulfil their human rights. As noted, the absence of formal, standard employment relationships in the gig economy and elsewhere has contributed to considerable gaps in social protection coverage and adequacy. States need to protect the rights of workers in all forms of employment, particularly those engaged in digital labour platforms, to ensure their rights to equal pay and to freedom of association and collective bargaining.

<sup>27</sup> General comment No. 27 (1999) on freedom of movement, para. 14.

<sup>28</sup> General comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant, para. 6.

<sup>29</sup> General comments No. 27, paras. 11–13, and No. 16 (1988) on the right to privacy, paras. 3 and 8; A/HRC/39/29, para. 10; A/HRC/29/32, para. 33.

## D. Ensuring accountability

50. Accountability for human rights violations is central to the framework of international human rights obligations. This framework defines who is responsible for what and towards whom, and expresses the obligations assumed by States to take steps, individually and through international assistance and cooperation, especially economic and technical, to the maximum of available resources, with a view to achieving progressively the full realization of economic, social and cultural rights. It makes clear that certain obligations are of an immediate nature, notably to remove discriminatory laws, policies and other measures and to assure minimum essential levels of each right for all, with particular attention to those left furthest behind. The framework enables duty bearers to be held accountable to rights holders for their decisions or omissions, and provides mechanisms for claiming rights, monitoring progress transparently, sanctioning poor performance and seeking redress for human rights violations.

51. While new, data-driven technologies bring about new challenges in terms of ensuring human rights accountability, a variety of tools and safeguarding methodologies exist to identify and address risks and harms. Appropriate due diligence processes, taking into account the full range of rights under international human rights law throughout the life cycle of a technological system, can help avoid unduly narrow analysis of potential risks. Such processes can be helpful in identifying and preventing possible human rights harm, including by determining necessary safeguards, and in developing effective remedies when harm does occur. Meaningful consultations with external stakeholders and, where possible, with representatives of potentially impacted individuals and groups, in order to avoid project-driven bias, can strengthen such processes and significantly enhance their effectiveness (A/73/348, para. 54). On this basis, it would, for example, be recommended to integrate ongoing human rights diligence and broad consultations into the process of developing and deploying comprehensive nationwide digital identification systems, in order to enable the identification and mitigation of human rights risks associated with the systems.

52. Often, there may be significant gaps in public knowledge and understanding concerning the technological means being used by Governments and private actors in many public services, such as social security, pensions, health care, taxation, education or recruitment. This is a particular problem in the context of the automated decision-making processes that rely on artificial intelligence. Comprehensive, publicly available information is important to enable informed decision-making and the relevant consent of affected parties. It is advisable to require administrative services to systematically inform the addressees of rights-affecting decisions if those decisions have been made automatically or with the help of automation tools. For human rights-critical applications, the introduction of registers containing key information about those tools and their use can be considered. Regulations requiring companies to disclose when artificial intelligence systems are used in ways that affect the exercise of human rights and share the results of related human rights impact assessments may also be a helpful tool.

53. An associated dimension in the use of artificial intelligence technologies is “explainability”, concerned with the tendency towards opacity of complex algorithmic tools, also known as the “black box” problem. Such systems, in particular those with self-learning capabilities, can often behave in a fashion that is not entirely explainable or predictable. On occasion, intellectual property protections may, in this context, prevent necessary scrutiny of the algorithms and data used to train them. Even access to the underlying source code and training data, however, may often be insufficient to offer adequate understanding of how a particular artificial intelligence system operates in practice. Additional efforts are necessary to create tools and methods that provide a sufficient level of explanation of how decisions have been reached, in particular when artificial intelligence is determining critical issues within judicial processes or regarding access to, eligibility for and use of critical social services that are essential for the realization of economic, social and cultural rights.

54. In addition, regular audits by internal and external reviewers throughout the life cycle of artificial intelligence systems can provide a critical guarantee of rigour and independence

in transparency and, eventually, accountability (A/73/348, para. 55).<sup>30</sup> According to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, States should consider avoiding using systems that can have material adverse human rights impacts that cannot be subject to meaningful auditing (ibid.).<sup>31</sup>

55. While new technologies are largely driven by the private sector, States have legal obligations under human rights law to protect affected human rights, including through the adoption of necessary legislative measures. New technologies may require traditional approaches to regulation to be refined, in order to reflect the specificities of emerging technologies. Enhancing the capacity of sectoral oversight bodies to address relevant issues raised by the use of new technologies, such as sectoral regulation and oversight, could also help ensure on-target interventions in human rights-critical areas affected by the use of artificial intelligence (A/73/348, para. 42).<sup>32</sup>

## **E. Protecting the right to privacy in the context of personal data**

56. Many new technologies that hold promise in terms of promoting human well-being rely heavily on the processing of large amounts of personal data. In such an environment, ensuring an adequate level of data privacy is essential in order to prevent human rights violations and abuses, including economic, social and cultural rights.<sup>33</sup> Uninhibited access to health or genetic information, for example, could enable insurers to exclude from coverage those that need health care most urgently. The Human Rights Council has called upon States to develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful or arbitrary collection, processing, retention or use of personal data by individuals, Governments, business enterprises and private organizations (Council resolution 42/15, para. 6 (f)). According to the General Assembly, the adoption and implementation of data protection legislation, regulation and policies could include the establishment of national independent authorities with powers and resources to monitor data privacy practices and investigate violations and abuses, and to provide appropriate remedies (Assembly resolution 73/179, para. 6 (g)).

57. Many States, intergovernmental organizations and other institutions have developed standards for the protection of personal data that can guide the design of personal data governance frameworks and mechanisms.<sup>34</sup> Within the United Nations system, the guidelines for the regulation of computerized personal data files (E/CN.4/1990/72) adopted by the General Assembly in its resolution 45/95, and the personal data protection and privacy principles adopted in 2018 by the High-level Committee on Management, provide a benchmark for rights-respecting processing within the United Nations system. These guidelines and principles underscore a number of important principles, including that the processing of personal data requires an adequate level of transparency, requiring data subjects to be informed about the processing of their personal data and about how to request appropriate access, rectification and/or erasures of those personal data in the case of unlawful, unnecessary or inaccurate entries. Moreover, the processing of personal data should be based on the free and informed consent of the individuals concerned, or another legal basis. It should be relevant, limited and adequate to what is necessary in relation to a specified purpose. Appropriate security measures should be taken to protect personal information against unauthorized disclosure, modification or deletion.

<sup>30</sup> See also Human Rights Council resolution 42/15, para. 5.

<sup>31</sup> See also AI Now Institute, New York University, *AI Now Report 2018* (New York, 2018), recommendation 4.

<sup>32</sup> See also AI Now Institute, *AI Now Report 2018*, recommendation 1.

<sup>33</sup> See Human Rights Council resolution 42/15, in which the Council notes with concern that automatic processing of personal data for individual profiling may affect the enjoyment of human rights, including economic, social and cultural rights.

<sup>34</sup> For a list of relevant international instruments and guidelines, see A/HRC/39/29, para. 28.

## IV. Responsibilities of the private sector

58. The High-level Panel on Digital Cooperation points out in its report that “[t]here is now a critical need for clearer guidance about what should be expected on human rights from private companies as they develop and deploy digital technologies”.<sup>35</sup> The Guiding Principles on Business and Human Rights (A/HRC/17/31, annex), endorsed by the Human Rights Council in 2011, provide a comprehensive framework intended to guide efforts by a range of actors, including Governments and companies, to identify, prevent, mitigate and remedy human rights harm related to the activities of companies, including in relation to new technologies.

59. A central premise of the Guiding Principles is that companies should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. In the context of new technologies and their impact on economic, social and cultural rights, it can be particularly valuable to assess and address the risks of business models that involve, for example: (a) collecting large volumes of personal health data and using and sharing such data without consent; (b) using new technologies for public service delivery, in partnership with or on behalf of Governments, that could disproportionately put vulnerable populations at risks; (c) providing and using technologies and technology-driven processes such as algorithms that may result in harm to people and direct and indirect discrimination.

60. According to the Guiding Principles (*ibid.*, principle 17), companies should carry out human rights due diligence across their activities and business relationships to identify, prevent, mitigate and account for how they address the actual and potential adverse human rights impacts, and particular efforts should be made to address risks of further marginalizing and discriminating vulnerable populations and groups. The human rights due diligence requirement extends across a company’s operations, products and services, and applies to those related to the delivery of public services and goods, including in the areas critical for the realization of economic, social and cultural rights such as smart cities, health and education services. Furthermore, human rights due diligence should be embedded in company operations as an ongoing process, also integrating rights holder perspectives and experiences. If new digital technologies are to fulfil their potential while mitigating accompanying risks, companies should meaningfully engage civil society, rights holders and vulnerable populations in their due diligence.

61. In cases of business-related human rights harms, the Guiding Principles recall the duties of States and the responsibilities of business enterprises to ensure access to effective remedy (*ibid.*, chap. III). In the context of new technologies, as highlighted above, unique and complex issues will need to be addressed, such as guaranteeing remedy when abuses result from decisions made by machines and algorithms rather than humans; providing effective operational-level grievance mechanisms when there may be millions of adversely-affected rights holders; and safeguarding access to remedy when dozens of companies, rather than a single corporate actor, are linked to a human rights abuse through the interaction of different technology products and services.

## V. Conclusions and recommendations

**62. In the present report, a number of actions are identified that Member States and other stakeholders can take to harness the opportunities of new technologies for the realization of economic, social and cultural rights, while addressing potential risks. Among them, the following deserve particular attention of States and, as applicable, private companies and other stakeholders:**

(a) **Fully recognize the need to protect and reinforce all human rights in the development, use and governance of new technologies as their central objective, and ensure equal respect for and enforcement of all human rights online and offline;**

---

<sup>35</sup> High-level Panel on Digital Cooperation, “The age of digital interdependence”, p. 17.

- 
- (b) Reaffirm and fulfil the obligations of States to adopt legislative measures, including measures concerning private sector activities, so that new technologies contribute to the full enjoyment of human rights by all, including economic, social and cultural rights, and adverse impacts on human rights are prevented;
- (c) Accelerate efforts to bridge digital divides and technological gaps between and within countries, and promote an inclusive approach to improving accessibility, availability, affordability, adaptability and quality of new technologies;
- (d) Invest in the right to social protection to build resilience for changes and instability, including those caused by technological change, and protect labour rights in all forms of employment;
- (e) Significantly enhance efforts to disseminate information to the public about the use of new technologies, in particular of artificial intelligence, in the public sector;
- (f) Ensure participation of all relevant stakeholders in decisions on the development and deployment of new technologies, and require adequate explainability of artificial intelligence-supported decisions, in particular in the public sector;
- (g) Systematically carry out human rights due diligence during the entire life cycle of systems based on new technologies, in particular artificial intelligence systems, that can have a significant impact on the enjoyment of human rights;
- (h) Create adequate legal frameworks and mechanisms to ensure full accountability in the context of the use of new technologies, including by reviewing and assessing the gaps in national legal systems, creating oversight mechanisms, where necessary, and making available avenues for remedies for harm caused by new technologies;
- (i) Address discrimination and bias in the development and use of new technologies, particularly in terms of access to products and services that are essential for the enjoyment of economic, social and cultural rights;
- (j) Pay particular attention to the impact of new technologies on economic, social and cultural rights in reporting and review under the universal periodic review and the human rights treaty bodies.
-

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/348632126>

# A cascade of exclusion: administrative burdens and access to citizenship in the case of Argentina's National Identity Document

Article in *International Review of Administrative Sciences* · January 2021

DOI: 10.1177/0020852320984541

CITATIONS

2

READS

104

2 authors:



**Mariana Chudnovsky**

Centro de Investigacion y Docencia Economicas (CIDE)

33 PUBLICATIONS 136 CITATIONS

[SEE PROFILE](#)



**Rik Peeters**

Centro de Investigacion y Docencia Economicas (CIDE)

52 PUBLICATIONS 368 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



State Capacities [View project](#)



Institutions and Public Administration [View project](#)



# A cascade of exclusion: administrative burdens and access to citizenship in the case of Argentina's National Identity Document

International Review of Administrative  
Sciences

0(0) 1–18

© The Author(s) 2021

Article reuse guidelines:

[sagepub.com/journals-permissions](https://sagepub.com/journals-permissions)

DOI: 10.1177/0020852320984541

[journals.sagepub.com/home/ras](https://journals.sagepub.com/home/ras)**Mariana Chudnovsky** Centre for Research and Teaching in Economics (CIDE),  
Mexico**Rik Peeters** Centre for Research and Teaching in Economics (CIDE),  
Mexico

## Abstract

Administrative burdens can hinder people's social, political and economic participation. However, most empirical studies usually tackle the issue of how they affect access to citizenship merely indirectly. This article examines administrative exclusion from Argentina's National Identity Document and its effects on a key social policy: the Universal Child Allowance. Findings indicate that: (1) administrative exclusion from official identity documents 'feeds back' into the construction of a vulnerable target group that is systematically excluded from social benefits and public services; and (2) limitations in the administrative capacity for identity registration and documentation 'trickle down' to complications in the implementation of social policies as target groups remain 'off the radar'. Findings also demonstrate the importance of understanding administrative burdens as a systemic issue. Burdens manifest themselves at the level of citizen–state interactions but their causes and consequences are tied up with intractable institutional characteristics, administrative capacities and social inequalities.

---

## Corresponding author:

Rik Peeters, Centro de Investigación y Docencia Económicas (CIDE), División de Administración Pública  
Carretera México-Toluca, 3655 Colonia Lomas de Santa Fe, CP 01210, Alcaldía Cuajimalpa Ciudad de México,  
México.Email: [rik.peeters@cide.edu](mailto:rik.peeters@cide.edu)

### **Points for practitioners**

Efforts by developing countries to develop effective social protection systems are often thwarted by limitations in the state's capacity to identify and reach marginalized citizens. This suggests the need for a systemic perspective of the state's entire capacity instead of merely focusing on the design of social protection programmes. Specifically, we demonstrate that complete, accessible and up-to-date civil registries, identity documents and other forms of registration are a precondition for transforming formal rights into a tangible reality for citizens.

### **Keywords**

administrative burdens, administrative exclusion, citizenship, identity documents, social policy

### **Introduction**

The study of administrative burdens has, in recent years, demonstrated how bureaucratic barriers in citizen–state interactions can hinder people's access to rights, benefits and services (e.g. Heinrich, 2016; Herd and Moynihan, 2018). This is consistent with the approach's more fundamental claim that administrative burdens can affect people's social, political and economic participation (Moynihan and Herd, 2010). However, studies often only indirectly tackle the relation between administrative burdens and citizenship. Instead, scholarly attention has been 'most prominent at the intersection of public administration and social policy' (Moynihan et al., 2015: 47), such as social programmes (Barnes and Henly, 2018), health care (Moynihan et al., 2016) and welfare benefits (Brodkin and Majmundar, 2010).

A handful of recent publications on the role of administrative burdens in access to official identity documents and registration (Heinrich, 2018; Nisar, 2018; Peeters and Widlak, 2018) suggest two consequences of administrative burdens that analyses of more isolated case studies on social policies tend to overlook. First, administrative burdens can trigger 'policy feedback mechanisms' (Moynihan and Soss, 2014) that shape distinct social groups. Administrative burdens in obtaining official identity documents contribute to the construction of a social group that is systematically excluded from social benefits and public services for which official identification is an administrative requirement. Second, administrative burdens may be experienced at the street level but often have systemic causes (Peeters, 2020). For instance, limitations in the state's capacity to register and document identity 'trickle down' to complications in access to social rights.

In the following, we answer the question how administrative burdens can hinder access to official identity documents and how this, in turn, implies exclusion from citizenship rights. We do this by providing evidence that exclusion from an official



identity document triggers a ‘cascade of exclusion’, such as exclusion from social protection and benefits. We have selected the case of Argentina because it has an almost universal social protection policy – Universal Child Allowance (Asignación Universal por Hijo (AUH)) – with the lowest administrative burdens in Latin America. However, access depends on the administrative requirement of possessing Argentina’s only National Identity Document (Documento Nacional de Identidad (DNI)), the provision of which is the responsibility of a different agency that, in turn, exhibits low capacity to reach the poorest socio-economic strata. In sum, we show that administrative exclusion from the DNI jeopardizes access to Argentina’s largest social protection programme, especially for the most vulnerable target groups.

Hence, the analysis of the Argentinean DNI and AUH cases indicates that administrative burdens exist within a broader context of limited state capacity, administrative-political interests and social inequalities that determine the dynamics of state–citizen interactions (Peeters, 2020; Shamsul Haque and Puppim de Oliveira, 2020). Evidence also contributes to understanding why people in developing countries often face higher burdens in their interactions with the state (Heinrich, 2016; Peeters et al., 2018). The argument is structured as follows. First, we discuss the literature on administrative burdens, highlighting the approach’s relevance for the construction of citizenship. Second, we present the findings of the case study on administrative exclusion from the DNI. Third, we illustrate the consequences of exclusion from the DNI for citizens through the AUH case. Fourth and finally, the concluding section reflects on the importance of understanding administrative burdens as a systemic issue with profound effects on the construction of citizenship.

## **Administrative burdens and citizenship**

### *Administrative burdens*

The literature on administrative burdens has, in recent years, identified how bureaucratic barriers can complicate people’s access to services and benefits for citizens. Administrative burdens are defined as an ‘individual’s experience of policy implementation as onerous’ (Burden et al., 2012: 741). Burdens can lead to learning, compliance and psychological costs (Moynihan et al., 2015), or even to ‘administrative exclusion’ (Brodkin and Majmundar, 2010) from access to rights, services and benefits. Evidence indicates that their consequences extend beyond a material loss of time and money, and also impact people’s ability to participate socially and economically (Bruch et al., 2010). Moreover, burdens produce ‘feedback mechanisms’ (Moynihan and Soss, 2014), which can be understood as policy outcomes that shape subsequent political participation, attitudes and distribution of power in the form of people’s ‘orientations toward the institutions and policies of government’ (Mettler and Soss, 2004: 62) and the construction of social groups

that are structurally excluded from public services and social benefits (Heinrich, 2018).

Furthermore, administrative burdens are distributive. Vulnerable social groups tend to be ‘administratively disadvantaged’ (Brodkin and Majmundar, 2010: 828), leading to, for instance, low participation in and negative experiences of targeted social programmes (Barnes and Henly, 2018). Even though the jury is still out on what exactly explains this, there are strong indications that human capital, attitudes towards the state and decision-making mechanisms are crucial for understanding why some people are more affected by the same administrative burdens than others (Christensen et al., 2020; Chudnovsky and Peeters, 2020).

Finally, the literature highlights that administrative burdens are often constructed. Understood as a form of ‘hidden politics’ (Moynihan et al., 2015) or ‘policymaking by other means’ (Herd and Moynihan, 2018), burdens may be designed into bureaucratic procedures for political purposes of restricting access to public services and social benefits that are overly in demand or deemed politically undesirable (Soss et al., 2011). The construction of operational dysfunction is an attractive, low-profile and effective tactic that avoids complex policymaking or legislative procedures.

### *Administrative burdens as a systemic issue*

Without discrediting the merits of the research done so far, the three aforementioned claims are mostly based on empirical studies that emphasize individual cases over analysis of more systemic factors. First, while examining the consequences of administrative burdens for citizens is consistent with the approach’s more fundamental claim that administrative burdens are crucial for citizenship (Moynihan and Herd, 2010), most of the actual empirical work within the administrative burdens framework only indirectly touches upon these topics and has, instead, focused on access barriers in social policies (Moynihan et al., 2015: 47), such as social programmes (Herd, 2015), health care and insurance (Moynihan et al., 2016), and welfare benefits (Brodkin and Majmundar, 2010).

Second, the relatively few empirical studies on explaining ‘why some people find the same objective sets of rules or procedures more onerous or emotionally taxing than others’ (Christensen et al., 2020: 132), highlight factors that lie outside the control of individuals, such as age, mental and physical health, educational level, and poverty (Christensen et al., 2020; Chudnovsky and Peeters, 2020). This suggests the importance of more structural vulnerabilities and inequalities for the distributive nature of burdens. However, studies mostly focus on how these factors influence individuals’ human capital needed for navigating burdens.

Third, rather than the product of political or strategic behaviour, less-examined explanations show that burdens may also have unintentional origins (Peeters, 2020). Besides more down-to-earth explanations such as benign neglect (Moynihan and Herd, 2010: 664) and administrative errors (Widlak and Peeters, 2020), studies have indicated the importance of, among other things, an

organization's information architecture (Peeters and Widlak, 2018), administrative capacity (Tabor, 2002) and level of professionalization (Heinrich and Brill, 2015: 279–280). This suggests that administrative burdens are tied up with systemic and intractable institutional practices, characteristics and capacities.

While administrative burdens may manifest themselves at the most basic level of citizen–state interactions, their causes and consequences can only be properly understood if studied in relation to their broader social, political and administrative context, including issues such as citizenship, social inequalities and institutional design and capacity. Contributions at this more systemic level include, for example, grounding the administrative burdens approach in the policy feedback tradition (Moynihan and Herd, 2010). Negative bureaucratic experiences feed back into people's attitudes and expectations regarding the state (Moynihan and Soss, 2014), and send messages about their place in society (Auyero, 2011; Mettler and Soss, 2004), which, in turn, can make citizens wary of seeking access to services and benefits (Chudnovsky and Peeters, 2020). Another example is how state capacity and social inequality affect administrative burdens and exclusion in developing contexts (Heinrich and Brill, 2015). For instance, faced with large social inequalities and capacity restraints, governments in these contexts are often forced to focalize their social policies through means-tested targeting (Fiszbein and Schady, 2009). This not only contributes to errors of exclusion (Robles Aguilar, 2014), but also places administrative burdens on already vulnerable citizens by demanding additional information regarding income, family situation and identification.

### *Constructing citizenship*

Proof of identity, residence or citizenship is a fundamental access point to the state. For citizens, it is a key administrative requirement for access to rights, legal protection and most public services and benefits – including the social programmes, health care and welfare benefits that have been so widely studied in administrative burden research. For the state, an apparatus capable of proper registration and documentation – such as civil registries, fiscal numbers, birth certificates and family and income data – is a precondition for, among other things, taxation, criminal justice and determining eligibility for social benefits.

Relatively few scholars have studied systems of registration, identification and documentation from an administrative burden perspective. Three exceptions teach us important lessons that analyses of more isolated case studies on social policies tend to overlook. First, through a case study of the burdens that a marginalized social group in Pakistan faces in obtaining a legal identity document, Nisar (2018) argues that the growing importance of a legal ID in Pakistani society, which is increasingly required at security checkpoints, for job applications or to sell property, might reduce burdens for most citizens but places vulnerable groups at an even bigger distance from society. Second, Peeters and Widlak's (2018) study of the Dutch civil registry shows how the loss of residence status due to administrative

burdens triggers the loss of access to every benefit or service for which proof of legal residency is a precondition – ranging from health care insurance, to parking permits, state pension contributions and receiving voting ballots. Third, Heinrich (2018) shows how the burdens that Texas state authorities place on the acceptance of the consular identification document – often used by undocumented Mexican immigrants – not only complicate the legal status of the directly affected immigrants, but also have a profound impact on their children’s access to health care and schooling.

These studies suggest that, first, exclusion from access to citizenship – in the form of an official identity document or residence status – often implies exclusion from other benefits and services as well. Thereby, exclusion ‘feeds back’ (see Moynihan and Soss, 2014) into the construction of a social group that is systematically excluded from access to the state. Second, the implementation of social policies is complicated because of the state’s reduced ability to reach out to vulnerable groups living ‘off the radar’. In other words, limitations in the state’s capacity to register and document the identity of all its citizens ‘trickles down’ to policy inefficiency. In the following, a case study of administrative burdens in the application procedure for Argentina’s DNI is presented to better understand these feedback mechanisms and how these complicate the successful implementation of social policies targeted at vulnerable groups.

## **Research design**

### *Case selection*

Cases were selected for their theoretical utility. The study of the non-take-up of the DNI – Argentina’s main identity document for citizens and alien residents – was conducted to answer the question what role administrative burdens have in explaining people’s non-take-up of official identity documents. In order to illustrate the systemic consequences of administrative exclusion from this identity document, a case study was conducted of the non-take-up of the AUH – Argentina’s main social programme targeted at vulnerable groups. Argentina serves as a critical case because it has an almost universal social protection policy, with the lowest administrative burdens in Latin America (Chudnovksy and Peeters, 2020). If the expected effects of documentation problems are observed here, it can be assumed that the findings can be generalized to other social policies and other countries in the region (Miles et al., 2014: 32).

The DNI case allows for an analysis of the relation between administrative burdens and citizenship since it is Argentina’s universal access requirement for state benefits and services. Furthermore, it can be assumed that significant problems exist with DNI coverage – despite access to identity documents being a formal right under Argentinean law. According to the most recent available data, 168,000 persons in urban sectors, aged between 0 and 17 years and born in Argentina did not have a DNI in 2011 (Tuñón et al., 2012). The AUH case allows for a focus on

the consequences of exclusion from the DNI since this is one of the few administrative requirements for obtaining access to the benefit. Moreover, as the country's main social programme, the AUH case is illustrative of the consequences of exclusion from the DNI.

### *Data collection*

Data on population coverage and the formal procedure for obtaining and renewing the DNI were obtained through document analysis, three interviews with public officials and one expert interview with the Director of Argentina's main non-governmental organization (NGO) for the promotion of access to identity documents, the Instituto Abierto para el Desarrollo y Estudio de Políticas Públicas (IADEPP). Interviewees were selected because of their experience with and knowledge of the DNI application procedure. Data on the role of administrative burdens in this procedure come from 15 interviews with citizens that do not have the DNI, held in some of the most precarious settlements in Argentina.

Data for the AUH case were also obtained through document analysis and interviews. Data on the programme's coverage among the target population come from a study by Chudnovsky and Peeters (2020) of a 2015 government survey. Interviews were held with the aforementioned expert from the DNI case, with four officials from the National Social Security Administration (Administración Nacional de la Seguridad Social (ANSES)) – the organization responsible for eligibility registration – and with 11 citizens in the same precarious settlements as where the interviews for the DNI case were held. All interviewed citizens were eligible for the AUH but administratively excluded because they did not possess the DNI. They were asked about the consequences of not having access to the AUH, as well as their outlook on access to the state in general. The expert and ANSES officials were asked about registration and documentation as preconditions for policy success and about the social consequences of the non-take-up of the AUH.

Interviews were held between February and May 2019 and in January 2020. Interviews with civil servants were recorded and transcribed. For privacy and security reasons, no audio recordings could be made of the interviews with citizens. Instead, extensive field notes were made. Following the objective of the study, interviews with citizens were held in some of the country's most vulnerable communities in the Buenos Aires province. Due to practical access limitations, rural communities were not taken into account, even though large geographical distance to the state might cause additional administrative burdens. Interviewees were selected in the field through a snowball method. The sampling was theoretically driven (Miles et al., 2014: 33). The objective of the case studies is not to measure and explain non-coverage of DNI and AUH, but to demonstrate the role of administrative burdens in the construction of citizenship and to illustrate the systemic consequences of administrative exclusion from official identity documents. Accordingly, interviewees were selected up to the point of theoretical saturation

(Corbin and Strauss, 2008). More information on the data collection and the interviewee profiles is provided in a methodological appendix (available online at <https://journals.sagepub.com/doi/suppl/10.1177/0020852320984541>).

### *Data analysis*

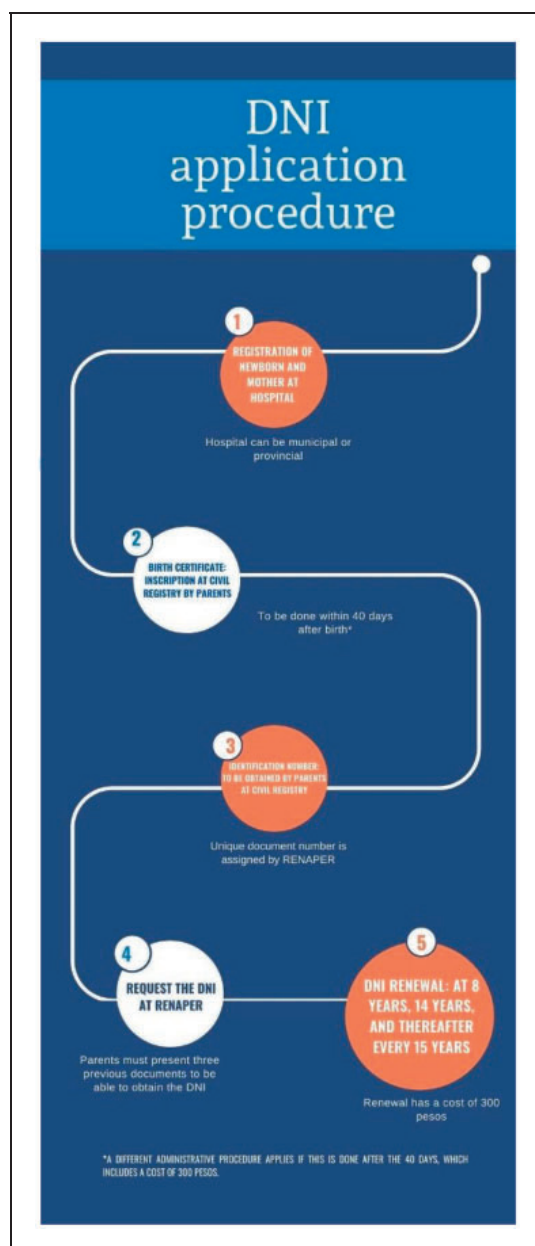
The research strategy followed here is ‘abductive’, which combines elements of induction and deduction (Mantere and Ketokivi, 2013). This strategy is useful for developing new hypotheses or theoretical explanations (Ashworth et al., 2018; Tavory and Timmermans, 2014). The interview data were collected with very limited theoretical preconceptions, whereas more explicit theoretical notions were used for the data analysis. Regarding the DNI interviews, ‘deductive coding’ (Miles et al., 2014: 81) of the field notes and transcripts followed the logic of finding evidence for the role of administrative burdens in the construction of citizenship. Data were analysed using codes derived from the administrative burdens framework developed by Moynihan and others (2015), which distinguishes between: (1) learning costs, that is, references to learning about the DNI, its administrative requirements and the application procedure; (2) psychological costs, that is, references to stress, stigmatization or loss of autonomy in the procedure for obtaining the DNI; and (3) compliance costs, that is, references to paperwork, waiting times, financial costs and other access requirements. For the AUH interviews, coding of the field notes and transcripts followed the logic of finding evidence for the systemic consequences of administrative exclusion from the DNI. The data were analysed using codes based on the two previously developed assumptions regarding the ‘trickle-down effects’ and ‘feedback mechanisms’. More information on the data analysis is provided in a methodological appendix (available online at <https://journals.sagepub.com/doi/suppl/10.1177/0020852320984541>).

## **DNI: administrative burdens in access to citizenship**

### *DNI coverage and formal procedure*

Argentina’s DNI can be obtained after birth and must be renewed at eight and 14 years of age, and thereafter every 15 years. It states a person’s name, sex, nationality, date of birth and unique document number, and includes a photograph, signature and fingerprint of the card holder. The DNI is issued by the National Registry of Persons (Registro Nacional de las Personas (RENAPER)), an agency of the Ministry of the Interior. The DNI is a requirement for access to a very broad range of services: from obtaining a credit card, to accessing social programmes, health care, education and voting. Figure 1 illustrates the basic steps needed to obtain the DNI.

Three documents are required to apply for the DNI (IADEPP, 2018; Poder Ciudadano, 2007): first, the registration of birth by the hospital in the corresponding municipality; second, the inscription of the birth certificate, including full



**Figure 1.** Steps to obtain the DNI.

name, place of birth and parent information, which is a provincial responsibility; and, third, the registration of the child's biometric data and the assignation of a unique and non-transferable number, which is a federal responsibility. The last two steps must be performed by the parents in the city where the child was born. Afterwards, citizens can obtain the DNI at the civil registry of each locality in the country, as well as in rapid documentation centres (RDCs) located in various shopping malls and airports. The first renewal at age eight costs 300 pesos and has the child's signature, photo and fingerprint.<sup>1</sup> The second renewal at age 14 involves

similar procedures and fees. In case of loss of the DNI, a replacement document costs 300 pesos. After four new copies of the document, the cost increases to 450 pesos.

Given that the first step is performed immediately after birth and the next two are not, almost all children in Argentina are registered but not necessarily inscribed and identified at a civil registry – a situation called ‘under registration’, which applies to around 7% of all children between 0 and 5 years old in Argentina (Harbitz et al., 2010; cf. Brito et al., 2013).<sup>2</sup> Argentinean provinces have a legal obligation to register births through civil registries at the local level but many have insufficient capacity to fulfil this responsibility (IADEPP, 2018). A child is considered a case of ‘under registration’ if registration at the civil registry is not completed within the child’s first year (IADEPP, 2018). If parents seek to obtain the DNI after this point, they must follow a different administrative procedure in a provincial registry, which involves a payment of 300 pesos, whereas the DNI is free of cost during the child’s first year. This procedure currently covers children up to 12 years old. After that age, a more complicated judicial process must be carried out to obtain the DNI.

Data regarding the population coverage of the DNI are scarce. The existing data, however, indicate a clear correlation between socio-economic vulnerability and non-coverage. In 2011, 168,000 persons in urban sectors, aged between 0 and 17 years and born in Argentina did not have the DNI, which is equivalent to 1.6% of that age range (Tuñón et al., 2012). Of this group, those living in the province of Buenos Aires, which surrounds the city and is one of the most vulnerable areas of the country, have a three times higher probability of being undocumented (1.8%) than those living in other cities of the country (0.6%) (Tuñón et al., 2012). This correlates with data on different socio-economic groups, which show that a child in the first socio-economic quartile has a 2.5 times higher probability of not having the DNI than their peers in the highest socio-economic quartile. The same pattern is observed when analysing household characteristics: the probability of not having the DNI is higher in single-parent households and in households with a larger number of children (Tuñón et al., 2012).

These results are confirmed by another study, which shows that 57% of all the people that have never had the DNI and/or birth certificate are from the very low social stratum and a further 26% from the low stratum (Calvelo et al., 2017: 6). Likewise, it is estimated that 73% of all people that at one point had the DNI before losing it (for instance, because they failed to renew it) belong to the very low stratum and 18.9% to the low stratum (Calvelo et al., 2017).

### *Citizen interviews: experience of administrative burdens*

Based on the typology by Moynihan and others (2015), Table 1 summarizes the costs of administrative burdens in the DNI procedure mentioned in the interviews with citizens.



**Table 1.** Administrative burdens in the DNI procedure mentioned by citizens.

Type of costs	Incidence (86 in 15 interviews)	Sample quote
Learning costs	19 (in 14/15 interviews)	'I had my baby at 15 and he didn't have documentation. Neither do I and I was a child too. They did not explain. ... At no point does anyone give you an explanation of how to do it as it was not considered a priority' (Brenda, 27)
Psychological costs	12 (in 6/15 interviews)	'I always had to carry tons of papers with me. I had about 10 papers of my son and I gave those papers to enrol him in school and they looked at me as if I were an irresponsible mother who never worried about getting her son's ID' (Karen, 26)
Compliance costs	55 (in 15/15 interviews)	'The truth is that because it is difficult to get a DNI, you have to get to know people who can help you... It is not a short process either, so you must have time and money to go' (Belén, 27)

*Learning costs.* Learning costs are observed in the form of misinformation about the costs of the DNI and a general lack of information about the application procedure. In the interviews, there is a repeated misunderstanding regarding the need to pay for the DNI. Formally, there are two ways of obtaining the first DNI: one is free (at the provincial civil registry and at RENAPER's central office); and the other – at the RDCs located in various shopping malls and airports – not only involves a payment, but also requires a bank card. Moreover, renewals involve a fee, whereas first-time application is free. This misunderstanding is further exacerbated by the well-intended RENAPER outreach programme of sending mobile offices (trucks) to disadvantaged neighbourhoods. Since these trucks are similar to the RDCs, obtaining the DNI here involves a payment with a debit or credit card. However, since they visit marginalized localities, these trucks have become the primary information point for citizens, which leads many to assume that obtaining the DNI always involves a payment. Furthermore, interviewees mention a lack of general information regarding the application procedure. Several of them believe that they will not be able to obtain the DNI without an intermediary or broker.

*Psychological costs.* Psychological costs emerge in the treatment of vulnerable citizens by street-level bureaucrats at provincial civil registries. Several interviewees mention bad manners, rudeness and unhelpfulness in their interactions with public officials. Moreover, officials sometimes do not have the correct information about their own procedures. Hence, even when citizens go to the civil registries,

their bureaucratic encounters may be far from helpful. Moreover, the bureaucratic encounters can lead to feelings of shame and inadequacy. This may also be the case for procedures that involve presenting an identity document, such as hospital admissions or school enrolment, where people are sometimes looked down upon for not having the DNI. The evidence coming from citizens is confirmed by the IADEPP director, who points out that public servants at civil registries are one of the least professionalized in the country: '[In the civil registries, there are] people who don't know how to provide an answer . . . and who mistreat you. . . . What capacity do the beneficiaries have, the problematic population, to understand?'

*Compliance costs.* Most commonly mentioned in the interviews are the various compliance costs designed into the procedure to obtain the DNI. First, parents must have the original birth certificate to obtain the DNI, as well as for its renewals. If they lose the birth certificate or simply do not have it, they must travel to the provincial civil registry where the birth was registered or should have been registered – even if this means going to the other end of the country. Second, financial costs are mentioned: parents must pay 300 pesos for the enrolment of their child after their first year, as well as for the two mandatory renewals. The only way to pay in cash in the case of late registration is at the RENAPER headquarters in the centre of the city of Buenos Aires, which is an obvious problem for the population living outside the capital and in marginalized communities.<sup>3</sup> Finally, several interviewees said that they feel 'played' when they tried to obtain their DNIs at the provincial civil registries. They are sometimes sent from one office to the other or are required to present additional information. These compliance costs are even higher for people who do not know how to read or write and receive very little assistance.

## **AUH: the consequences of exclusion from the DNI**

### *AUH coverage and formal procedure*

The AUH covers around 3.6 million children, representing 28% of the Argentinean population under the age of 18. It is a focalized cash transfer but does not depend on means-tested targeting. People qualify for the programme if they are not formally employed (with an income less than the minimum wage) and have children younger than 18 years old that reside in Argentina. Eligibility is determined automatically through government records and verified monthly by the ANSES. The programme has very few administrative entry requirements. As a result, it has a relatively high coverage: 18%, roughly 350,000 people, are identified as eligible but uncovered – a figure that rises to 20% for the section of the target group that lives in extreme poverty (Chudnovsky and Peeters, 2020). One of the few administrative requirements is that both parents and children must have the DNI. An analysis of non-participation in the AUH shows that, besides factors such as lack of time, interest and information, not having the DNI emerges as an

**Table 2.** Consequences of exclusion from the DNI.

Type of consequence of administrative exclusion	Incidence	Sample quotes
Feedback mechanisms	37 (in 15/16 interviews)	<p>‘[W]hen the procedures become very complex, [people] begin to live their lives without a DNI. Instead of going through all the steps of late registration, they rather decide not to do it at all’ (IADEPP director)</p> <p>‘[W]here there is one person [in a household] without documents, in general, there are several who do not have them’ (ANSES official)</p>
Trickle-down effects	28 (in 5/5 interviews) <sup>a</sup>	<p>‘ANSES has strong capacities, but everything else has to work to make ANSES effective’ (ANSES official)</p> <p>‘[T]he personnel [of the provincial agencies that do the registration by hand] is of very low qualification. It is one of the least qualified in public administration. . . . In general, they do not have a high-school requirement. . . . This leads to common problems, such as enrolling the name “Gómez” with an “s” instead of with a “z”, not to mention Eastern European surnames with a “v”, “s”, “k” or “y” (IADEPP director)</p>

Note: <sup>a</sup>No citizen interviews were included in the analysis of trickle-down effects.

important explanation for non-take-up, though exact figures about the number of people excluded for this specific reason are not available (Chudnovsky and Peeters, 2020).

### *Interviews: the consequences of administrative exclusion*

Using the hypotheses developed earlier, Table 2 summarizes the interview findings regarding the consequences of administrative exclusion from the DNI.

*Feedback mechanisms: life ‘off the grid’.* The consequences of problems regarding the DNI for citizens are severely felt by vulnerable population groups, according to the interviews with the expert and the civil servants. If they never had the DNI or at one point in life lost it, it is very common that they remain living ‘off the grid’. Late registration is perceived as costly and complicated. Moreover, lack of official identification tends to be ‘contagious’: it is not unusual to find an entire family line

(grandparents, parents and children) without the DNI. This is confirmed by the interviews with citizens. There is a large variety of reasons for not having the DNI – including losing papers after a divorce, teenagers running away from home, living as a homeless single mom and so on – but almost all interviewees mention that they have somehow learned to survive without an official ID. They are well aware, however, of the consequences this has. Besides not being able to get the AUH benefit, interviewees also mention complications in access to school or health care for their children. This points to a systematic exclusion and marginalization of the most vulnerable population.

*Trickle-down mechanisms: administrative capacity and policy inefficiency.* According to the interviews with civil servants, limited administrative capacity regarding the DNI indirectly affects the policy efficiency of the AUH. The people at ANSES are aware that the success of the AUH also depends on other elements of the Argentinean state apparatus. In this context, capacity issues in the administration of the DNI are mentioned as a main concern. For instance, a lack of coordination between the information gathered in local hospitals, on the one hand, and provincial civil registries, on the other, complicates the reliability and completeness of civil registration. Capacity issues also emerge at the street level, where enrolment in the AUH is delayed because of limitations in access to the DNI system and a lack of computers to process enrolment, which also causes waiting times for citizens. In short, findings indicate that limitations in the administrative capacity to provide official identity documents trickle down to problems in the implementation of social policies.

## Conclusion

A legal ID is the gateway to many public services, rights and benefits. Interestingly, the study of administrative burdens has paid little attention to barriers that citizens face in obtaining an identity document. Despite the approach's claim that burdens are crucial for citizenship (Moynihan and Herd, 2010), scholarly attention has been 'most prominent at the intersection of public administration and social policy' (Moynihan et al., 2015: 47), such as social programmes (Barnes and Henly, 2018), health care and insurance (Moynihan et al., 2016), and welfare benefits (Brodkin and Majmundar, 2010). Following the few studies that do study administrative burdens in access to official identity documents and registration (Heinrich, 2018; Nisar, 2018; Peeters and Widlak, 2018), our case studies of administrative exclusion from Argentina's DNI and from its most important social programme (AUH) presented evidence of: (1) a 'cascade of exclusion' from a broad range of social benefits and public services for which documentation and registration are administrative requirements (an exclusion that, moreover, tends to be 'passed on' by parents to their children); and (2) a 'trickle-down effect' of limitations in the registration and documentation of citizens into the implementation of social policies, which is jeopardized if vulnerable target groups live 'off the radar'.

These findings contribute to a fuller understanding of the role that administrative burdens play in constructing citizenship. Furthermore, the study highlights the importance of analysing administrative burdens as a systemic issue. Burdens are not only policy-specific: while administrative burdens manifest themselves at the basic level of citizen–state interactions, their causes and consequences can only be properly understood if studied in relation to their broader social and administrative context. As the Argentinean case indicates, a context of social inequality and limited administrative capacities may simultaneously increase administrative burdens in access to the state and reduce people’s capacity to overcome them.

The findings presented here have several shortcomings that are mostly a result of the relatively limited number of observations (Onwuegbuzie and Leech, 2007: 235–236): first, the AUH case illustrates only a fraction of the consequences of exclusion from the DNI; second, the effects of administrative exclusion from the DNI on policy efficiency and social marginalization are not directly measured; and, third, the collected data allow for theorizing but are limited in terms of their capacity to test causal inferences. In order to control for the validity of our findings, theoretical sampling, the use of multiple data sources and the description of an ‘audit trail’ (see the online appendix, available at <https://journals.sagepub.com/doi/suppl/10.1177/0020852320984541>) were used (Onwuegbuzie and Leech, 2007: 235–236). However, future studies can more systematically study the consequences of exclusion from official documentation and registration, and expand the observations to representative population samples and varying population groups (including rural communities), in order to measure the effects of exclusion on social inequality and policy implementation. In terms of practical relevance, our findings indicate the importance of complete, accessible and up-to-date civil registries, official identity documents and other forms of registration as a precondition for transforming formal rights into a tangible reality for citizens. This is especially the case for developing countries, where efforts to include vulnerable citizens in social protection systems are often thwarted by limitations in the state’s capacity to identify and reach the ones that need protection the most.

### **Acknowledgement**

We would like to thank Sergio Campos for his support in preparing the final version of this article.

### **Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

### **Funding**

The author(s) received no financial support for the research, authorship, and/or publication of this article.

### **ORCID iDs**

Mariana Chudnovsky  <https://orcid.org/0000-0002-3966-4731>

Rik Peeters  <https://orcid.org/0000-0002-9013-6192>

## Notes

1. For comparison, Argentina's minimum wage is 12,000 pesos. Procedures made in shopping centres and airports involve an additional fee of 50 pesos.
2. This is a common issue in Latin America and the Caribbean, for which two principal causes can be identified: first, the outdated legal frameworks in many countries, which call for civil registration to be carried out on paper and through a 'two-book' system (one for birth registration and one for identification); and, second, agencies' lack of adequate resources, both human and financial, to administer all citizens into their systems (Harbitz, 2013).
3. An express procedure to obtain the DNI can only be done online, for a cost of 1500 pesos, to be paid by credit or debit card.

## Supplemental material

Supplemental material for this article is available online.

## References

- Ashworth RE, McDermott AM and Currie G (2018) Theorizing from qualitative research in public administration: Plurality through a combination of rigor and richness. *Journal of Public Administration Research and Theory* 19(2): 318–333.
- Auyero J (2011) Patients of the state: An ethnographic account of poor people's waiting time. *Latin American Research Review* 46(1): 5–29.
- Barnes C and Henly J (2018) 'They are underpaid and understaffed': How clients interpret encounters with street-level bureaucrats. *Journal of Public Administration Research and Theory* 28(2): 165–181.
- Brito S, Corbacho A and Osorio Rivas R (2013) Birth registration: The key to social inclusion in Latin America and the Caribbean (no. IDB-MG-145). Available at: <https://publications.iadb.org/en/publication/10898/birth-registration-key-social-inclusion-latin-america-and-caribbean> (accessed 12 November 2019).
- Brodkin EZ and Majmundar M (2010) Administrative exclusion: Organizations and the hidden costs of welfare claiming. *Journal of Public Administration Research and Theory* 20(4): 827–848.
- Bruch S, Marx-Ferree M and Soss J (2010) From policy to polity: Democracy, paternalism, and the incorporation of disadvantaged citizens. *American Sociological Review* 75(2): 205–226.
- Burden BC, Canon DT, Mayer KR, et al. (2012) The effect of administrative burden on bureaucratic perception of policies: Evidence from election administration. *Public Administration Review* 72(5): 741–751.
- Calvelo L, Poy S and Tuñón I (2017) Aproximación a la medición del cumplimiento del derecho a la identidad en Argentina. Paper presented at the International Conference on Population of the Southern Cone, Santa Fe, AR.
- Christensen J, Aarøe L, Baekgaard M, et al. (2020) Human capital and administrative burden: The role of cognitive resources in citizen–state interactions. *Public Administration Review* 80(1): 127–136.
- Chudnovksy M and Peeters R (2020) The unequal distribution of administrative burden: A framework and an illustrative case study for understanding variation in people's experience of burdens. *Social Policy & Administration*. Epub ahead of print 7 August 2020. DOI: 10.1111/spol.12639.

- Corbin J and Strauss A (2008) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: SAGE.
- Fiszbein A and Schady N (2009) Conditional cash transfers: Reducing present and future poverty (no. 47603). Available at: <http://documents.worldbank.org/curated/en/914561468314712643/Conditional-cash-transfers-reducing-present-and-future-poverty> (accessed 12 November 2019).
- Harbitz M (2013) Mia Harbitz, Senior expert in public registries, Inter-American Development Bank. *iD People*. Available at: <http://www.id-world-magazine.com/id-people/?p=138> (accessed 12 November 2019).
- Harbitz ME, Benítez Molina JC and Arcos Axt I (2010) Inventario de los registros civiles e identificación de América Latina y el Caribe. Available at: <https://publications.iadb.org/es/inventario-de-los-registros-civiles-e-identificacion-de-america-latina-y-el-caribe> (accessed 12 November 2019).
- Heinrich CJ (2016) The bite of administrative burden: A theoretical and empirical investigation. *Journal of Public Administration Research and Theory* 26(3): 403–420.
- Heinrich CJ (2018) ‘A thousand petty fortresses’: Administrative burden in U.S. immigration policies and its consequences. *Journal of Policy Analysis and Management* 37(2): 211–239.
- Heinrich C and Brill R (2015) Stopped in the name of the law: Administrative burden and its implications for cash transfer program effectiveness. *World Development* 72(C): 277–295.
- Herd P (2015) How administrative burdens are preventing access to critical income supports for older adults: The case of the Supplemental Nutrition Assistance. *Public Policy & Aging Report* 25(2): 52–55.
- Herd P and Moynihan DP (2018) *Administrative Burden: Policymaking by Other Means*. New York, NY: Russell Sage Foundation.
- IADEPP (Instituto Abierto para el Desarrollo y Estudio de Políticas Públicas) (2018) Derecho a la identidad jurídica: Estrategias de abordaje para su efectivización. Available at: [http://iadepp.org/wp-content/uploads/2018/11/cuadernillo\\_tapa\\_color.pdf](http://iadepp.org/wp-content/uploads/2018/11/cuadernillo_tapa_color.pdf) (accessed 12 November 2019).
- Mantere S and Ketokivi M (2013) Reasoning in organization science. *Academy of Management Review* 38(1): 70–89.
- Mettler S and Soss J (2004) The consequences of public policy for democratic citizenship: Bridging policy studies and mass politics. *Perspectives on Politics* 2(1): 55–73.
- Miles MB, Huberman AM and Saldaña J (2014) *Qualitative Data Analysis: A Methods Sourcebook*. Thousand Oaks, CA: SAGE.
- Moynihan DP and Herd P (2010) Red tape and democracy: How rules affect citizenship rights. *The American Review of Public Administration* 40(6): 654–670.
- Moynihan DP and Soss J (2014) Policy feedback and the politics of administration. *Public Administration Review* 74(3): 320–332.
- Moynihan DP, Herd P and Harvey H (2015) Administrative burden: Learning, psychological, and compliance costs in citizen–state interactions. *Journal of Public Administration Research and Theory* 25(1): 43–69.
- Moynihan DP, Herd P and Ribgy E (2016) Policymaking by other means: Do states use administrative barriers to limit access to Medicaid? *Administration & Society* 48(4): 497–524.
- Nisar MA (2018) Children of a lesser god: Administrative burden and social equity in citizen–state interactions. *Journal of Public Administration Research and Theory* 28(1): 104–119.

- Onwuegbuzie AJ and Leech NL (2007) Validity and qualitative research: An oxymoron? *Quality & Quantity* 41: 233–249.
- Peeters R (2020) The political economy of administrative burdens: A theoretical framework for analyzing the organizational origins of administrative burdens. *Administration & Society* 52(4): 566–592.
- Peeters R and Widlak A (2018) The digital cage: Administrative exclusion through information architecture – The case of the Dutch civil registry’s master data management system. *Government Information Quarterly* 35(2): 175–183.
- Peeters R, Trujillo Jiménez H, O’Connor E, et al. (2018) Low-trust bureaucracy: Understanding the Mexican bureaucratic experience. *Public Administration & Development* 38(2): 65–74.
- Poder Ciudadano (2007) Acceso al Documento Nacional de Identidad y Derechos básicos en la Ciudad Autónoma de Buenos Aires y Provincia de Buenos Aires. Available at: [http://www.poderciudadano.org/up\\_downloads/temas/96\\_1.pdf?PHPSESSID](http://www.poderciudadano.org/up_downloads/temas/96_1.pdf?PHPSESSID) (accessed 4 October 2020).
- Robles Aguilar G (2014) *Targeting Efficiency and Take-Up of Oportunidades, a Conditional Cash Transfer, in Urban Mexico in 2008 (Dissertation)*. Oxford: Oxford University Press.
- Shamsul Haque M and Puppim de Oliveira JA (2020) Building administrative capacity under developmental states in Chile and Singapore: A comparative perspective. *International Review of Administrative Sciences*. Epub ahead of print 20 August 2020. DOI: 10.1177/0020852320943656 .
- Soss J, Fording RC and Schram SF (2011) *Disciplining the Poor: Neoliberal Paternalism and the Persistent Power of Race*. Chicago, IL: University of Chicago Press.
- Tabor S (2002) *Assisting the Poor with Cash: Design and Implementation of Social Transfer Programs*. Social Protection Discussion Paper no. 0223. Washington, DC: World Bank.
- Tavory I and Timmermans S (2014) *Abductive Analysis. Theorizing Qualitative Research*. Chicago, IL: University of Chicago Press.
- Tuñón I, Fourcade H, González MS, et al. (2012) Los indocumentados en Argentina. La cara invisible de la pobreza. Available at: <http://bibliotecadigital.uca.edu.ar/repositorio/investigacion/indocumentados-argentina-cara-invisible.pdf> (accessed 12 November 2019).
- Widlak A and Peeters R (2020) Administrative errors and the burden of correction and consequence: How information technology exacerbates the consequences of bureaucratic mistakes for citizens. *International Journal of Electronic Governance* 12(1): 40–56.

**Dr Mariana Chudnovsky** is a research professor of public administration at the Centre for Research and Teaching in Economics (CIDE), Mexico. Her research focuses on state capacities, civil services, administrative burdens, and social and health policies in Latin America from a comparative perspective. ORCID iD: <https://orcid.org/0000-0002-3966-4731>

**Dr Rik Peeters** is a research professor of public administration at the Centre for Research and Teaching in Economics (CIDE), Mexico. His main areas of expertise are street-level bureaucracy, administrative burdens, and state–citizen interactions, with a special emphasis on developmental and low-trust contexts. ORCID iD: <https://orcid.org/0000-0002-9013-6192>





SEARCH

## Exclusion and identity: life without ID

**CONTENT TYPE**

Long Read

**POST DATE**

14th December 2018



Photo credit: **Francisco Javier Argel**

Questions of **identification and ID**, with their associated privacy risks, are only increasing. There are multiple dimensions to understanding the impact of ID and identification; a key one is to understand how it can exclude. This is why Privacy International is conducting research to explore this important and underreported aspect.

Read our case studies: **Carolina analliana**.

In the identity discourse, identity is often closely linked to themes of "inclusion". For example, the **World Bank** gives one of the purported goals of ID systems as "Inclusion and access to essential services such as health care and education, electoral rights, financial services, and social safety net programs".

But the importance placed on 'inclusion' means that the concept needs to be interrogated. Does ID genuinely lead to further inclusion, and become a genuine reason

for people to be able to exercise their rights? Does it really serve to enable the access that proponents claim?

The challenge is, these claims about identity are based on assumptions about both the **nature of identity**, and crucially, what can be achieved with the implementation of identity systems. When it comes to understanding inclusion and exclusion, at the centre of this is a myth: that an identity system can be universal.

State-led identification schemes usually have some kind of claim to universality, and that they will cover the entire population (which could be the population of citizens, or that of residents). This idea that identity can be universally implemented is not reflected in the reality of identity systems. We see a **myriad of ways** in which people either cannot access ID, or use the ID that they have.

So, if we reject the idea that any identification system will be universal, either in its registration or use, then we have to begin to question the concept of identity being inclusive. Rather, it risks becoming something different: a way of placing artificial barriers in the way of people accessing their rights.

In certain contexts, the issue is that some people are compelled to have ID cards, whereas other – often more privileged – members of society are not. This can be ID that is specific to a particular group: for example, in the UK, non-EU residents are required to have a **Biometric Residence Permit**. Or it can be that the circumstances mean that a particular scheme, even if voluntary for other members of society, is effectively mandatory for a particular group, for example, in situations where an ID card is required to claim state benefits. This makes these particular groups more at risk of being tracked or profiled.

### *Identity and exclusion*

Identity documents and cards can be sources of exclusion in different ways. Hurdles to access and use ID can occur at different stages of the process, from enrolment and registration through to authentication and verification. It can range from people not having an ID card at all, to issues with using the ID.

Some of these problems are the result of direct government policy or action. One way of doing this is a situation where a particular group has a different identity document from others. A number of countries make use of identity documents for non-citizens that are in some way different from that of citizens: for example, being a different colour, marked with a word like foreigner or having an **identity number that is in a different range**. In some cases, this can be a powerful way of denying citizenship to some groups.

Take the case of the **Rohingya in Myanmar**. The government attempted to force Rohingya to be issued with identity documents that did not mention their religion or ethnicity (Myanmar citizenship being ethnically-based), a step that the Rohingya feared was a prelude to denying them citizenship. In **Kenya** in 1989, people of Somali descent – often excluded, and whose citizenship is questioned – were issued with a pink identity document with the express goal of making them more identifiable to the security services. They also face additional hurdles to being recognised as Kenyan citizens.

But there are other hurdles that exist when it comes to ID – **bureaucratic issues**, for instance, can make it hard to get ID or to use it. It is important to remember that even technical or bureaucratic failings reflect other aspects of exclusion in society. Let us consider the Aadhaar biometric system in India. There were **reports of people starving to death** because their fingerprints were not recognised when they were claiming the food rations to which they were entitled. This is because the elderly and manual workers like farmers have fingerprints that fade over time. Thus, the biometric failings reflect the exclusion of these groups in society.

Another group of people who can have difficulty with identification documents is trans people. When an individual's name and gender does not match **what is printed on their legal identity documents**, it can make those documents unusable. And so it becomes increasingly hard for them to **live their everyday lives**.

### *Amounting crisis*

Not having an ID – or having one that is unusable – can make life very difficult. Accessing financial services, government services and benefits can become hard or impossible. The challenge is that we are seeing more and more things that require ID to use. Education, health, getting a bank account – these are some other things that **increasingly need ID to access**. Thus, not having an ID can – in some countries – form a massive barrier for individuals.

An example of this is in Chile, the subject of several case studies published by Privacy International. The Chilean ID system has its **origins in the 1930s**. A 9-digit number is issued as part of the birth registration process – the RUN (Rol Único Nacional – Unique National Number). This is the number that is featured on Chilean ID cards. However, this is more commonly known as the “RUT” (Rol Único Tributario – Unique Tax Number) – a Chilean individual's RUT is identical to their RUN.

It is the RUT that has become ubiquitous in Chile, the idea that this is to be given during

transactions. Having a RUT number is necessary for activities from opening a bank account to getting health insurance. It's also necessary for the signing of most legal contracts, including employment, housing, and marriage.

RUT is also widely used in the private sector. It is still demanded by companies even when it is not a legal requirement. For example, it is usual for shoppers at supermarkets to be asked for their RUT number at checkout. Supermarket loyalty card schemes are linked to the RUT. Shockingly, so too are the loyalty schemes at pharmacies. Thus, the shopping and health data of millions of Chileans is all linked back to the individual. One of Privacy International's partners in Chile, Datos Protegidos, has been conducting a **campaign on this issue**.

The impact and potential for data exploitation of the RUT in the private sector are huge. The **"invisible manipulation"** that this can bring is massive. But there is another aspect to this: the use of the RUT in the private sector is also part of its normalisation in Chilean society. It is both a product and a cause of the ubiquity of the RUT in Chilean society.

Thus, the social aspect of having an ID with the spread and reach of the Chilean system becomes important: it means that the card or ID number is asked for in more and more situations, from websites through to the doorman at an apartment building. There are even **software suites** available for the electronic reading and verification of IDs when entering a building.

The issue with this scope of ID provision becomes clear with the people who lack a RUT, and the resulting problems they face. As our case studies illustrate, the challenge of not having an ID is immense: the lack of access to essential services, plus the constant reminder of one's status as 'lesser'.

One of the key factors here is immigration. The region faces an **unprecedented challenge**; including the at least 2.3 million Venezuelans who have emigrated since 2014. This has put pressure on the migration systems of many countries in Latin America, including Chile. There are reports that things like getting ID cards are taking a lot longer. Challenges like this can affect the ID system – for example, by overburdening the immigration bureaucracy, preventing people from getting the documentation to which they are entitled. In Chile, this – combined with the ubiquity of the RUT – places immigrants in a devastating position.

### *Conclusion*

We must question ID requirements if we are to build an inclusive world that does not deny

anyone their entitlements. They can be denied access to government services, bank accounts, and more. Any ID has to come with the realisation that having such a requirement will exclude.

If we want inclusion, the best option is to not require ID at all. In other situations, it may be that the best option is to broaden the requirements to multiple sources of identity, rather than just linking it to a singular system.

Identity systems create their own reality, one in which identification is required. A consequence of this is the exclusion of people who either don't have or can't use their ID. Essentially, it creates an environment that is hostile to these groups.

**TAGS**

**OUR CAMPAIGN**

Demanding identity systems on our terms

**LEARN MORE**

ID Systems

Identity

**OUR FIGHT**

Safeguarding Peoples' Dignity

**LOCATION**

Global South

Chile

**RELATED CONTENT**



LONG READ

## Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba

In this article we provide background on the initial challenge of the Huduma Namba and subsequent developments which led to an important ruling of the High Court of Kenya on the retrospective effect of the Data Protection Act as we reflect on its wider implications for the governance and regulation of digital ID systems. **CONTINUE**

**READING**



## Afghanistan: What Now After Two Decades of Building Data-Intensive Systems?

Over the last 20 years, vast data-intensive systems were deployed in Afghanistan by national and foreign actors. As we highlight some of these systems we present our concerns as to what will happen to them.

**CONTINUE READING**

## Why we need to talk about digital health

In this piece we outline the main discussions and measures we need to see being systematically adopted to inform decision-making about digital solutions in the health sector, and provide examples of where these were not integrated in decision-making processes and with what consequences. **CONTINUE READING**



## IPANDETEC publish a report on the development of digital identities in Central America

This article was written by Abdías Zambrano, Public Policy Coordinator at IPANDETEC, and is adapted from a blog entry that originally appeared here. Digital identity can be described as our digital personal data footprint, ranging from banking information and statistics to images, news we appear in **CONTINUE READING**

**GET INVOLVED**

**ACT WITH US** ● **DONATE** ● **JOIN**

## NEWSLETTER

Click here to sign-up to our mailing-list!

---

## FOLLOW US

---

## NAVIGATION

**NEWS**

**ACT**

**CAMPAIGNS**

**LEARN**

**IMPACT**

**ABOUT**

**DONATE**

**HOW WE FIGHT**

**ABOUT**

**PRIVACY**

**RESOURCES**

## CONTACT US

62 Britton Street,  
London, EC1M 5UY  
UK

Charity Registration No: 1147471

[Click here to contact us.](#)

[Click here for media and press enquiries.](#)





# Global ID Coverage, Barriers, and Use by the Numbers: Insights from the ID4D-Findex Survey



Trusted and inclusive identification (ID) systems can serve as a powerful tool for development, accelerating progress in number of areas, such as **women's empowerment and gender equality, financial inclusion, and health**. Moreover, "legal identity for all, including birth registration" is one of the 169 targets of the Sustainable Development Goals (SDGs), and ID and civil registration systems are increasingly seen as critical for realizing the SDG's principle of 'leaving no one behind'.

Yet, many people worldwide are unable to prove their identity, and many ID systems lack the features and qualities that would enable them to deliver on their promise for development. To better understand the nature of the 'global identification challenge', the World Bank's **Identification for Development (ID4D)** initiative partnered with the **Global Findex** team to gather survey data across 97 countries about ID coverage, barriers to obtaining one, and their use (e.g. for accessing government or financial services). This is the first time nationally representative data have been collected for such a large number of countries, offering unique insights.

## KEY INSIGHTS

- **Close to 40% of adults in low-income countries (LICs) do not have an ID.**<sup>1</sup> Coverage gaps in middle-income countries (MICs) are significantly smaller.
- **Women and the poor are less likely to have an ID:** in surveyed LICs, 44% of women do not have an ID (vs. 28% of men) and 43% of the poorest 20% do not have an ID (vs. 25% of the richest 20%). Less-educated people, younger adults, people out of the workforce, and those living in rural areas, are also less likely to have an ID.
- **Many people without an ID find it too difficult to obtain one.** In countries with large ID coverage gaps (>20 percent), 1 in 3 adults without an ID find it "too difficult to apply"; not being able to provide supporting documents is also cited by many as a challenge.
- At the same time, **demand for a national ID or similar foundational credential depends on its perceived usefulness and the availability of alternative identity documents.**
- **People with an ID are more likely to own bank accounts and mobile phones,** and financial and mobile services are among the most frequently reported uses of one's ID.

## METHODOLOGY

For this note, we have analyzed survey data from 97 countries where respondents were asked:

- 1) whether they personally had the country's national ID or equivalent foundational identity credential;
- 2) for those without the ID, what their reasons were for not having one;
- 3) for those with the ID, whether they had used it for specific purposes.

The surveys were completed in 2017 and are nationally representative. Survey respondents are aged 15 and above; our analysis was further restricted to those respondents who are above the mandatory or minimum ID age (in countries with no mandatory age) of their country. The data collection methodology is described in detail on the **Global Findex website**. Estimates are weighted to be representative at the global, regional, and country level.

<sup>1</sup> Survey respondents were asked about a specific foundational ID, using local terminology to the extent possible (e.g. 'Kartu Tanda Penduduk' in Indonesia or 'Aadhaar' in India). Although birth certificates are foundational identity documents, survey responses are limited to credentials issued by national ID systems or equivalent ID systems and held by individuals aged 15 and above. The terms 'national ID', 'ID', and 'proof of identity' are used interchangeably in this note.

## WHO DOES—AND DOES NOT—HAVE AN ID?

The ID coverage gap is concentrated in LICs, where more than 1 in 3 adults do not have an ID (Figure 1).<sup>2</sup> From a regional perspective, Sub-Saharan Africa has the largest coverage gap with close to 30 percent of adults lacking an ID. Middle income countries are closer to the goal of providing a proof of identity for all adults, with over three-quarters of surveyed MICs having achieved coverage of 90 percent or above.

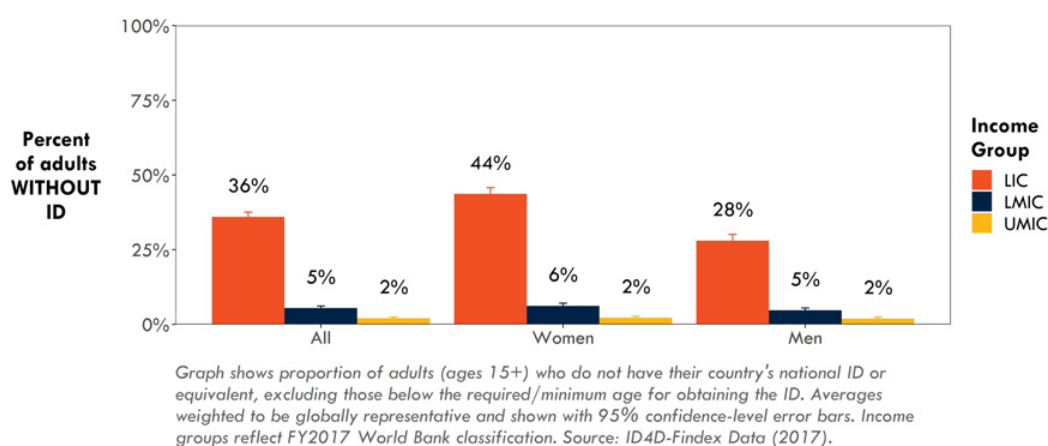
**Women in LICs are less likely to have proof of identity: on average, 44 percent of women in LICs do not have an ID, compared to 28 percent of men** (Figure 1). Gender gaps in middle- and high-income countries tend to be much smaller. A few surveyed countries stand out as having particularly large gender differences in ID coverage: in Afghanistan, almost twice as many men as women report having an ID (known locally as a Tazkira). In Chad, Niger, Benin, and South Sudan, there is more than a 20-percentage point difference in ID ownership between men and women (Figure 2).

The reasons for the gender gap in ID coverage are complex and the ID4D-Findex data can only provide some clues. Among the surveyed countries with the greatest

gender gaps in ID coverage, several also have [legal barriers for women's access to identity documents](#). For instance, the World Bank's Women, Business and the Law report shows that in Afghanistan, Benin, and Pakistan, a married woman cannot apply for a national ID in the same way as a married man. Legal barriers to accessing IDs for women are often the result of prevailing social norms and tend to demonstrate deep rooted assumptions about the appropriate role of women in society. For instance, Chad ranks 158th and Niger ranks 151st out of 160 countries on UNDP's gender inequality index<sup>4</sup>.

Regression analysis also shows that in LICs, married men are considerably more likely to have an ID than unmarried men, all else equal; for women, however, marital status does not change the likelihood of having an ID. One speculative explanation for this trend is that after marriage, men often become the head of household, taking on more responsibility for accessing services for which an ID is often needed, such as mobile and financial services. Conversely, women who transition from their parent's household to their husband's household may not have a similar shift in responsibilities, leading to a relatively constant rate of possessing an ID before and after marriage.

Figure 1. Share of adults without an ID, by gender and country income group<sup>3</sup>

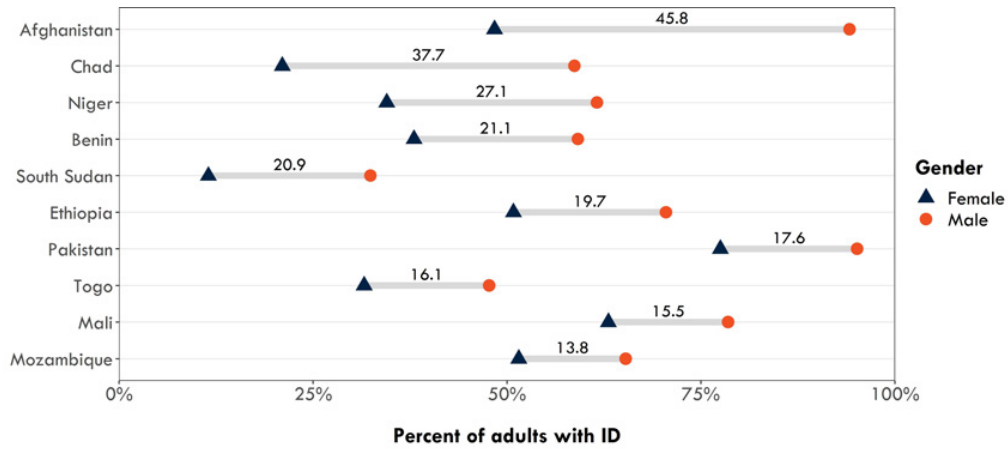


2 Based on data from the 18 low income countries that were included in the survey—Afghanistan, Benin, Burkina Faso, Chad, Ethiopia, Guinea, Haiti, Madagascar, Malawi, Mali, Mozambique, Niger, Rwanda, Senegal, South Sudan, Togo, Uganda, and Zimbabwe—weighted to be regionally representative.

3 LMIC = lower-middle income country; UMIC = upper-middle income country

4 See: <http://hdr.undp.org/en/content/gender-inequality-index-gii>

**Figure 2. Countries with the greatest gender gaps in ID coverage**

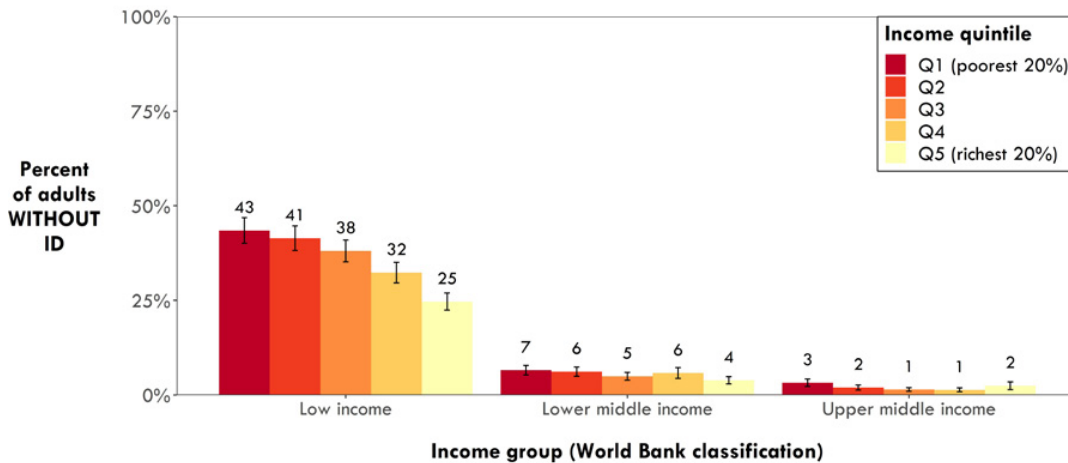


Graph shows proportion of adults (ages 15+) who do not have their country's national ID or equivalent, excluding those below the required/minimum age for obtaining the ID. Differences in coverage shown between men and women are significant at the 99% confidence level or above. Averages weighted to be representative at the country level. Source: ID4D-Findex Data (2017).

**Within countries—and especially in LICs—the poor are at a greater risk of getting left behind.** There is a clear association between being poor and not having an ID and the 'income gap' in ID coverage is greatest in low-income countries. Across LICs, 43 percent of respondents in the poorest income quintile do not have an ID, compared to 25 percent in the richest quintile. 'Income gaps' also vary

significantly by economy. Among surveyed countries, the income gap is greatest in Togo, Lao PDR, Mozambique, and Ethiopia, where there is a greater than a 30 percentage-point difference between the top and bottom quintiles of the income distribution. Niger, Haiti, and Benin, also all have income gaps greater than 20 percentage points.

**Figure 3. Share of adults without an ID, by income quintile**

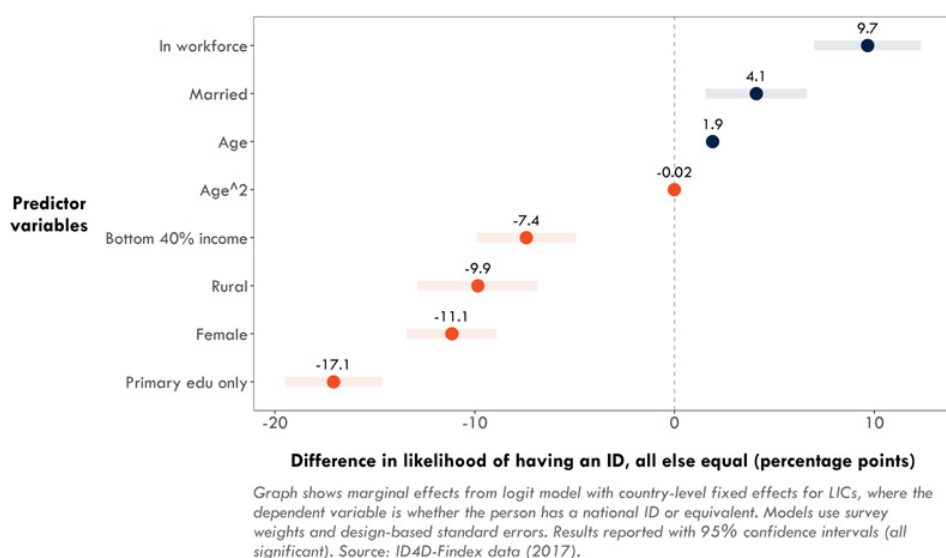


Graph shows proportion of adults (ages 15+) who do not have their country's national ID or equivalent, excluding those below the required/minimum age for obtaining the ID. Averages weighted to be globally representative and shown with 95% confidence intervals. Source: ID4D-Findex Data (2017).

As shown in Figure 4, these differences in income and gender persist even when controlling for other factors. The ID4D-Findex data also reveal some additional important individual-level predictors of who has an ID. **All else equal, people in LICs are *more likely* to have an ID when they are married, older, and in the workforce,<sup>5</sup> and *less likely* to have an ID when they have attained only a primary level of education, are female, live in a rural area, and are in the bottom 40 percent of the income distribution.**

All else equal, an adult living in a LIC with primary education or less is nearly 18 percentage points less likely to have an ID, compared with adults who have completed secondary school or above. In addition, a person living in a rural area in a LIC is approximately 10 percentage points less likely to have an ID than a person living in urban areas, while a person in the bottom of the income distribution is about 7 percentage points less likely to have an ID than a person in top of the income distribution.

**Figure 4. Individual-level predictors of the respondent having an ID (LICs only)**



## WHY DON'T PEOPLE HAVE AN ID?

**What explains these coverage gaps? Not having access to an ID may be the result of overall supply constraints as well as multiple economic, social, and procedural barriers that affect people at the individual level.<sup>6</sup>** For example, people often face high direct and indirect costs to obtaining a national ID or other foundational documents. A synthesis of ID4D Diagnostics in 17 African countries shows that fees for ID cards can be as high as US\$ 8-10, and applicants will often need to spend an additional US\$ 10-25 on travel costs and supporting documentation<sup>7</sup>. People living in the most remote and marginalized

communities often experience the highest costs due to the large distances to the nearest registration office.

These barriers may be multiplied if applicants need to present supporting documents that require additional fees and visits to government offices. Furthermore, people in marginalized groups may also be less likely have the supporting documentation required to obtain national IDs, such as birth certificates or certificates of nationality. Globally, for example, UNICEF reports that only 56 percent of children under the age of 5 born to families among the poorest 20 percent in their countries had their births registered, compared to 82 percent of those among the richest 20 percent<sup>8</sup>.

<sup>5</sup> However, as indicated by a small but statistically significant negative coefficient on the age-squared term, the marginal effect of age on the likelihood of having an ID decreases slightly over time.

<sup>6</sup> For a more in-depth discussion of different types of barriers, see the ID4D Practitioner's Guide, available at <http://id4d.worldbank.org/guide>.

<sup>7</sup> <http://documents.worldbank.org/curated/en/156111493234231522/The-State-of-identification-systems-in-Africa-a-synthesis-of-country-assessments>.

<sup>8</sup> <https://data.unicef.org/topic/child-protection/birth-registration/>

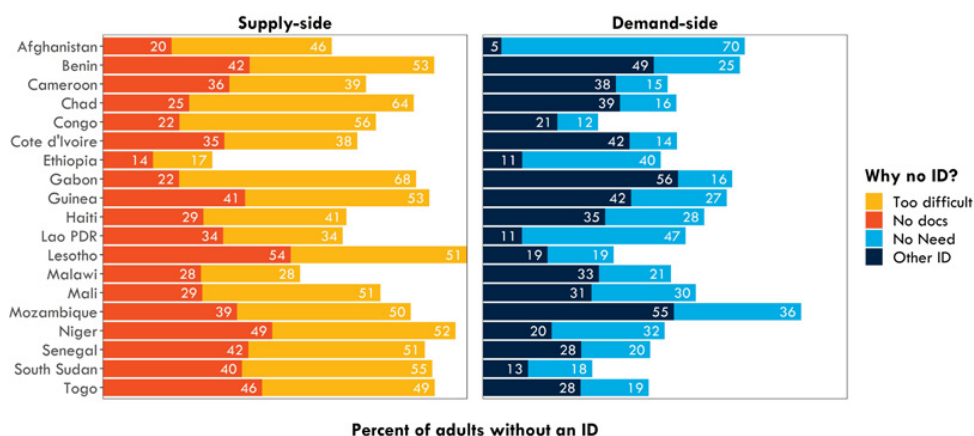
**Beyond these barriers, people may also not have a particular ID because it is not necessary for their daily lives.** For example, some people may see little need for a national ID if they do not commonly use services or perform transactions that would require it. This might be because formal services are not available in their geographic area, because someone else in the household is interfacing with service providers on their behalf, and/or because services are accessible through channels that do not require government-recognized proof of identity. In addition, in some countries, people may have multiple forms of identification, such as passports, driver’s licenses, voter ID cards, beneficiary IDs for a government program, or student or employee IDs that satisfy their identification needs.

**When asked about different reasons why they did *not* have an ID, respondents in countries with ID coverage less than 80 percent cited ‘supply-side’ barriers more commonly than ‘demand-side’ factors in countries with ID coverage.** However, the precise challenges that people selected vary by country. In Gabon, for example—where difficulties with ID card printing and the scarcity of access points have been well documented<sup>9</sup>—nearly 70 percent of people without an ID indicated that this was because the process to apply was too difficult (Figure 5).

Not having supporting documents—which might include a birth certificate, certificate of nationality, proof of address, ID cards of the applicant’s parents, etc.—is also a common barrier to obtaining an ID in many countries. In Lesotho, where under-5 birth registration is less than 50 percent and an even higher share of adults have no birth certificates, lack of necessary documents was cited by over half of those without an ID or a total 16 percent of adults.

**Although supply-side barriers appear to be more common in LICs, this is not always the case.** In Afghanistan, for example, 70 percent of people without an ID responded that they do not have the ID because they have no need for it, as did 40 percent of those in Ethiopia—in both countries, the majority of people without an ID are women. In a few surveyed countries with low ID coverage, we also see high proportions of people without an ID reporting the possession of other identity documents, including in Gabon (56 percent), Mozambique (55 percent), and Benin (49 percent). Without more detailed, country specific information, we cannot, however, accurately assess how well these alternative identity documents empower their holders, i.e. to what extent they allow a person to access public services, open a financial account, or obtain a SIM card.

**Figure 5. Reasons for not having an ID, cited by adults without one**



Percent of adults without an ID

Graph shows proportion of adults (ages 15+, excluding those below the required/minimum age for obtaining the ID) who reported various reasons for not having their country’s national ID or equivalent; multiple answers possible. Only countries with ID coverage less than 80% are shown. Averages weighted to be representative of the country level. Source: ID4D-Findex Data (2017).

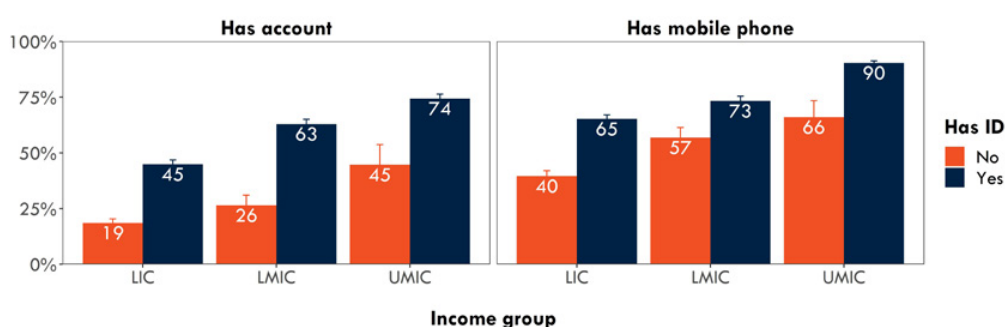
9 See, for example, <http://www.gabonco.com/carte-nationale-d-identite-une-piece-d-etat-civil-devenue-rarissime.html> and <http://www.gabonactu.com/gouvernement-envisage-detablir-cartes-nationales-didentite-cedoc/>.

## HOW DO IDS FACILITATE ACCESS TO SERVICES?

From a development perspective, access to government-recognized identity credentials matters because exercising one's rights and accessing basic services and economic opportunities often require official proof of identity. In turn, unique and verifiable IDs can facilitate more effective delivery of services and payments, helping

to minimize fraud and leakages and improve targeting. The ID4D-Findex data provide insights on the association between having an ID and having a bank account or a mobile phone. In addition, respondents who reported having an ID were asked whether they had ever used it to (a) apply for a government service, (b) to receive financial support from the government, (c) to use financial services, and/or to (d) apply for a SIM card or mobile phone service.

Figure 6. ID ownership and having a financial account and a mobile phone



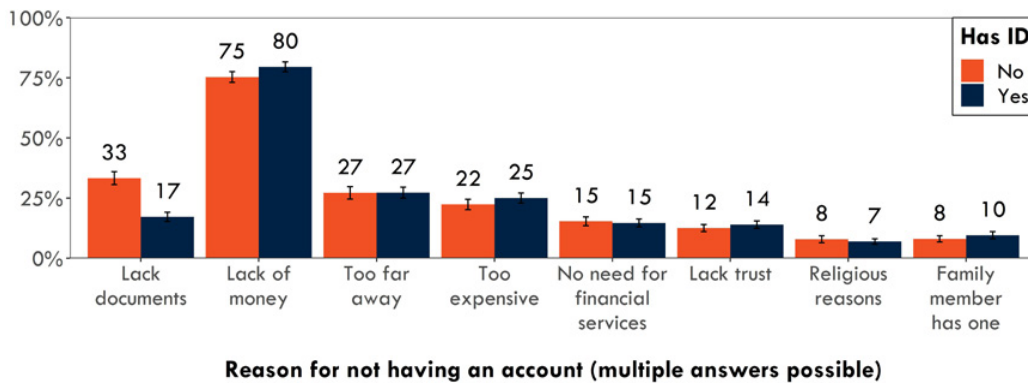
Graph shows proportion of adults (ages 15+, excluding those below the required/minimum age for obtaining the ID) who have an ID vs. those who own a financial account or mobile phone. Averages weighted to be globally representative and shown with 95% confidence-level error bars. Income groups reflect FY2017 World Bank classification. Source: ID4D-Findex Data (2017).

The ID4D-Findex data show that people with IDs are more likely to have a financial account and own a mobile phone than those without. In LICs, an estimated 65 percent of people with IDs have a mobile phone, compared with only 40 percent of those without an ID (Figure 6). Similarly, 45 percent of people with an ID have an account at a financial institution in LICs, compared with only 19 percent of those without an ID.

While we cannot establish a causal relationship with the Findex data—i.e., that having an ID directly led to account or mobile ownership—regression analysis show that **the positive relationship between having an ID and using financial and mobile services persists even after controlling for gender, age, location, education level, income, employment status, marital status, and the country in which a person is living**—all factors that are likely to be correlated both with having an ID and having access to services.

While having a national ID may not always be necessary or sufficient to open a financial account, not having one will often present a severe constraint to accessing financial services. As shown in Figure 7, 33 percent of unbanked people in LICs without an ID cited “lack of documents” as a reason for not having an account; compared with only 17 percent of those with an ID. At the same time, an official ID may only be part of the documentation required to open an account; in many economies, financial institutions also require proof of address, proof of employment, or proof of income. Furthermore, other factors—such as a lack of money, being too far away from a financial service provider, and finding the account opening process too expensive—are cited as frequently or more often than missing documentation as core barriers to account opening. Therefore, although having access to official proof of identity is vital for ensuring financial inclusion because it eliminates a hard constraint to access, many other barriers remain and must be addressed holistically.

Figure 7. ID ownership and barriers to account opening

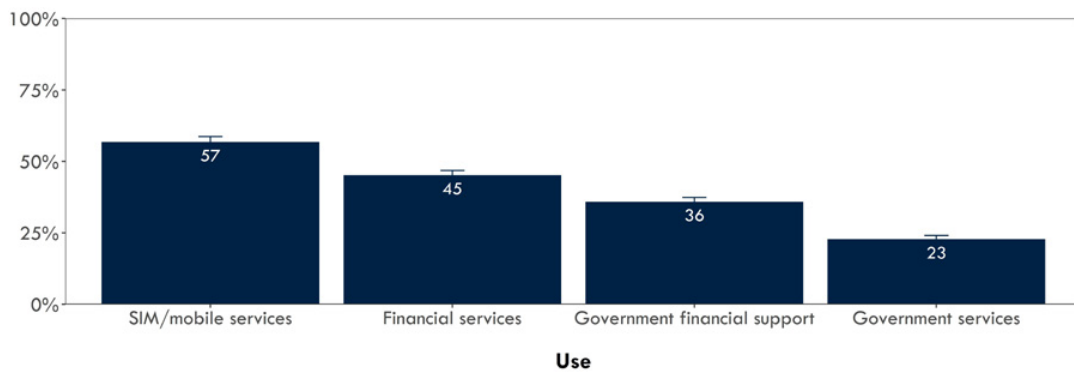


Source: ID4D-Findex data (2017), low-income countries only.

When asked directly whether they had used their IDs for specific purposes, respondents confirmed the frequent use of these credentials to access financial services and mobile phones. Globally, approximately 57 percent of people with an ID have used it to apply for a SIM card or mobile phone service, and 45 percent have used it to access financial

services (Figure 8). The higher reported use of IDs for mobile services fits with the fact that mobile services are more available in most developing countries, and around 80 percent of the surveyed population owns a mobile phone. Furthermore, SIM card registration is mandatory in all LICs included in the main ID4D-Findex questions.<sup>10</sup>

Figure 8. Self-reported use of ID for private- and public services



Graph shows proportion of adults (ages 15+, excluding those below the required/minimum age for obtaining the ID) who report using their national ID or equivalent for different purposes. Averages weighted to be globally representative and shown with 95% confidence-level error bars. Source: ID4D-Findex Data (2017).

10 See [https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofOfID\\_R\\_WebSpreads.pdf](https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofOfID_R_WebSpreads.pdf)

**In addition to accessing financial services and mobile phones, one third of people in LICs say they have used the ID to receive financial support from the government,** and 16 percent say that have used it to apply for government services. These rates are higher in LMICs, where approximately 39 percent of people reported using the ID to receive financial support and 27 percent reported using it to access services. The lower reported use of IDs to access government services in LICs—compared with LMICs and HICs—is likely due to a combination of more limited availability of public services and greater use of informal identification mechanisms when applying for one.

Economies with the highest share of people who report using their IDs for government services and support tend to be ones where the public sector is engaged in extensive service provision. Eastern European and Central Asian countries included in the ID4D-Findex survey stand out in this regard. For example, 89 percent of people with an ID in Belarus, 79 percent in Kazakhstan and about 70 percent in Estonia, Russian Federation, Turkmenistan, and Ukraine cite using their ID to access government services. On the African continent, a handful of surveyed countries also have

a high share of ID holders who report using their credential to access government services, including 76 percent in Morocco, 61 percent in Rwanda, and 60 percent in Namibia. People frequently report using their IDs to receive financial benefits in a handful of South and East Asian countries that invest heavily in social protection, including Thailand (48 percent) and India (37 percent).

**These results also point to a number of areas for future research.** Ultimately, ensuring universal access to identification is only the first step; in order for ID systems to be catalytic for individual welfare and development they must be trusted, empowering, and applied appropriately. Additional work is therefore needed to better measure how—and when—people use their IDs, the barriers they do (and do not) face if they lack a particular ID, and the impact of making an ID mandatory for services that people used to access informally. In addition, more detailed quantitative and qualitative work is needed to better understand how the quality and type of various ID systems—e.g., digital, biometric, mobile, etc.—affect the accessibility and convenience of different services and benefits.

## About ID4D

The World Bank Group's Identification for Development (ID4D) Initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, legal, and among others.

The mission of ID4D is to enable all people to access services and exercise their rights by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of inclusive and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible with support from the World Bank Group, Bill & Melinda Gates Foundation, the UK Government, the Australian Government and the Omidyar Network.

To find out more about ID4D, visit [id4d.worldbank.org](http://id4d.worldbank.org). To participate in the conversation on social media, use the hashtag #ID4D.



# Identity Proofing and Verification of an Individual

Issue No: 3.0  
Feb 2017

## Document History

This document, Good Practice Guide 45 version 3, replaced Good Practice Guide 45 version 2.3 in February 2017.

Version	Date	Comment
1.0	April 2012	First issue
1.1	January 2013	Updated in accordance with IDAP schedule
2.0	May 2013	Second issue
2.1	September 2013	Included changes as a result of lessons learned. Not published
2.2	December 2013	Updated post 2.1 review, version number updated to align with IDAP operations manual
2.3	July 2014	Updated post 2.2 review
3.0	Feb 2017	Included new Level 1 definition, eIDAS regulation, copy changes.

## Identity Proofing and Verification of an Individual

### Purpose and Intended Readership

This document should be read by organisations that are responsible for identity proofing an individual where any HMG Department or service will be relying on that identity. This includes those responsible for the procurement, assessment or delivery of an Identity Assurance (IDA) service.

### Executive Summary

Within the UK there is no official or statutory attribute or set of attributes that are used to uniquely identify individuals across Government. Neither is there a single official or statutory issued document whose primary purpose is that of identifying an individual.

Without such attributes or documentation it is difficult for any person to be absolutely certain of the identity of another. This document is designed to demonstrate how a combination of the breadth of evidence provided, the strength of the evidence itself, the validation and verification processes conducted and a history of activity can provide various levels of assurance around the legitimacy of an identity.

### Changes from Previous Issue

This section provides a summary of the significant changes made from Issue 2.3 to 3.0.

- 2.4 & 2.5 issued during website migration – no content changes
- Updated KBV in Annex C
- Updated definition for Level 1 identity
- Updated IPV Element C for Level 3
- Moved Evidence Category requirements from definitions table to main body of the document
- Moved Annex D into the main body of the document
- Copy and readability changes

### Contents

<b>1. Introduction</b> .....	<b>5</b>
Key Principles.....	5
<b>2. Purpose</b> .....	<b>5</b>
<b>3. Desired Outcomes and Aims</b> .....	<b>5</b>
<b>4. Relationship to IPV standards</b> .....	<b>6</b>
Key Principles.....	6
Relationship to IPV standards.....	6
<b>5. Identity Proofing Definitions</b> .....	<b>8</b>
Key Principles.....	8
Definitions.....	8
<b>6. Overview of Identity Proofing</b> .....	<b>10</b>
Key Principles.....	10
Process .....	10
<b>7. Levels of Identity Proofing Assurance</b> .....	<b>12</b>
Key Principles.....	12
<b>Levels of Identity Proofing</b> .....	<b>12</b>
Level 1 Identity .....	12
Level 2 Identity .....	12
Level 3 Identity .....	12
Level 4 Identity .....	12
<b>8. Identity Proofing and Verification</b> .....	<b>13</b>
Key Principles.....	13
Evidence Categories .....	13
<b>Identity Proofing and Verification (IPV) Elements</b> .....	<b>14</b>
IPV Element A – Strength of Identity Evidence .....	14
IPV Element B – Outcome of the Validation of Identity Evidence.....	15
IPV Element C – Outcome of Identity Verification .....	17
IPV Element D – Outcome of Counter Identity Fraud Checks .....	18
IPV Element E – Activity History of the Claimed Identity .....	18
<b>9. Requirements for each Level of Identity</b> .....	<b>20</b>
Key Principles.....	20
<b>Requirements</b> .....	<b>20</b>
Level 1 Identity .....	20
Level 2 Identity .....	21
Level 3 Identity .....	21
Level 4 Identity .....	22
<b>10. Annex A - Evidence Examples (IPV Element A)</b> .....	<b>23</b>
<b>11. Annex B - Validation (IPV Element B)</b> .....	<b>25</b>
<b>Determining whether Identity Evidence is Genuine</b> .....	<b>25</b>
Examination of the security features of a physical document.....	25
Physical document containing cryptographically protected information.....	25
Electronic evidence containing cryptographically protected information.....	25
<b>Checking if the Identity Evidence is Valid</b> .....	<b>25</b>

## Identity Proofing and Verification of an Individual

<b>12. Annex C - Verification (IPV Element C)</b> .....	<b>26</b>
<b>Knowledge Based Verification</b> .....	<b>26</b>
<b>KBV Principles</b> .....	<b>26</b>
Principle 1: Clarity.....	26
Principle 2: Breadth .....	26
Principle 3: Security.....	26
Principle 4: Sources.....	27
<b>Physical Comparison</b> .....	<b>27</b>
<b>Biometric Comparison</b> .....	<b>28</b>
<b>13. Annex D – Counter Identity Fraud Capabilities (IPV Element D)</b> .....	<b>29</b>
<b>14. Annex E - Example Activity Events (IPV Element E)</b> .....	<b>30</b>
<b>15. Reference</b> .....	<b>31</b>

# Identity Proofing and Verification of an Individual

## 1. Introduction

### Key Principles

- This document is intended to provide guidance on the Identity Proofing and Verification (IPV) of an individual
- This document is intended to state HMG IPV requirements and show how they can be interpreted in the context of International Standards
- This document is under regular review with the content and context made available for indicative purposes only

## 2. Purpose

1. The purpose of this document is to establish a common framework for establishing the requirement for identity proofing and verifying the identity of an individual.
2. This document will provide assurance guidance regarding the acceptability, validation and verification of identity evidence that may be presented by an individual to support their identity.
3. In addition this document will characterise the elements of validation and verification processes that should be carried out.

## 3. Desired Outcomes and Aims

4. This document has a number of aims:
  - To provide organisations with an understanding of the capabilities they will need to be able to demonstrate in order to perform identity proofing
  - To provide information to independent assessment organisations so that benchmarks or profiles can be developed to support the independent assessment and certification of organisational and technical capabilities
  - To establish a common framework establishing requirements for the validation and verification of the identity of individuals

### 4. Relationship to IPV standards

#### Key Principles

- This document covers identity proofing and verification only and has been written to align with, but not directly correlate to other National and International standards and guidance
- The identity levels provided in this document are intended to fulfil the criteria for identity levels in other National and International standards and guidance

#### Relationship to IPV standards

5. This document has been written with the intention of achieving alignment to various National and International standards describing levels of identity assurance, including CESA Good Practice Guide No. 43 (GPG 43), Requirements for Secure Delivery of Online Public Services (RSDOPS) (reference [a]), eIDAS Regulation (reference [b]), ISO/IEC 29115 & NIST 800-63; these being the leading standards in the world at this time. It provides an interpretation of these levels of assurance in the context of IPV for UK public sector for both citizen and internal system users.
6. This is not meant to imply that there is direct correlation between the Assured Identity Levels in this document and the levels in those standards but that it is seen that this document fulfils various criteria as demonstrated in those standards.
7. This document only covers the identity proofing and verification processes, therefore, it may only fulfil part of the requirements of these standards and further measures are required in order to wholly comply (e.g. issuing of a credential).

## Identity Proofing and Verification of an Individual

GPG 45	RSDOPS	eIDAS	29115:2011	ISO 29003 <sup>1</sup>	NIST 800-63 <sup>2</sup>
N/A	Level 0 <sup>3</sup>	N/A	N/A	N/A	N/A
N/A	Level 1 <sup>4</sup>	N/A	LOA 1 <sup>5</sup>	LOA 1 <sup>6</sup>	Level 1 <sup>7</sup>
Level 1	N/A <sup>8</sup>	Low	LOA 2	LOA 2	N/A
Level 2	Level 2	Substantial	LOA 3	LOA 3	N/A
Level 3	Level 3	High	N/A	LOA 4	Level 2
Level 4	N/A <sup>9</sup>	High	LOA 4	LOA 4	Level 3

**Table 1 - Relationship to identity proofing standards**

---

<sup>1</sup> ISO/IEC29003 is currently in working group draft within ISO & BSi; this assessment is made on the draft available at the time of writing

<sup>2</sup> NIST 800-63 is under a major revision; this assessment is made on the draft available at the time of writing.

<sup>3</sup> RSDOPS defines level 0 over 15 security components, there are no personal registration requirements at level 0 therefore identity proofing is not needed.

<sup>4</sup> RSDOPS defines level 0 over 15 security components, there are no identity proofing requirements at level 1 (an identity may be asserted but it is not checked) therefore identity proofing is not needed.

<sup>5</sup> ISO/IEC 29115 has no identity proofing requirements at LOA1

<sup>6</sup> ISO/IEC 29003 has no identity proofing requirements at LOA1

<sup>7</sup> NIST 800-63 has no identity proofing requirements at Level 1

<sup>8</sup> RSDOPS does not contain a personal registration requirement that includes identity proofing lower than level 2.

<sup>9</sup> RSDOPS is only concerned with delivery of online services, this limits its scope to identity levels 1, 2 and 3; a level 4 identity mandates that the person is physically present.

## Identity Proofing and Verification of an Individual

### 5. Identity Proofing Definitions

#### Key Principles

- The definitions of identity relevant terms provided here are intended to support a common understanding in the context of this document

#### Definitions

8. The following definitions explain the purpose and meanings of the terms used within this document.

Term	Definition
Activity Event	An action, transaction or other point in time occurrence (including issue date) that demonstrates an interaction between the Claimed Identity and another entity. Only Activity Events that are connected to an Identity with Personal Details that match those of the Claimed Identity can be used however, shortenings and aliases are permitted (e.g. Mike for Michael).
Activity Event Package	The Activity Event Package is the collection of Activity Events that is used to evaluate the Activity History of the Claimed Identity.
Applicant	The individual who is stating the claim to an identity.
Assessment	The activity of performing the identity proofing process as defined in this document.
Assured Identity	A Claimed Identity that is linked to an Applicant with a defined level of confidence that it is the Applicant's real identity.
Authoritative Source	An authority that has access to sufficient information from an Issuing Source that they are able to confirm the validity of a piece of Identity Evidence.
Biometric	A measure of a human body characteristic that is captured, recorded and/or reproduced in compliance with ICAO 9303, ISO/IEC 19794 or other recognised standards.
Citizen Category	A type of evidence category.
Claimed Identity	A declaration by the Applicant of their current Personal Name, date of birth and address.
Evidence Categories	A collective term for the categories of evidence i.e. Citizen (C), Money (M) and Living (L).
Evidence Details	A combination of the unique reference number(s) and, where applicable, issue date and expiry date included on a piece of Identity Evidence.
Financial Organisation	An organisation that has been classified as a "financial institution" or "credit institution" by the Money Laundering Regulations 2007.
Genuine	To be what something is said to be; i.e. authentic not counterfeit.
Identifier	A thing that is used to repeatedly recognise the same individual. The Identifier isn't required to demonstrate the identity of the individual.
Identity	A collection of attributes that uniquely define a person. The fact of being whom or what a person or thing is.
Identity Assurance	A process that determines that level of confidence that the Applicant's Claimed Identity is their real identity.
Identity Evidence	Information and/or documentation that is provided by the Applicant to support the Claimed Identity. Identity Evidence must, as a



## Identity Proofing and Verification of an Individual

Term	Definition
	minimum, contain the Personal Details <b>OR</b> the Personal Name and photo/image of the person to whom it was issued. Identity Evidence must be current, i.e. it must not be considered invalid because of its age by the Issuing Source at the time of Assessment. Examples of Identity Evidence are given in Annex A.
Identity Evidence Package	The Identity Evidence Package is the collection of Identity Evidence provided to support the Claimed Identity. The Identity Evidence Package must contain at least one piece of Identity Evidence that demonstrates address and one that demonstrates date of birth. The Identity Evidence Package must only contain one piece of Identity Evidence in any Evidence Category.
Identity Evidence Profile	The Identity Evidence Profile sets out the minimum criteria for the strength of Identity Evidence in the Identity Evidence Package.
Issuing Source	An authority that is responsible for the generation of data and/or documents that can be used as Identity Evidence.
Knowledge Based Verification (KBV)	A process that challenges the Applicant using information about the Claimed Identity to verify that the Applicant is indeed that Claimed Identity.
Living Category	A type of evidence category.
Money Category	A type of evidence category.
Personal Details	A combination of Personal Name and <b>at least one of</b> date of birth or address. (Not to be confused with Personal Data as defined by the Data Protection Act.)
Personal Name	A proper name used to identify a real person, as a minimum this contains forename and surname (also known as given name and family name); it may include titles, other/middle names and suffixes.
Proprietary Apparatus	Any apparatus that is, or has been, specially designed or adapted for the making of false documents, and any article or material that is, or has been, specially designed or adapted to be used in the making of such documents.
Proprietary Knowledge	Knowledge about the format, layout and material that is required for the making of a false document.
Public Authority	An organisation that has been classified as such by the Freedom of Information Act 2000.
Valid	To know that something stated is true.
Validation	A process performed to determine whether a piece of Identity Evidence is Genuine and/or Valid.
Verification	A process performed to determine whether the Applicant is the owner of the Claimed Identity.

**Table 2 – Definitions**

### 6. Overview of Identity Proofing

#### Key Principles

- The process should enable a legitimate individual to prove their identity in a straightforward manner whilst creating significant barriers to those trying to claim to be somebody they are not
- The individual shall expressly declare their identity
- The individual shall provide evidence to prove their identity
- The evidence shall be confirmed as being Valid and/or Genuine and belonging to the individual
- Checks against the identity confirm whether it exists in the real world
- The breadth and depth of evidence and checking required shall differ depending on the level of assurance needed in that the identity is real and belongs to the individual

#### Process

9. The Applicant shall be required to declare the name, date of birth and address that they wish to be known as so that there is no ambiguity about the identity that is going to be used (Claimed Identity).
10. The Applicant shall be required to provide evidence that the Claimed Identity exists (Identity Evidence Package). This may be provided electronically or physically depending on the level of assurance required and the capabilities of the organisation that is going to proof the Applicant.
11. The evidence provided shall be checked in order to determine whether it is Genuine and/or Valid (Validation).
12. The Applicant shall be compared to the provided evidence and/or knowledge about the Claimed Identity to determine whether it relates to them (Verification).
13. The Claimed Identity shall be subjected to checks to determine whether it has had an existence in the real world over a period of time (Activity History).
14. The Claimed Identity shall be checked with various counter-fraud services to ensure that it is not a known fraudulent identity and to help protect individuals who have been victims of identity theft (Counter-Fraud Checks).
15. At the end of the process there is an Assured Identity that describes the level of confidence that the Applicant is the owner of the Claimed Identity and that identity is genuine.

## Identity Proofing and Verification of an Individual

16. The identity proofing process does not need to be performed in the order outlined above, however the organisation performing the proofing shall ensure that all the steps are adequately completed.

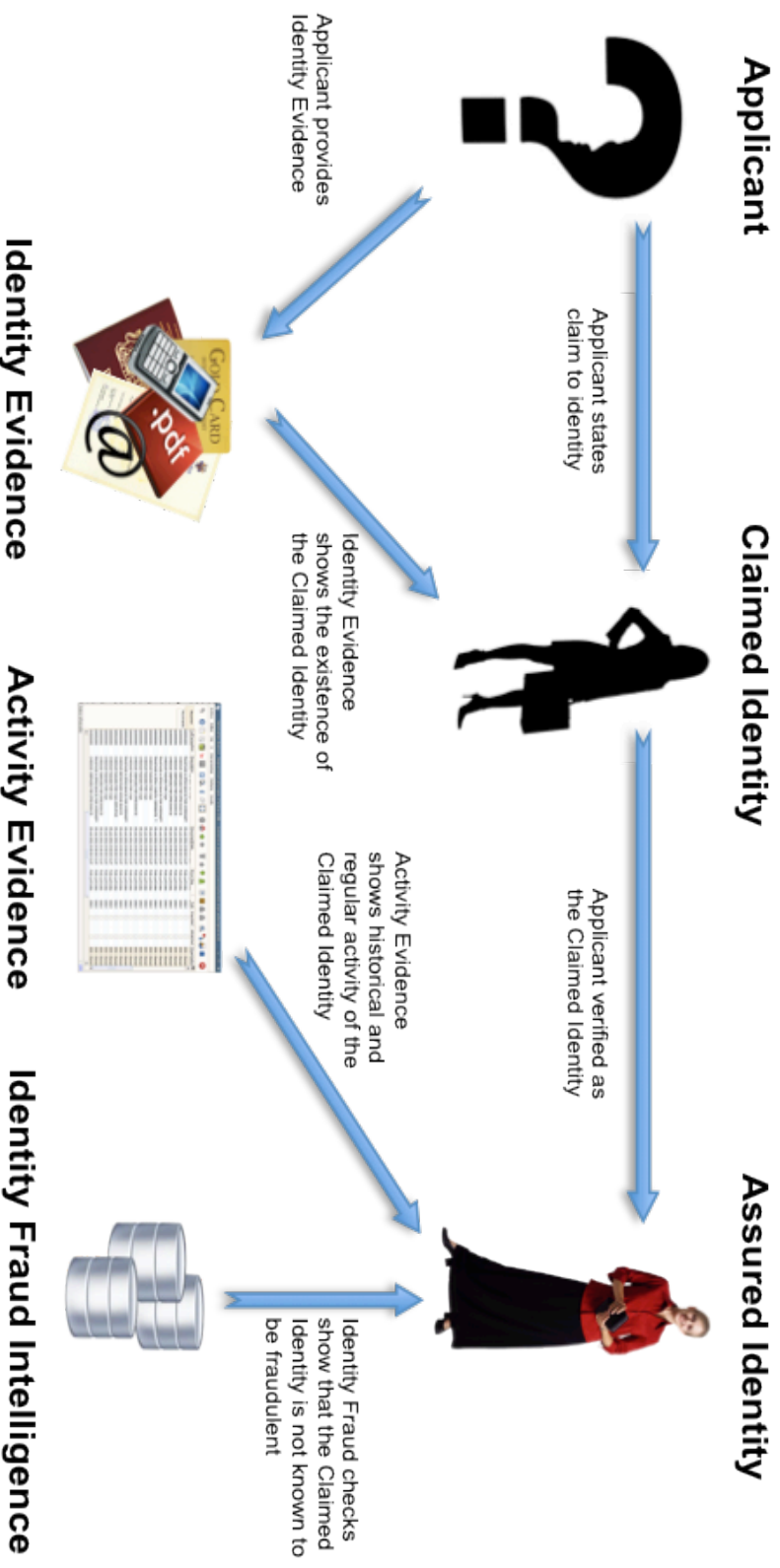


Figure 1 - Overview of the Identity Proofing and Verification Process

### 7. Levels of Identity Proofing Assurance

#### Key Principles

- Four levels of identity proofing are provided, each of which provide an increasing level of confidence that the applicant's claimed identity is their real identity

#### Levels of Identity Proofing

17. This document has been written with the intention of achieving alignment to National and International standards describing levels of identity assurance, including RSDOPS, GPG 43, (reference [a]). For further information see Chapter 2; note that RSDOPS contains security controls at Level 0, however it has no personal registration requirements at Level 0 therefore identity proofing is not performed.

#### Level 1 Identity

18. A Level 1 Identity is a Claimed Identity with some checks that support the existence of that identity. The steps taken determine that the Applicant may be the owner of the Claimed Identity.

#### Level 2 Identity

19. A Level 2 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity. The steps taken determine that the identity relates to a real person and that the Applicant is, on the balance of probabilities, the rightful owner of the Claimed Identity.

#### Level 3 Identity

20. A Level 3 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken determine that the identity relates to a real person and that the Applicant is, beyond reasonable doubt, the rightful owner of the Claimed Identity.

#### Level 4 Identity

21. A Level 4 Identity is a Level 3 Identity that is required to provide further evidence and is subjected to additional and specific processes, including the use of Biometrics, to further protect the identity from impersonation or fabrication. This is intended for those persons who are very high risk; for example who may be in a position of trust or situations where compromise could represent a danger to life.

## 8. Identity Proofing and Verification

### Key Principles

- Evidence categories are used to characterise the breadth of evidence that supports a Claimed Identity
- Identity Proofing and Verification (IPV) elements are used to characterise and score the checks carried out against a Claimed Identity

### Evidence Categories

22. There are 3 Evidence Categories that are described in this section.
23. Evidence shall be assessed against each category and can be considered in multiple categories where it meets the required criteria. To be considered in a specific category Evidence shall meet at least one of the criteria as shown in the table below.

Category	Criteria
Citizen	<ul style="list-style-type: none"> <li>• Be issued by a Public Authority (or national equivalent)</li> <li>• Be issued by an organisation through a process determined by a Public Authority (or national equivalent)</li> </ul>
Money	<ul style="list-style-type: none"> <li>• Be issued by a Financial Organisation regulated by a Public Authority (or national equivalent)</li> <li>• Be issued by a Financial Organisation regulated by a body mandated by national legislation</li> </ul>
Living	<ul style="list-style-type: none"> <li>• Be issued by an organisation that provides employment to the Applicant</li> <li>• Be issued by an organisation that provides education services to the Applicant</li> <li>• Be issued by an organisation that provides training services to the Applicant</li> <li>• Be issued by an organisation that provides certified assessment of the Applicant</li> <li>• Be issued by an organisation that provides licensing of the Applicant</li> <li>• Be issued by an organisation that provides an essential utility to the Applicant</li> <li>• Be issued by an organisation that provides living support to the Applicant</li> <li>• Be issued by an organisation that operates a community or social group/network to which the Applicant belongs</li> <li>• Be issued by an organisation that operates a loyalty programme to which the Applicant belongs</li> <li>• Be issued by an organisation that operates a subscription service to which the Applicant subscribes</li> <li>• Be issued by an organisation that provides health services to the Applicant</li> <li>• Be issued by an organisation that provides goods or services to the Applicant</li> </ul>

**Table 3 – Evidence Categories**

24. Where evidence meets the required criteria for multiple categories it may only be used to fulfil one category requirement at a time per Identity Proofing and Verification (IPV) Element (i.e. it doesn't count as fulfilling two categories for a specific IPV Element but can be in different categories for different IPV Elements). This does not mean the evidence must be in the same category for

## Identity Proofing and Verification of an Individual

all Applicants, the same type of evidence (e.g. a Bank credit account) may be used in different categories for different Applicants.

### Identity Proofing and Verification (IPV) Elements

25. There are 5 IPV elements that are described in the following sections.

#### IPV Element A – Strength of Identity Evidence

26. The purpose of this element is to record the strength of the Identity Evidence provided by the Applicant in support of the Claimed Identity. The following Table demonstrates the properties of the Identity Evidence and the corresponding score for this element. The Identity Evidence must, as a minimum, meet all the properties defined for a particular strength to achieve that score.

Score	Properties of the Identity Evidence
1	<ul style="list-style-type: none"> <li>• The issuing source of the Identity Evidence performed no identity checking</li> <li>• The issuing process for the Identity Evidence means that it can reasonably be assumed to have been delivered into the possession of an individual</li> <li>• The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates <b>OR</b> The issued Identity Evidence contains a photograph/image/Biometric of the person to whom it relates</li> </ul>
2	<ul style="list-style-type: none"> <li>• The Issuing Source of the Identity Evidence confirmed the applicant's identity through an identity checking process</li> <li>• The issuing process for the Identity Evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates</li> <li>• The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates <b>OR</b> The issued Identity Evidence contains a photograph/image/Biometric of the person to whom it relates</li> <li>• Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods and those methods ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed</li> <li>• Where the issued Identity Evidence is, or includes, a physical object it requires Proprietary Knowledge to be able to reproduce it</li> </ul>
3	<ul style="list-style-type: none"> <li>• The Issuing Source of the Identity Evidence confirmed the applicant's identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007</li> <li>• The issuing process for the Identity Evidence ensured that it was delivered into the possession of the person to whom it relates</li> <li>• The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates</li> <li>• The Personal Name on the issued Identity Evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases and initials for forenames and surnames are not permitted</li> <li>• The issued Identity Evidence contains a photograph/image/Biometric of the person to whom it relates <b>OR</b> The ownership of the issued Identity Evidence can be confirmed using cryptographic methods</li> <li>• Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods that ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be</li> </ul>

## Identity Proofing and Verification of an Individual

Score	Properties of the Identity Evidence
	<p>confirmed</p> <ul style="list-style-type: none"> <li>Where the issued Identity Evidence is, or includes, a physical object it contains developed security features that requires Proprietary Knowledge and Proprietary Apparatus to be able to reproduce it</li> </ul>
4	<ul style="list-style-type: none"> <li>The Issuing Source of the Identity Evidence confirmed the applicant's identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007</li> <li>The Issuing Source visually identified the applicant and performed further checks to confirm the existence of that identity</li> <li>The issuing process for the Identity Evidence ensured that it was delivered into the possession of the person to whom it relates</li> <li>The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates</li> <li>The Personal Name on the issued Identity Evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases and initials for forenames and surnames are not permitted</li> <li>The issued Identity Evidence contains a photograph/image of the person to whom it relates</li> <li>The issued Identity Evidence contains a Biometric of the person to whom it relates</li> <li>Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods that ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed</li> <li>Where the issued Identity Evidence is, or includes, a physical object it contains developed security features that requires Proprietary Knowledge and Proprietary Apparatus to be able to reproduce it</li> </ul>

**Table 4 - Strength of Identity Evidence**

27. Examples of Identity Evidence are given in Annex A.

### IPV Element B – Outcome of the Validation of Identity Evidence

28. The purpose of this element is to record the score obtained from the Identity Evidence Validation process. The following table demonstrates the characteristics of the Validation processes and the corresponding score for this element.

Score	Identity Evidence Validation
1	<ul style="list-style-type: none"> <li>All Personal Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source</li> </ul>
2	<ul style="list-style-type: none"> <li>All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source</li> </ul> <p><b>OR</b></p> <ul style="list-style-type: none"> <li>The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment and confirmed the integrity of the physical security features</li> </ul> <p><b>OR</b></p> <ul style="list-style-type: none"> <li>The issued Identity Evidence has been confirmed as Genuine by confirmation of the integrity of the cryptographic security features</li> </ul>

## Identity Proofing and Verification of an Individual

Score	Identity Evidence Validation
3	<ul style="list-style-type: none"> <li>• The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment and confirmed the integrity of the physical security features <b>OR</b> The issued Identity Evidence has been confirmed as Genuine by confirmation of the integrity of the cryptographic security features <b>AND</b></li> <li>• All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source <b>OR</b> Evidence Details from the Identity Evidence have been confirmed as not known to be invalid by comparison with information held/published by the Issuing Source/Authoritative Source</li> </ul>
4	<ul style="list-style-type: none"> <li>• The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment including the integrity of any cryptographic security features <b>AND</b></li> <li>• All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing Source/Authoritative Source</li> </ul>

**Table 5 - Outcome of the Validation of Identity Evidence**

29. Guidance on determining if Identity Evidence is Valid or Genuine is in Annex B.



## Identity Proofing and Verification of an Individual

### IPV Element C – Outcome of Identity Verification

30. The purpose of this element is to record the score obtained from the Identity Verification process. The following table demonstrates the outcomes of the Verification processes and the corresponding score for this element.

Score	Identity Verification Outcome
1	<ul style="list-style-type: none"> <li>The Applicant's ownership of the Claimed Identity has been confirmed by a Knowledge Based Verification process based on pre-shared or known facts</li> </ul>
2	<ul style="list-style-type: none"> <li>The Applicant's ownership of the Claimed Identity has been confirmed by a series of reliable Knowledge Based Verification challenges</li> </ul> <p><b>OR</b></p> <ul style="list-style-type: none"> <li>The Applicant's ownership of the Claimed Identity has been confirmed by a physical comparison of the Applicant to the strongest piece of Genuine Identity Evidence</li> </ul> <p><b>OR</b></p> <ul style="list-style-type: none"> <li>The Applicant's ownership of the Claimed Identity has been confirmed by a Biometric comparison of the Applicant to the strongest piece of Genuine Identity Evidence</li> </ul>
3	<ul style="list-style-type: none"> <li>The Applicant's ownership of the Claimed Identity has been confirmed by a physical or Biometric comparison of the Applicant using a photograph/image/biometric to the strongest piece of Genuine Identity Evidence</li> </ul>
4	<ul style="list-style-type: none"> <li>The Applicant's ownership of the Claimed Identity has been confirmed by a physical or Biometric comparison of the Applicant using a photograph/image/biometric to multiple pieces of Genuine Identity Evidence</li> </ul> <p><b>AND</b></p> <ul style="list-style-type: none"> <li>The Applicant's ownership of the Claimed Identity has been confirmed by a series of reliable Knowledge Based Verification challenges</li> </ul>

**Table 6 - Outcome of Identity Verification**

31. Further guidance on Knowledge Based Verification is contained in Annex C.

## Identity Proofing and Verification of an Individual

### IPV Element D – Outcome of Counter Identity Fraud Checks

32. The purpose of this element is to record the score obtained from the Counter Identity Fraud Check process. The following Table demonstrates the outcomes and the corresponding score once any investigation activity has been carried out for this element.

Score	Counter Identity Fraud Checks
1	<ul style="list-style-type: none"> <li>● No confirmed evidence from an authoritative source that the Claimed Identity may be deceased</li> </ul>
2	<ul style="list-style-type: none"> <li>● No confirmed evidence, from a reliable and authoritative source, that:               <ul style="list-style-type: none"> <li>○ The provided Identifier is being used for fraudulent activity</li> <li>○ The Claimed Identity has been subject to identity theft, regardless whether it was successful or not</li> <li>○ The Claimed Identity is unknown by an organisation that could reasonably be expected to have knowledge of them</li> <li>○ The Claimed Identity is likely to be targeted by third parties, including politically exposed persons</li> <li>○ The Claimed Identity may be deceased</li> <li>○ The Claimed Identity is known to be a fraudulent identity</li> </ul> </li> </ul>
3	<ul style="list-style-type: none"> <li>● No confirmed evidence, from a reliable, authoritative and independent source, that:               <ul style="list-style-type: none"> <li>○ The provided Identifier is being used for fraudulent activity</li> <li>○ The Claimed Identity has been subject to identity theft, regardless whether it was successful or not</li> <li>○ The Claimed Identity is unknown by an organisation that could reasonably be expected to have knowledge of them</li> <li>○ The Claimed Identity is likely to be targeted by third parties, including politically exposed persons</li> <li>○ The Claimed Identity may be deceased</li> <li>○ The Claimed Identity is known to be a fraudulent identity</li> </ul> </li> </ul>
4	<ul style="list-style-type: none"> <li>● No confirmed evidence, from multiple reliable, authoritative and independent sources, that:               <ul style="list-style-type: none"> <li>○ The provided Identifier is being used for fraudulent activity</li> <li>○ The Claimed Identity has been subject to identity theft, regardless whether it was successful or not</li> <li>○ The Claimed Identity is unknown by an organisation that could reasonably be expected to have knowledge of them</li> <li>○ The Claimed Identity is likely to be targeted by third parties, including politically exposed persons</li> <li>○ The Claimed Identity may be deceased</li> <li>○ The Claimed Identity is known to be a fraudulent identity</li> </ul> </li> </ul>

**Table 7 - Outcome of Counter-Fraud Checks**

33. Further guidance on Counter-Fraud Checks is contained in Annex D.

### IPV Element E – Activity History of the Claimed Identity

34. The purpose of Activity History is to prove a continuous existence of the Claimed Identity over a period of time backwards from the point of Assessment. Activity History is determined by collating Activity Events across multiple Evidence Categories into a single Activity Event Package.

## Identity Proofing and Verification of an Individual

35. To qualify, the Activity Event shall relate to an interaction between the Claimed Identity and a source of Activity Events. This can be in either direction, e.g. the Claimed Identity using the services of the source or the source initiating an interaction with the Claimed Identity including issuing something to the Claimed Identity. Activity Event data must refer to an individual whose Personal Details match those of the Claimed Identity, allowing for any changes in Claimed Identity that have occurred over the time period being assessed for the Activity History.
36. The degree of assurance that can be taken from the Activity History process is linked to the quality of the data used, how easily it can be fabricated and how well its integrity is protected. The proofing organisation shall take this in to account when assessing the Activity History, expanding the data sources and extending the history period where there is insufficient confidence in the Activity Events.
37. The proofing organisation shall be able to demonstrate with the Activity Events a continuous existence of the Claimed Identity over the period required by the Identity Level.
38. The following table describes the scoring profile for this element.

Score	Properties of Activity History
1	• No demonstration of an Identity's Activity History was required
2	• Claimed Identity demonstrates an Activity History of at least 180 calendar days
3	• Claimed Identity demonstrates an Activity History of at least 405 calendar days
4	• Claimed Identity demonstrates an Activity History of at least 1080 calendar days

**Table 8 - Activity History of the Claimed Identity**

39. Examples of Activity Evidence are given in Annex E.

### 9. Requirements for each Level of Identity

#### Key Principles

- The 4 levels of identity attract increasing requirements in terms of the IPV element scores as documented in Chapter 6

#### Requirements

40. The following tables set out the minimum criteria for each IPV element in the various Identity Levels. If higher scores are achieved in an IPV element, they do not materially affect the other IPV element requirements; e.g. if Level 4 Identity Evidence is provided yet only Level 3 Identity Evidence was required, the Validation and Verification requirements remain as Level 3.

#### Level 1 Identity

Category	Requirements
Identity Evidence Profile	There is no Identity Evidence Package required.
Validation of Identity Evidence	There is no Validation of Identity Evidence required.
Verification	As a minimum the Applicant must be Verified as being the owner of the Claimed Identity by a process that is able to achieve a score of 1 for Verification.  However where <b>Genuine</b> Identity Evidence is needed to be used as the basis for the Verification then that Identity Evidence must achieve a score of 2 in IPV Element A and must be Validated with a process that is able to achieve a score 2 (IPV Element B).
Counter-Fraud Checks	As a minimum the Claimed Identity must be subjected to a Counter-Fraud Check by a process that is able to achieve a score of 1.
Activity History	There is no requirement to prove the activity of the Claimed Identity therefore there is no requirement for the Activity Event Package or for any Activity History to be demonstrated.

**Table 9 - Requirements for a Level 1 Identity**

## Identity Proofing and Verification of an Individual

### Level 2 Identity

Category	Requirements
Identity Evidence Profile	<p>The Identity Evidence Package must contain Identity Evidence that as a minimum meets one of following profiles:</p> <ul style="list-style-type: none"> <li>- 1 piece of Identity Evidence with a score of 3</li> <li>- 1 piece of Identity Evidence with a score of 2</li> </ul> <p><b>OR</b></p> <ul style="list-style-type: none"> <li>- 3 pieces of Identity Evidence with a score of 2</li> </ul> <p>These are referred to as an Identity Evidence Profile of 3:2 and 2:2:2 respectively.</p>
Validation of Identity Evidence	Each piece of Identity Evidence must be Validated with a process that is able to achieve a score that matches the Identity Evidence Profile; i.e. where the profile is 3:2 the Validation processes must be able to also achieve scores of 3:2 respectively, where it is 2:2:2 it must be able to achieve scores of 2:2:2.
Verification	As a minimum the Applicant must be Verified as being the owner of the Claimed Identity by a process that is able to achieve a score of 2 for Verification.
Counter-Fraud Checks	As a minimum the Claimed Identity must be subjected to a Counter-Fraud Check by a process that is able to achieve a score of 2.
Activity History	As a minimum the Activity Event Package must be able to achieve a score of 2 for the Activity History of the Claimed Identity.

**Table 10 - Requirements for a Level 2 Identity**

### Level 3 Identity

Category	Requirements
Identity Evidence Profile	<p>The Identity Evidence Package must contain Identity Evidence that as a minimum meets one of following profiles:</p> <ul style="list-style-type: none"> <li>- 2 pieces of Identity Evidence with a score of 3</li> </ul> <p><b>OR</b></p> <ul style="list-style-type: none"> <li>- 1 piece of Identity Evidence with a score of 3</li> <li>- 2 pieces of Identity Evidence with a score of 2</li> </ul> <p>These are referred to as an Identity Evidence Profile of 3:3 and 3:2:2 respectively.</p>
Validation of Identity Evidence	Each piece of Identity Evidence must be Validated with a process that is able to achieve a score that matches the Identity Evidence Profile; i.e. where the profile is 3:3 the Validation processes must be able to also achieve scores of 3:3 respectively, where it is 3:2:2 it must be able to achieve scores of 3:2:2 respectively.
Verification	As a minimum the Applicant must be Verified as being the owner of the Claimed Identity by a process that is able to achieve a score of 3 for Verification.
Counter-Fraud Checks	As a minimum the Claimed Identity must be subjected to a Counter-Fraud Check by a process that is able to achieve a score of 3.
Activity History	As a minimum the Activity Event Package must be able to achieve

## Identity Proofing and Verification of an Individual

Category	Requirements
	a score of 3 for the Activity History of the Claimed Identity.

**Table 11 - Requirements for a Level 3 Identity**

### Level 4 Identity

Category	Requirements
Identity Evidence Profile	<p>The Identity Evidence Package must contain Identity Evidence that as a minimum meets one of following profiles:</p> <ul style="list-style-type: none"> <li>- 1 piece of Identity Evidence with a score of 4</li> <li>- 1 piece of Identity Evidence with a score of 3</li> </ul> <p><b>OR</b></p> <ul style="list-style-type: none"> <li>- 2 pieces of Identity Evidence with a score of 3</li> <li>- 1 piece of Identity Evidence with a score of 2</li> </ul> <p>These are referred to as an Identity Evidence Profile of 4:3 and 3:3:2 respectively.</p>
Validation of Identity Evidence	Each piece of Identity Evidence must be Validated with a process that is able to achieve a score that matches the Identity Evidence Profile; i.e. where the profile is 4:3 the Validation processes must be able to also achieve scores of 4:3 respectively, where it is 3:3:2 it must be able to achieve scores of 3:3:2 respectively.
Verification	As a minimum the Applicant must be Verified as being the owner of the Claimed Identity by a process that is able to achieve a score of 4 for Verification.
Counter-Fraud Checks	As a minimum the Claimed Identity must be subjected to a Counter-Fraud Check by a process that is able to achieve a score of 4.
Activity History	As a minimum the Activity Event Package must be able to achieve a score of 4 for the Activity History of the Claimed Identity.

**Table 12 - Requirements for a Level 4 Identity**

## Identity Proofing and Verification of an Individual

### 10. Annex A - Evidence Examples (IPV Element A)

41. No single piece of evidence can be considered as proof of identity. However combined with other pieces of evidence they can be used in order to develop a level of assurance as to the identity of an individual.
42. The following tables provide examples of the types of evidence data that may be provided and the Evidence Categories they could be considered to be in. The Tables should not be considered as complete or definitive.

Identity Evidence	Citizen	Money	Living
Fixed line telephone account			X
Gas supply account			X
Electricity supply account			X
Police bail sheet	X		X

**Table 13 - Level 1 Identity Evidence**

Identity Evidence	Citizen	Money	Living
Firearm Certificate	X		X
DBS Enhanced Disclosure Certificate	X		
HMG issued convention travel document	X		
HMG issued stateless person document	X		
HMG issued certificate of travel	X		
HMG issued certificate of identity	X		
Birth certificate	X		
Adoption certificate	X		
UK asylum seekers Application Registration Card (ARC)	X		
Unsecured personal loan account (excluding pay day loans)		X	X
National 60+ bus pass	X		X
An education certificate gained from an educational institution regulated or administered by a Public Authority (e.g. GCSE, GCE, A Level, O Level)	X		X
An education certificate gained from a well recognised higher educational institution			X
Residential property rental or purchase agreement		X	X
Proof of age card issued under the Proof of Age Standards Scheme (without a unique reference number)			X
Police warrant card	X		
Freedom pass	X		X
Marriage certificate	X		X
Fire brigade ID card	X		
Non bank savings account		X	
Mobile telephone contract account		X	X
Buildings insurance			X
Contents insurance			X

## Identity Proofing and Verification of an Individual

Identity Evidence	Citizen	Money	Living
Vehicle insurance			X

**Table 14 - Level 2 Identity Evidence**

Identity Evidence	Citizen	Money	Living
Passports that comply with ICAO 9303 (Machine Readable Travel Documents)	X		
EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004	X		
Northern Ireland Voters Card	X		X
US passport card	X		
Retail bank/credit union/building society current account		X	
Student loan account		X	X
Bank credit account (credit card)		X	X
Non-bank credit account (including credit/store/charge cards)		X	
Bank savings account		X	
Buy to let mortgage account		X	X
Digital tachograph card	X		X
Armed forces ID card	X		
Proof of age card issued under the Proof of Age Standards Scheme (containing a unique reference number)			X
Secured loan account (including hire purchase)		X	X
Mortgage account		X	X
EEA/EU full driving licences that comply with European Directive 2006/126/EC	X		X

**Table 15 - Level 3 Identity Evidence**

Identity Evidence	Citizen	Money	Living
Biometric passports that comply with ICAO 9303 (e-passports) and implement basic or enhanced access control (e.g. UK/EEA/EU/US/AU/NZ/CN)	X		
EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004 that contain a biometric	X		
UK Biometric Residence Permit (BRP)	X		
NHS staff card containing a biometric			X

**Table 16 - Level 4 Identity Evidence**



### 11. Annex B - Validation (IPV Element B)

#### Determining whether Identity Evidence is Genuine

##### Examination of the security features of a physical document

43. The proofing organisation capability to Validate identity documents will affect the determined level of identity assurance. The proofing organisation shall have sufficiently trained staff and appropriate equipment to inspect the security features of common forms of physical documents that they accept as Identity Evidence. As a minimum a proofing organisation conducting physical inspection of Identity Evidence shall be able to detect the following common document frauds:

- Counterfeit documents – where a document has been created outside of the normal competent authority processes (e.g. a copy)
- Forged documents – where original documents have been modified to include false details (e.g. changed Personal Details)

##### Physical document containing cryptographically protected information

44. For physical documents provided by the Applicant that contains cryptographically protected information the proofing organisation shall have sufficient equipment, systems and training to be able to interrogate the cryptographically protected information, to ensure that it has not been altered since the Issuing Source produced the Identity Evidence and determine that the cryptographically protected information relates to the physical document to which it is attached.

##### Electronic evidence containing cryptographically protected information

45. For electronic Identity Evidence provided by the Applicant that contains cryptographically protected information (e.g. in a PDF document), the proofing organisation shall have sufficient systems and training to interrogate the cryptographically protected information and determine that it relates to the Identity Evidence, and that the Identity Evidence has not been altered since it was produced by the Issuing Source.

#### Checking if the Identity Evidence is Valid

46. The proofing organisation should confirm that forms of Identity Evidence that include features such as check digits and specific identifier structures are consistent with their specification. Only an Issuing/Authoritative Source may confirm whether the Identity Evidence is Valid; Identity Evidence cannot be determined to be Valid simply from inspection of the Identity Evidence itself (see Genuine).

### 12. Annex C - Verification (IPV Element C)

#### Knowledge Based Verification

47. Knowledge Based Verification (KBV) uses information about the Claimed Identity that should be only known by them to verify that the Applicant is indeed that Claimed Identity. This is usually achieved by challenging the Applicant in a manner so that only the owner of the Claimed Identity could reasonably be expected to respond correctly.

#### KBV Principles

48. There must be a sensible balance between achieving assurance that the Applicant is the owner of the Claimed Identity and an acceptable experience. With this in mind the proofing organisation shall follow a number of KBV principles:

##### Principle 1: Clarity

49. The KBV process must be clear so that the Applicant is able to understand and correctly respond:
- a. KBV process must be relevant, sensible and proportionate
  - b. KBV process must be carefully constructed as to be clear and obvious to the Applicant what is being asked of them
  - c. There must be an expectation that the owner of the Claimed Identity can reasonably be expected to be able to complete the KBV process

##### Principle 2: Breadth

50. The KBV process should cover a wide range of information:
- a. KBV process should be based on a range of information and not reliant upon one single KBV source
  - b. KBV process should cover different Evidence Categories

##### Principle 3: Security

51. The KBV process must protect the Claimed Identity from impersonation:
- a. The KBV process must be constructed so that the loss or theft of a possession such as a wallet/purse would not provide the required information to pass it
  - b. KBV data must not be used where it is known, or likely, that it is in the public domain. Information in the public domain in this context means KBV data that can be accessed by someone other than the person to whom it relates either with or without a degree of research or is contained within an open dataset or website

## Identity Proofing and Verification of an Individual

- c. Where the KBV process offers the User a selection of suggested answers (i.e. multiple choice) then all the answers must be plausible and the correct answer should not be easily guessed
- d. KBV process must be constructed so that it is unlikely that the answers can be drawn from information available in the public domain, including social networking sites and public registers
- e. The KBV process must minimise the risk that it can be passed by a close family member or friend, however it is accepted that in some cases this might not be possible
- f. The KBV process must ensure that where this includes multiple questions that one question doesn't effectively answer another
- g. The KBV process must ensure that where multiple possible answers are presented that they vary from user to user in a manner that makes it unlikely that the correct answer is predictable
- h. The KBV process must ensure that answers have not previously been provided by the Applicant elsewhere in the service
- i. The KBV process must not reveal personal information to the Applicant that they have not already provided

### Principle 4: Sources

52. The KBV process shall use suitable sources in the KBV process:
- a. In this context a source is considered to be the organisation that captures/generates the original data, not any intermediary that is used to gain access to that data
  - b. A source is considered to be an organisation in its entirety however where that organisation has within itself separate acceptance and proofing processes then data that originates from those separate processes can be considered as a separate source
  - c. A source used for KBV must be independent from the Applicant
  - d. Where the source of the KBV is the proofing organisation then they must only use a delivery method that ensures it is delivered to the Claimed Identity (not the Applicant)

### Physical Comparison

53. The physical comparison step of verification requires the Applicant to be verified by a visual confirmation that they appear to be the person to whom the Identity Evidence was issued. The two methods by which this may be completed are an in person face-to-face process and a remote process (e.g. using a

## Identity Proofing and Verification of an Individual

video/video streaming link). In either case the proofing organisation shall consider a number of basic principles:

- Any person performing the comparison must be able to clearly see both the Applicant and the image to which the Applicant is being compared
- Any person performing the comparison shall have sufficient training in performing identification of persons
- The quality of images must be sufficient to allow the identification of the Applicant as the person depicted by the Identity Evidence

### Biometric Comparison

54. The biometric comparison step of verification requires the Applicant to be verified by a biometric confirmation that they appear to be the person to whom the Identity Evidence was issued. The proofing organisation shall consider a number of basic principles:

- The False Non-Match Rate (FNMR) of the biometric matching system
- The False Match Rate (FMR) of the biometric matching system
- The quality of the biometric against which the Applicant is being compared

55. In particular the proofing organisation shall ensure they have a sufficiently low FMR in order to have confidence that the biometric system is effective at detecting imposters.

### **13. Annex D – Counter Identity Fraud Capabilities (IPV Element D)**

56. As part of the counter identity fraud checks the proofing organisation shall perform checks with reliable, authoritative and independent sources. The following demonstrates the conditions to be considered those sources:

- Authoritative: recognised as being a suitable source for the information being sought/checked within Good Industry Practice
- Reliable: demonstrate they can provide a dependable service
- Independent: demonstrate that the staff and processes operate independently from those involved in the identity proofing processes within the proofing organisation

## Identity Proofing and Verification of an Individual

### 14. Annex E - Example Activity Events (IPV Element E)

57. The following Table provides examples of activity events that could be used to demonstrate a history of activity.

<b>Citizen</b>	<b>Money</b>	<b>Living</b>
Electoral roll entry	Repayments on an unsecured personal loan account (excluding pay day loans)	Land registry entry
	Repayments and transactions on a non-bank credit account (credit card)	National pupil database entry
	Debits and credits on a retail bank/credit union/building society current account	Post on internet/social media site
	Repayments on a student loan account	Repayments on a secured loan account
	Repayments and transactions on a bank credit account (credit card)	Repayments on a mortgage account
	Debits and credits on a savings account	Repayments on a gas account
	Repayments on a buy to let mortgage account	Repayments on an electricity account

**Table 17 - Example Activity Events**

## Identity Proofing and Verification of an Individual

### 15. Reference

- [a] CESG Good Practice Guide No. 43, Requirements for Secure Delivery of Online Public Services, Issue 1.1, December 2012.
- [b] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market



[Home](#) [Voters](#) [ID to Vote](#)

## ID to Vote

To vote at the federal election you have to prove your identity and address. There are three ways to do this:

Other languages and printable format

### Option 1: Show one of these pieces of ID

- your driver's licence
- any other card issued by a Canadian government (federal, provincial/territorial or local) with your photo, name and current address

### Option 2: Show two pieces of ID

Both must have your name and at least one must have your current address.

Examples:

- voter information card and bank statement
- utility bill and student ID card

See the full [list of accepted ID](#) below to prove your identity and address under Option 2.



### Option 3: If you don't have ID

You can still vote if you declare your identity and address in writing and have someone who knows you and who is assigned to your polling station vouch for you.

The voucher must be able to prove their identity and address. A person can vouch for only one person (except in long-term care institutions).

## List of accepted ID to prove your identity and address under Option 2

### From a government or government agency

- band membership card
- birth certificate
- Canadian citizenship card or certificate
- Canadian Forces identity card
- Canadian passport

### From a financial institution

- bank statement
- credit card
- credit card statement
- credit union statement
- debit card
- insurance certificate, policy or statement

- card issued by an Inuit local authority
- firearms licence
- government cheque or cheque stub
- government statement of benefits
- health card
- income tax assessment
- Indian status card or temporary confirmation of registration
- library card
- licence or card issued for fishing, trapping or hunting
- liquor identity card
- Métis card
- old age security card
- parolee card
- property tax assessment or evaluation
- public transportation card
- social insurance number card
- vehicle ownership
- Veterans Affairs health care identification card

### From Elections Canada

- targeted revision form to residents of long-term care institutions
- voter information card

### From an educational institution

- correspondence issued by a school, college or university
- student identity card

### From a health care facility or organization

- blood donor card
- CNIB card
- hospital card
- label on a prescription container
- identity bracelet issued by a hospital or long-term care institution
- medical clinic card

- mortgage contract or statement
- pension plan statement
- personal cheque

### From a private organization

- employee card
- residential lease or sub-lease
- utility bill (e.g.: electricity; water; telecommunications services including telephone, cable or satellite)

### Letters of confirmation

- letter from a public curator, public guardian or public trustee
- letter of confirmation of residence from a First Nations band or reserve or an Inuit local authority
- letter of confirmation of residence, letter of stay, admission form, or statement of benefits from one of the following designated establishments:
  - student residence
  - seniors' residence
  - long-term care institution
  - shelter
  - soup kitchen
  - a community-based residential facility

Additional pieces of ID may be added. We accept e-statements and e-invoices. Print them or

show them on a mobile device.

This list of accepted ID is also available in [multiple languages](#). For the list in other formats, such as Braille and audio, call 1-800-463-6868.

## Important information about ID

- We accept pieces of ID in their original format. If your document was issued electronically, like an e-statement or an e-invoice, bring a printout or show it on a mobile device.
- We accept different pieces of ID from the same source if the documents serve different purposes. For example, we accept an invoice and a transcript from the same school.
- Your name and address must be printed on the ID. They can't be added by hand, unless they are added by the issuer of the document, like a residence administrator or a guardian.
- We accept expired ID, as long as it has your name and current address.
- The pieces of ID listed above are authorized by the Chief Electoral Officer. No other pieces will be accepted.
- The pieces of ID required for a federal election are not the same as for provincial, territorial or municipal elections.

[Policy on Voter Identification](#)

[FAQs on ID](#)

[FAQs on the October 26, 2020, Federal By-Elections](#)



SEARCH

# My ID, my identity? The impact of ID systems on transgender people in Argentina, France and the Philippines

We spoke to trans-right activists in three country: the Philippines, France and Argentina to understand how ID systems in their countries are impacting their lives and how certain legal frameworks may help them.

## KEY FINDINGS

- From accessing healthcare to picking a parcel or going to university, ID systems can get in the way of the most simple things when your ID doesn't reflect who you are.
- Some legal systems are in theory facilitating the correction of ID cards but in some countries, administrative difficulties remain in practice.
- Argentina has set a high standard when it comes to gender identity recognition and facilitating the correction of ID cards but societal issues remain.
- Removing gender altogether from ID systems could become a key next step.

## CONTENT TYPE

Long Read

## POST DATE

15th January 2021





Este informe está disponible en **español**.

Most national ID or identifying documents include a gender marker. This is often known as a 'sex marker,' even though the term is inaccurate. The presence of such markers, especially on birth certificates, contribute to our society's emphasis on gender as a criterion for assigning identities, roles and responsibilities within society. With gender being such a determining and dominant identifier, it puts it at the centre of so many arrays of our lives and societal norms and standards. Importantly this categorisation creates a basis for discrimination, and inequality.

The emphasis of gender as an identifier is harmful to all persons who do not identify with the gender they were assigned at birth. Intersex people are also heavily impacted, as babies across the world are facing **unnecessary and brutal surgeries** just for the sake of them having genitals that will match whatever gender is ticked on a birth certificate.

The lack of fluidity and flexibility in current registration systems and identification systems means that people all over the world face barriers to enjoy their rights to self-determination by not being allowed to be recognised by the gender they self-identify with versus the gender assigned to them (at birth).

These gender/sex markers can be difficult, to impossible, to change and can be a site of harassment and create a significant risk surface for trans people whose gender expression doesn't match the gender on their ID to access services and enjoy their rights securely, safely and equality because of legal barriers, stigma, violence and discriminatory policies and practices.

## Definitions and premises

Feminist discourses have given rise to debates and diverging views on gender and its implications. In our effort to promote privacy as the right to establish one's own boundaries, we align ourselves with a feminist tradition that understands gender as a socially- and culturally-constructed interpretation of biological sex. As Judith Butler wrote in *Gender Trouble*: "Gender is the repeated stylization of the body, a set of repeated acts within a highly rigid regulatory frame that congeal over time to produce the appearance of substance, of a natural sort of being."

Gender norms, as imposed by societies, limit space, freedoms, opportunities, possibilities and rights of persons in general, but in particular of persons that do not "fit" established binary and cis gender norms. Drawing on our understanding that gender identity falls under the realm of privacy – where privacy is understood as the right to self-define or the right to choose how to present segments of one's identity – we believe individuals should be free to define their own gender.

This piece will make references to trans women (women who were assigned a "male" gender-marker at birth), trans men (men who were assigned a "female" gender-marker at birth) but also non-binary and gender-fluid people: people whose gender expression does not fit within the strict male/female binary division.

## What happens when your ID does not match who you really are?

Whilst we've been exploring the impact of identity systems on people on issue that Privacy International has been working on relates to exclusion. For example, what happens to migrant groups when **they can't get access to ID**? How does not being able to access identity systems **affect historically marginalised groups**? Yet exclusion emerges not only from those who can't get their birth registered, or get an ID card: also excluded are people who have these documents but cannot make use of them.

While there are still many who are not registered at birth, for those who do receive a birth certificate then in most parts of the world it will show whether we've been assigned 'male' or 'female'. These are often the 'breeder documents' that lead to the issuing of other forms of ID, like national ID cards in those places where these are present. The use of an ID card spreads across a broad sweep of people's lives in many countries: people for example have to be ready to show it when they open a bank account, for any administrative procedures, including access to welfare services or sometimes even to access healthcare where there is not universal access to such a service.

There are risks and consequences when your birth certificates and ID documents do not

reflect the identity you present as. This is the reality that many transgender people are facing across the world. Ensuring that your birth certificate and ID reflect the name you are using and your gender becomes a key part of transitioning. In this context, the avenue for resolution the state can offer you end up becoming life changing.

But even when, on paper, a state may have a positive approach to gender recognition – one that would allow trans people to rectify their gender on their ID without having to endure any invasive administrative or medical procedures in order to prove they are who they say they are – the reality can differ in practice and prove more of a struggle than expected.

In this piece we will initially provide an overview of the main legal systems currently in place across the world, before looking more closely at three case studies: the Philippines, France and Argentina. For each of those countries we have spoken to representatives of trans organisations to hear what their experience of gender recognition has been like and what changes they would like to see.

## **The four common legal frameworks**

When it comes to gender recognition rights and in particular the right for transgender people to correct their ID and birth certificates for them to match the gender they identify with, the world is currently divided between four main legal frameworks: 1) the countries where gender recognition simply does not exist, 2) the countries where trans gender people can correct their ID but are required to undergo surgery for that to happen, 3) gender recognition exists without requiring surgery but requires judicial and/or lengthy administrative procedures, and 4) gender recognition exists without requiring surgery and with minimal administrative procedure.

### **1) Gender recognition does not exist**

**In many countries in the world** – including the Philippines and other parts of South East Asia, all of North and East Africa, most of the Middle East and Central America, and three states in the US – there is still no avenue to allow trans gender people to correct their birth certificate. This means that they cannot have an ID that matches their true identity. Even as they may live a life under the gender they identify with and be known under a name that fits this identity, their ID will still only refer to their deadname (the name given to them at birth) and the sex marker they were assigned at birth. As we will explain below with the case studies of the Philippines, such a situation exposes trans people to serious risks: being outed as trans, with potential consequences including police violence or violence from border control officers and being prevented access to adequate healthcare. Having

an ID that does not reflect their actual identity can also have a serious negative impact on trans people's mental health as it constitutes a constant trigger.

## 2) Gender recognition exists but requires trans people to undergo surgery

**In some countries** – including China, **India**, parts of Central Asia, parts of South East Asia, South Africa, parts of Australia and many states in the United States – trans people can only have their birth certificate and ID corrected if they undergo genital surgery.

This requirement is hugely problematic and bears serious consequences not just for trans people themselves but for society as a whole and our understanding of gender construction. There are many kinds of therapy, treatments and confirmation surgery that trans people may choose to undergo as part of their transition. They may include facial reconstruction, breast surgery, genital surgery, voice training, hormone therapy, hair removal... None of them is required or expected for people to be valid as the gender they identify with. In fact, **many trans people** – and trans men in particular – choose not to ever undergo genital surgery.

Expecting people to undergo genital surgery in order for them to have their gender and name recognised equates to a de facto forced sterilisation, as this type of surgery will prevent them from having their own biological children.

Moreover, states that impose surgery as a condition for being able to correct a birth certificate and ID act as if one specific type of genital surgery "makes" someone a woman or a man and thus perpetuate a vision of gender based on an extremely narrow understanding of both gender and biological sex.

As Lisa Jean Moore and Paisley Currah explain in their paper "**Legally Sexed – Birth Certificates and Transgender Citizens**" (Feminist Surveillance Studies, 2015), which looked at the history of birth certificate correction in the City of New York, requiring surgery also creates inequalities, as the type of surgery required is often the most expensive one, thus resulting in a situation where only trans people who can afford to transition are allowed to have their birth certificate/ID documents corrected.

All those reasons make requiring surgery a dangerous, privacy invasive and potentially traumatic requirement for trans people who should not have to be forced into a surgery they may not want to have – or be forced to prove that they indeed had such a surgery – in order to have identity credentials which match their gender identity.

Beyond the trans community, this requirement perpetuates a belief that gender is a



binary that can be reduced to the shape of a person's genitals. This requirement also roots itself in the transphobic argument that if changing ones' gender marker on an ID is available too easily people would use exploit it to commit fraud (**Moore and Currah, 2015**). This argument leads to a discourse that trans people are lying about their identity until they prove otherwise and that they should have to endure a long and painful process in order for their gender to be recognised.

### **3) Gender recognition exists without requiring surgery but requires judicial and/or lengthy administrative procedures**

**In most of South America**, Western Europe, many states of the Unites States and in Canada, trans people are allowed to correct their gender on their ID without having to undergo surgery. However, while there is no requirement for surgery, there can still be lengthy and stressful medical, administrative or judicial requirements.

Indeed, in some places correcting your ID may involve having to sit through a committee of psychologists who assess the "authenticity" of one's claims or may require lengthy administrative procedures to obtain the correction of one's ID. In France, for instance, trans people still have to obtain the authorisation of a judge to have their gender corrected.

### **4) Gender recognition exists without requiring surgery and with minimal administrative procedure**

In countries like Argentina and Uruguay, recent laws have been passed to facilitate transitioning processes. Trans people just need to request the correction of their gender and provide the name they wish to use to the relevant administrative body and their birth certificate and IDs will be automatically corrected.

In this piece we will look at the case of two countries that both allow gender recognition without requiring surgery – Argentina and France – to understand the contrasting experience and nuances within similar legal framework.

### **Is gender even needed?**

Having sex, or gender, on identification documents is something that can seem so ubiquitous that it is never questioned. However, this is beginning to change.

Some countries are now making efforts towards recognising a third gender. **India**, for instance, legislated in 2014 to recognise a third gender and a person's right to self-identify.

**In Canada**, following a campaign from the Gender Free ID coalition, Kori Doty's child, Searyl, was the first to be born with "U" (unspecified or unknown) on their health card. **In Germany**, since January 2019, people now have the option to choose "other" on their driving licence, birth certificate and other official documents.

However, other countries are also exploring the possibility of removing gender altogether from identification documents altogether. In 2012, **New Zealand** made a proposal to the International Civil Aviation Organization, suggesting gender should be removed from travel documents. While the change for travel documents may take a long time due to the need for international regulations and its associated costs, other countries are working on developing gender-free national initiatives. In France, driving licences no longer feature a gender marker. In July 2020, **in a letter written by the Education Minister to parliament**, the Dutch government announced their plan to remove gender from ID cards in five years from now when other changes to ID card will be made.

### **Exploring the reality on the ground**

In this section, we present three case-studies to illustrate how the legal frameworks outlined in a previous section play out in practice. For each of the three countries studies, we spoke to representatives of trans organisations to hear what their experience of gender recognition had been like and what changes they would like to see. We take the opportunity to thank these individuals and organisations for taking the time to share their knowledge and expertise, and for enabling us to showcase the extraordinary work they are undertaking to advocate for the rights of trans people.



### Case study 1. The Philippines: “Discrimination against trans people begins with their ID” – Naomi Fontanos

In 2018, the Philippines passed a law to establish a new ID system. Entitled The Philippine Identification System Act – or PhilSys Act – the law allowed **the creation of a “super ID”** that would replace the multiple forms of identification cards Filipinos have been using. This national ID **is meant to feature** the owner’s full name, sex, blood type, date and place of birth, marital status, and photo. While the PhilSys registry is meant **to collect additional information** including phone number, email address and biometrics data (10 fingerprints and iris scan).

The ID is meant to not only be used when interacting with the state – **including for tax, benefits, access to schools and hospitals** – but also **for private transactions**, like opening a bank account.

As of October 2020, however, the ID still has not been rolled out. The government announced at the end of 2019 that Filipinos would all be enrolled by 2022.

Back in 2018, PI spoke to Naomi Fontanos, a trans woman and trans rights activist, co-founder and Executive Director of the organisation **Ganda Filipinas**, about this very law. You can listen to the recording of the interview **here**.

Ganda Filipinas has long been campaigning for gender recognition, the right for trans people to be able to correct their ID and birth certificate.

*"It is very important in order to access other civil, political economic and cultural rights in our country. I have always maintained, as a trans activist, that discrimination against trans people begins with their ID because it creates a domino effect in trans people's lives. For example, if a trans person applies for a job and the gender and name on their ID do not match their gender presentation they will most likely be denied that job. And everything will go downhill from there because if a trans person doesn't have a job they will join the statistics of poor people in this country. And if you're poor you can't have healthcare. And if you don't have healthcare, you get sick."*

At the time Naomi expressed serious concerns about the new law, especially as trans organisations had been excluded from this debate. "Without legal gender recognition for us, the national ID system traps us into this identity we no longer identify with."

When we spoke to Naomi again this year, she stressed that while the national ID systems has yet to be implemented, trans people remain impacted anyway by the current system where the multiple IDs they carry fail to reflect who they are.

Indeed, while having an ID that does not reflect your identity can aggravate feelings of gender dysphoria and negatively impact the mental health of trans people, there are other consequences too for trans Filipinos.

*"Even without a national ID, our experience is that when trans people attempt to access services or establishments where they are required to show an official document to ascertain our gender, we almost always end up being discriminated against. For example, if a trans woman applies for a gym membership, in spite of her female appearance or feminine gender presentation, she might be asked to use the male toilet, male changing room or male sauna or other facilities based on the gender indicated in a legal document such as a national ID. And we have seen this happen. There are also establishments that bar entry to trans women because of stereotypes or misconceptions about being trans and the ordeal usually begins by checking a trans woman's bona fide information facilitated by asking her to present an ID. And of course, we all know that when data like these are collected, marginalized communities are always the first to be put under stricter surveillance methods by the state. We know from experience elsewhere that when data are weaponized to crackdown on citizens suspected of crime or illegal behavior, the most vulnerable are the first ones to be victimized by the police state including the poor, trans people, or other populations deemed 'unacceptable' or 'undesirable' or 'unwanted' in society."*

Naomi, points as an example the "**Oplan X men**" scandal, that the Filipino Commission on

Human Rights is currently investigating. The city of Makati, in the Manila region, was targeting trans women and arresting them in the streets. The profiling and arrests were allegedly conducted to **"save them from exploitation and human trafficking."**

*"Having a national ID that will contain our legal name and gender that do not match our gender presentation will make us more vulnerable to abuses like this because it confirms our trans status under forced surveillance by the police,"*

The gap between someone's identity and someone's ID also affects their ability to receive healthcare. *"When a trans woman is admitted to a hospital and the doctor realises she has a male gender marker and male name on her ID, she will be automatically assigned to a male ward. So instead of enabling well-being, they end up experiencing more grief and misery when exposed to the healthcare system,"* explains Naomi.



**Case Study 2. France "When your ID does not match your identity, you end up at the mercy of everyone you interact you with: your employer, your professors, your landlord..."**

**In 2016, France passed a law** allowing trans people to change their gender without having to provide any medical documents to certify that they are indeed transgender. Until 2016, a person wishing to correct their birth certificate and ID had to provide a certificate from a psychiatrist and prove that they had undergone irreversible medical procedures, **i.e. sterilisation**, in order to be able to correct their ID.

While this change in the law is unquestionably a step in the right direction and a major

improvement compared to the previous context, in practice the legal procedure to correct an ID remains an obstacle course for many. Moreover, the ambiguous wording in the legal texts leave trans people at the mercy of the goodwill of the civil servants in charge of their case.

We spoke to two trans activists from France: the first is Anaïs, who is on the board of trustees of the organisation **OUTrans**, a Paris-based feminist organisation that offers support to trans people and also engages in advocacy at a national level. The other activist we spoke to is also a French trans activist working as part of a different organisation. He wishes to remain anonymous, so we will call him Joe.

While both Anaïs and Joe appreciate that the 2016 law has changed the lives of many trans people in France they also both acknowledge its limitations. Anaïs says:

*"The 2016 law liberated many things. Many people did not think they would one day be able to live their trans identity socially and legally. They would be discouraged by what they saw as the obstacle course from those that were pioneering and attempting to correct their ID. Now it's definitely much easier and it has become possible to do. The mere fact that we now have a chapter in the Civil Code about sex change – even if the term is not right – means that trans people have become real from a legal perspective while before they could only be found in court rulings. The problem is that the 2016 law made things easier but it did not go all the way."*

Joe and Anaïs both consider that one of the key issues with the current situation is that there are two separate procedures that trans people need to do in order to correct their ID. The first is the change of name. This is a procedure that is not specific to trans people. They have to follow the same process as any person that wishes to change their first name would. This is done at the town hall.

Already at this stage, the wording of the law is problematic. As Joe explained to us, people have to demonstrate a "prolonged and constant use of the name". This very request implies that people have to live for an extended period of times with ID documents that do not match their name. The other problem is that there is no clear definition of what prolonged means. Nor a list of documents they are expected to provide to prove that they indeed go by this name. Joe says:

*"There is a real lack of uniformity across France. When you change your name, you are expected to provide all sorts of documents proving that you have been using your name for a prolonged period and in different spheres of your life (professional, family, hobbies, friends). Yet those documents are not listed anywhere and so the treatment of those*

*requests hugely differ from one town hall to another. In Paris, it is generally OK, because people received specific trainings and it often works out well. Although even in Paris I have heard of people being requested a sworn statement from their friends that they indeed use the requested name."*

Anaïs highlights a different issue that trans people are confronted to when changing their name:

*"The person who is making the request has to prove the "legitimate interest" of their request and this is where things get complicated. While French law prohibits judging someone on their appearance, at the same time according to the law pertaining to the change of name part of proving the legitimate interest involves proving that the name you are choosing matches the gender of your appearance. So, on the one hand people cannot be judged on their appearance but on the other hand we ask employees from the civil registrar to assess the appearance of trans people. So, we see people feeling obliged to act as an archetype of their gender in order to make sure their request will go through."*

Anaïs also stresses that the lack of visibility of trans people in France contribute to the difficulty trans people are facing when going through this procedure that is not specific to trans people.

*"In France you do not have a strong visibility of trans people. It is not like in the US, where you have a Caitlyn Jenner that everyone knows and who has transitioned. There is no trans celebrity that everyone knows. So, when we speak about trans identity people do not always know what it is. And so if you are an employee from the civil registrar of a town hall and you spend your days issuing passports and one day you see a person coming in to change their name, it might very well be the first trans person you see in your life. You will have no idea what trans identity is, or what it implies and so your assumptions might be absurd or based on stereotypes, or your reaction might just be "I had no idea you could do this."*

*When a person comes to the decision to transition, they have spent enormous amount of time reflecting about themselves and when the procedures start they end up feeling like the whole world is against them. So you have on the one hand someone who feels that society is putting a spoke in their wheel and on the other hand someone who does not even know what trans identity is and who is unknowingly hampering the whole process. It is making life harder for both trans people and for civil registrar employees."*

Once the change of name has been approved, the birth certificate is automatically updated but for everything else (ID card, social security, taxes, diplomas...) it is up to the

individual to request the change for each document.

When this is completed, a trans person can then request their sex marker to be corrected on their ID documents. This time it requires a judiciary procedure that involves filing a request at a tribunal and potentially attending a court hearing. The procedure – which involves providing similar documents to the one requested for the name change – can take from six months to a year. While requesting any medical document is illegal, both Joe and Anaïs say their organisations have witnessed some tribunals with dubious practices, like in the city of Orleans, where only requests where people including medical documents have been accepted.

For both the name change and the correction of the sex marker there is a major risk. If the request is denied, appealing the decision implies the start of a legal battle, with legal fees to pay. Joe says this reality discourages trans people from trying to correct their ID and birth certificate early on in their transition for fear that their request could be rejected.

This reality means that trans people in France spend months to years with ID documents that do not reflect who they are.

Both Anaïs and Joe would like to see a system where the process is reduced to a single procedure done directly with a local authority, whereby trans people could change the details on their identity documents upon request – both the name and sex marker – all at once without having to go to court. Anaïs stresses that the court system in France is already overwhelmed and there is no need for the involvement of judges on this matter.

Joe points to Argentina as a model for how things should be done. He also highlights the absence of options for migrants in France who would like to have their name and ID recognised when their country of origin does not allow them to do so.

While France has normalised a system where trans people are expected to live months to years with an ID that does not match their identity, the consequences for trans people are very real. Joe points us to the example of someone whose change of name had been accepted but whose ID had not yet been updated; requesting a new ID is a procedure that can be lengthy in itself. The person tried to change their name on their **Carte Vitale**, the state social security card allowing immediate reimbursement for healthcare services. But the lack of an ID led to a situation in which the social security services suspected fraud and withdrew the person's ability to access their services altogether, thereby de facto banning them from accessing affordable health care.

Joe generally describes a life that leaves trans people at the mercy of any person they



interact with.

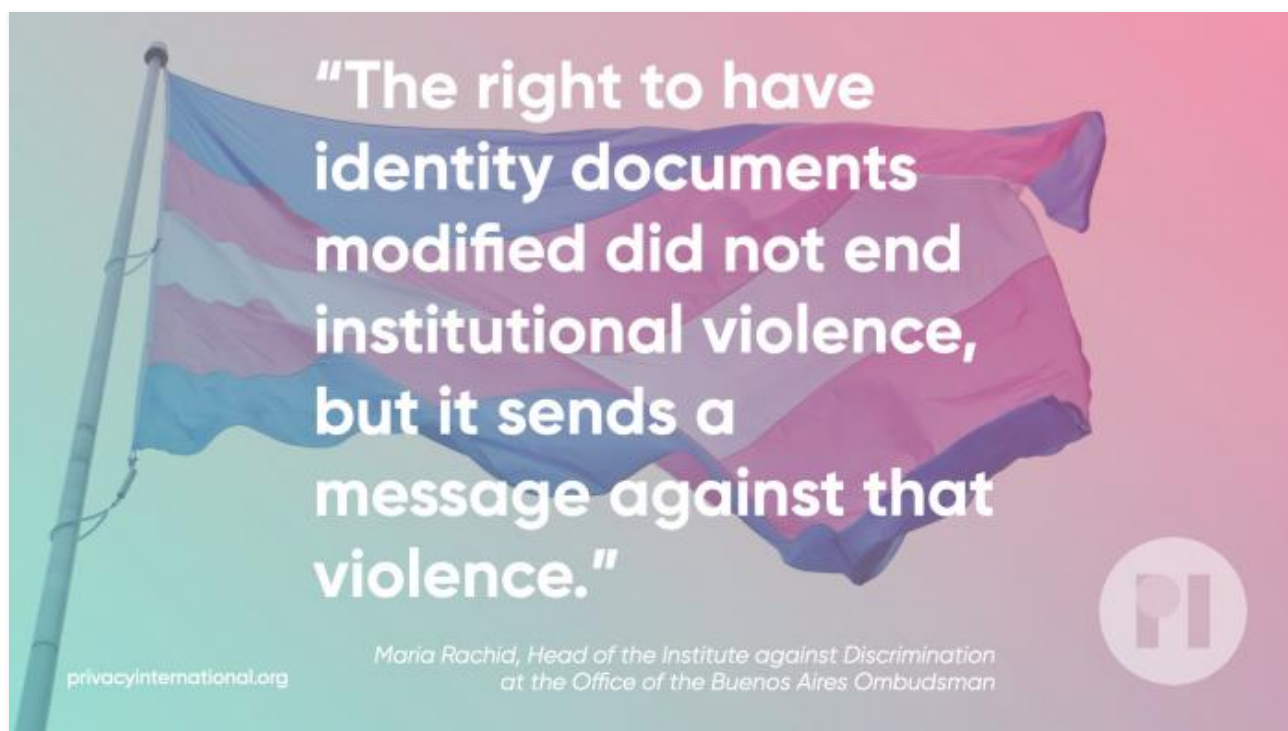
*"At university, I had a friend who completely passed as a man. Every time they would read student's names out loud at the start of every class to take the register, he would not respond to the call, in order to not out himself as trans. So, he would be marked as an absentee and he had to speak to every professor at the end of the class to explain the situation. You find yourself at the mercy of the good will of everyone you interact with: your professors, your employers...*

*You are exposed to discrimination in every field where you will be asked to present an ID. It's a source of discrimination in access to housing. Landlords may not want to rent a flat to a trans person. It can be a problem in recruitment because an employer might think it will be an issue they will have to handle, and they do not want to have to deal with this. You can be faced with transphobic doctors and risk receiving poor treatment. In the context of an ID check by the police you might be exposed to police violence or at the very least a longer ID check.*

*Even to pick up a parcel from a post office, things are more difficult, unless you receive everything under your legal name – and that is assuming that everyone even knows what your legal name is. It happened to me once: I had to negotiate for thirty minutes with a post office employee who was refusing to give me my parcel arguing that the name on my ID did not match the name on the parcel despite the fact that my last name was identical and I had the tracking number."*

When it comes to accessing healthcare, there are still issues awaiting trans people even after they have an ID that matches the gender they identify with. Indeed, the Carte Vitale features people gender through a code number ('1' for men and '2' for women). While the number can be changed once the sex marker on a person's ID has been changed, this bears consequences for trans people as well. For instance, trans men are no longer allowed to turn to gynaecologists even though they may still require their expertise. Likewise, trans women will no longer be entitled to a prostate exam even though they still have one.

This situation not only highlights the need for state services across every sector to be better informed and trained in responding to the specific needs of trans people but also the limitations and issues necessarily arise from a strictly binary system.



### **Case Study 3. Argentina "The right to have identity documents modified did not end institutional violence, but it sends a message against that violence."**

As the interview we conducted with Joe illustrates, Argentina is often held as a model when it comes to the right for trans people to correct their civil registry and identity documents. In May 2012, the Senate approved the **Gender Identity Law**. Article 1 of the law claims that everyone has the right:

- a) To the recognition of their gender identity;
- b) To the free development of their person according to their gender identity;
- c) To be treated according to their gender identity and, particularly, to be identified in that way in the documents proving their identity in terms of the first name/s, image and sex recorded there.

According to this law, in order to amend their ID, a person only needs to submit a request to the National Bureau of Vital Statistics and requesting the amendment of their birth certificate and new identity card with the same number as their already existing one. There is no additional procedure or requirement beyond the simple request.

We spoke to Maria Rachid, head of the Institute against Discrimination at the Office of the Buenos Aires Ombudsman and a former member of parliament in Argentina who drafted the Gender Identity Law. Rachid has long been an activist in LGBT circle and founded Federación Argentina LGBT, an umbrella organisation that brings together 150

Argentinian LGBTIQ organisations.

When she started drafting the law, Rachid first looked at the laws in other countries and noticed the worrying limitations of various legal frameworks.

*"Those laws required a medical diagnosis before a person could apply for a modification of their identity documents or undergo sex reassignment treatments or surgeries. One of the reasons for this was the medicalization of transgender identities. Those laws regarded transgender identities as some sort of pathology in which people are born in the wrong body, and which must therefore be corrected by means of a modification of their identity documents, surgeries and medical treatments.*

*As an organization [Federación Argentina LGBT], we believe that a person's identity is in no way the result of a pathology or a medical condition, and that people can define their identities themselves, without the need for any medical, legal, psychological or other authorization. We do not believe transgender people are sick, but rather that there is some sort of social phenomenon by which society assigns someone a specific sex and gender, and this defines many aspects of that person's life.*

*Thus, we believed that the modification of one's identity and the access to treatments and surgeries had to be based on a personal decision."*

Rachid worked on ensuring that the law would be there to facilitate people's procedures and prevent obstacles. They worked to draft the law in a way that would ensure that the process would happen through an administrative office – not a court, where the individual could face a rejection or legal fee – moreover they also included a "Human Treatment Clause" that states that even if a person does not wish to correct their name and gender on their ID they can still expect from any institution that they refer to them by their preferred name and gender upon request.

The law also takes into account the reality of migrants by stating that even in instances where a person's country of origin does not recognise their gender identity this is not an excuse for the Argentinian State to deny them the enjoyment of their fundamental rights. Therefore, migrants can apply to the National Immigration Office to correct any identity paper issued by the state of Argentina.

While Rachid acknowledges that the law did not solve all the risks that trans people are confronted with she is nonetheless confident that the law has helped trans people deal with specific institutional situations because the law sent a very clear and strong messages to all Argentinian institutions: everyone gets to define their gender identity and

their identity is valid.

*"The risks that transgender people were exposed to had to do with the institutional violence to which transgender people were permanently exposed. Now, the right to have identity documents modified did not end that violence, but it did help a lot in overcoming this situation. This is still a problem to this day, because the only means of survival available to many transgender persons is sex work, and this exposes them to permanent institutional violence. Nevertheless, the issue with their identity documents was a perfect excuse to direct institutional violence specifically at transgender people. There were even local statutes which penalized transgender identity in some Argentine provinces, all of which were of course repealed after the enactment of the Gender Identity Law.*

*Now, there were other types of institutional violence that originated in other institutions: hospitals, schools, etc. There was a permanent violence which was based on and originated in the failure to acknowledge transgender people's identity. When the right to have one's identity acknowledged in identity documents was recognized, it was not only the modification of those documents that was important, but also the message that the State sent through that modification. The message that identity is acknowledged has an effect which is much more powerful than the concrete change in an ID, as the fact that one's identity is respected by public or private institutions impacts our access to all types of rights: the right to health, the right to work, the right to justice.*

*The fact that institutions respect people's right to their own identity is a tool that can be used to eradicate violence from everyday life. At the very least, this sends a message against that violence, even if it still exists in society and we still have to work to eliminate it. The fact that institutions recognize people's identities is a message against the violence transgender people endure to this very day, and that message is a very important tool for transgender people."*

Maria mentions in particular the case of hospitals where trans people could face mistreatment for having an ID that did not match their identity and led many trans people **to not seek healthcare**, with very real consequences over their lives "All of this violence and negation of rights resulted in transgender people having an average lifespan of 35 to 40 years, which is half the average lifespan of the general population," she says.

Maria says the law has not faced any serious barriers when it comes to its implementation. The main issue has been that in some provinces, the process can be longer than in others.

There is more to be done for trans people to ensure their protection is comprehensive:

*"We are working on the bill for an "Integral Transgender Law" which establishes a series of public policies in various areas: health, education, housing, labour, etc. We believe this to be the next step: recognizing rights and adopting public policies to guarantee access to those rights. We are talking about a population that was expressly excluded for many years, so the State and society must make a major effort to revert that exclusion, and this requires very strong public policies which are ultimately temporary, of course, such as affirmative actions.*

*Our bill provides for a quota of transgender people in the public administration and incentives for companies that hire transgender people, as well as a grant for transgender persons over 40. Keep in mind that the average lifespan of a transgender person is 35 to 40 years, so those over 40 are truly survivors. They reach that age in very poor health and in most cases they have no formal education or work experience other than as sex workers, and at that age and in those conditions, in bad health, with no formal education and no work experience, it is very hard to make them a part of an active workforce, and that is why we believe they must be given a grant as compensation and to ensure their subsistence, given the conditions in which they were forced to live for so long. So, we believe transgender persons over 40 should be given a monthly grant."*

When asked what advice she would give to people and organisations lobbying for trans rights, she said she would advise them to follow the path of Uruguay. *"Uruguay has enacted a Comprehensive Transgender Law, which encompasses both our Gender Identity Law and the integral law we have been working on, which has not yet been enacted in Argentina."*

**Uruguay: In October 2018, Uruguay passed the Comprehensive Law for Transgender Persons. The law not only facilitate the right for transgender people to have their ID corrected but also offer them a package of additional rights. For instance, various government and state authorities are required to allocate 1% of their job opportunities to trans people. The law also allows children to correct their ID and receive hormonal treatment without the consent of their parents.**

She also reminds that there is more to gender than the male/female binary and that future laws should take this into consideration:

*"Under the Argentine law the State is required to acknowledge a person's self-perceived gender. At the beginning all changes were towards the 'male' or 'female' category, but now people are requesting other categories: 'non-binary', 'genderfluid', etc., and even though the law requires the State to record their self-perceived gender, there is still some*

*resistance from some institutions. I believe the new administration will change this, but up until a couple of months ago, with the previous administration, there were some national institutions which resisted using any category other than 'male' or 'female', even though the law in no way limits the potential categories. So, one suggestion might be that the law clearly state that there may be multiple categories and not only 'male' and 'female'."*

Finally, she insists that coordination across the state administration is key to facilitating the procedures of trans people:

*"I would advise them to make sure that the applicant is allowed to request that the office or agency which receives the application for a modification of identity documents automatically notify other institutions, so that they do not have to file for the same modification with their bank, the register of motor vehicles, the register of real property, etc. It would be great if the office or agency with which the application is first filed were able to directly notify all these other institutions, should the applicant request it."*

When asked about her opinion on ID documents that do not feature any gender or sex marker, as is now the case in the Netherlands, Maria says she sees it as a future to strive towards. However, she warns about the need to ensure affirmative action can be preserved in the short term, so that trans people can receive preferential benefits to compensate for the inequalities they are enduring.

*"Maybe it is necessary to have a gender identity law in place first, but the best scenario for us would be for identity documents and official forms not to include a person's sex. This does however pose a problem when it comes to affirmative actions, which we are trying to address in our bill. Even though, in our opinion, these categories were created by an oppressive system to ensure some people have more rights than others, and even though no legal distinction remains today, there are still some social distinctions and people in some of those original categories still face some disadvantages, wherefore the legal system should provide them with certain benefits to ensure equality."*

## **Conclusion – The laws that transform our society**

As we argued in our report **From Oppression to Liberation Reclaiming the Right to Privacy**, we can effectively say that the state enforces patriarchal perceptions of unchanging binary gender divisions through ID systems.

In order to be able to live their lives with dignity and access basic services, including healthcare, it is this very system that trans people have to battle and fight against.

While better laws do not “fix” societies and deep-rooted issues like transphobia which remain even in countries with the most progressive legal frameworks, as Maria Rachid of Argentina explained in her interview, they can send a very strong signal to institutions and society at large. Thus, a legal framework that allows trans people to correct their ID with very limited administrative procedure and with the certainty that their request will be granted not only protects trans people and their right to have an ID that matches their actual identity. It also sends a message to society at large that exclusion and intolerance towards trans people will not be tolerated by the state, and therefore it should not be tolerated within our societies.

Considering the discrimination and exclusion trans people face, it is essential to have a legal framework allowing and facilitation gender recognition, as well as laws that are there to specifically provide extra support to trans people. But further, we also need as a society to ask ourselves what we want our civil registration documents like birth certificates, as well as IDs, to be like. If we accept that these documents and systems contribute to shaping the gender binary and gender norms, we need to think about the kind of society we want and how our systems and documents will contribute to shaping it.

And while this report focused on the experience of trans people who identified within traditional gender binaries, many others would benefit from gender-free ID. For Anaïs, such a change would also provide recognition for non-binary people:

*“We talk about binary trans people, but we are not discussing the whole question of non-binary trans people. It is very clear that if the gender mention was to disappear from anything administrative, we would solve a lot of issues. My gender belongs to me. It does not belong to the state, the state has nothing to do with my gender. We are 100% in favour of removing gender altogether and France is starting to go in that direction. Driving licenses, for instance, no longer have a sex marker.*

*Until recently the legal history of France was going in the direction of removing gender in every law that distinguished between men and women. The only thing that has changed this direction are laws encouraging gender equality because when you have laws guaranteeing equal access to men and women to run in certain elections, or equal access to public jobs or to managerial positions you force the state to identify gender in order to guaranty equality. Gender is now used for affirmative action while for us trans people it would be easier to see it disappear altogether.”*

Issues of discrimination and inequality cannot be ignored, and we, as an organisation, understand the importance of having data that accurately relays that, as well as

mechanism of affirmative action to offer a form of redress. But we are confident that affirmative action can be promoted and perpetuated without relying on a sex marker on one's IDs.

Yet, as we work on shaping the future of ID systems and the future of society at large, we need to make sure gender stays in its rightful place. Gender is a societal construct. It is something we should get to define for ourselves, it is fluid for some of us and may change over the course of our lives or be multiple all at once. As such it is not something for the states to impose on us and it is certainly not a relevant marker to identify someone for any state-related purpose. In other words, gender is for our personal and self-defined identity, not our IDs.

And with gender marker removed from our identification documents, we open the door to a world that will be freer for all: there will be less pressure on parents to assign a gender to their child at birth, less pressure on all of us to define ourselves or match certain expectations, or to comply with norms and roles historically associated with the gender we have been assigned to by society.

This is an essential development as we strive for a world where we are all equal. We believe this is what a world where we are free to be human would look like.

Este informe está disponible en **español**.

## **TAGS**

### **OUR CAMPAIGN**

Demanding identity systems on our terms

### **LEARN MORE**

LGBTIQ+

Gender

ID Systems

Identity

### **OUR FIGHT**

ID, Identity and Identification

## **RELATED CONTENT**





NEWS &amp; ANALYSIS

## The Clearview/Ukraine partnership - How surveillance companies exploit war

Clearview announced it will offer its surveillance tech to Ukraine. It seems no human tragedy is off-limits to surveillance companies looking to sanitise their image.

**CONTINUE READING**



EXPLAINER

## Electronic monitoring using GPS tags: a tech primer

Electronic tags have been a key part of criminal justice for many years throughout the world. As traditional radio-frequency tags are replaced by GPS ankle tags, we examine how these different technologies work and the seismic shift that will result from 24/7 location monitoring and data analytics, enabled by GPS tags.

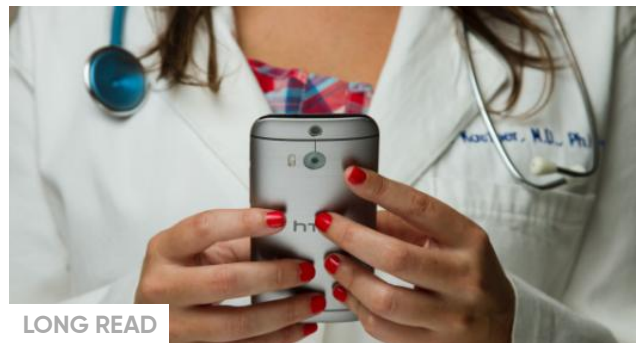
**CONTINUE READING**



NEWS &amp; ANALYSIS

## Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba

In this article we provide background on the initial challenge of the Huduma Namba and subsequent developments which led to an important ruling of the High Court of Kenya



LONG READ

## The use of SMS in the delivery of reproductive and maternal healthcare

Short Message Services (SMS) are being used in MHealth initiatives which aim to deliver crucial information to expecting and new mothers. But there are concerns that

on the retrospective effect of the Data Protection Act as we reflect on its wider implications for the governance and regulation of digital ID systems. **CONTINUE**

**READING**

there is limited transparency about numerous aspects of SMS health services, and how the data is being processed, by whom and in accordance to what safeguards. **CONTINUE READING**

## GET INVOLVED

**ACT WITH US** ● **DONATE** ● **JOIN**

## NEWSLETTER

Click here to sign-up to our mailing-list!

---

## FOLLOW US

## NAVIGATION

**NEWS**

**ACT**

**CAMPAIGNS**

**LEARN**

**IMPACT**

**ABOUT**

**DONATE**

**HOW WE FIGHT**

## **ABOUT**

## **PRIVACY**

## **RESOURCES**

## **CONTACT US**

62 Britton Street,  
London, EC1M 5UY  
UK

Charity Registration No: 1147471

[Click here to contact us.](#)

[Click here for media and press enquiries.](#)



## General Assembly

Distr.: General  
11 October 2019

Original: English

---

### Seventy-fourth session

Agenda item 70 (b)

**Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms**

### **Extreme poverty and human rights\***

#### **Note by the Secretary-General**

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on extreme poverty and human rights, Philip Alston, submitted in accordance with Human Rights Council resolution [35/19](#).

---

\* The present report was submitted after the deadline in order to reflect the most recent developments.



---

## Report of the Special Rapporteur on extreme poverty and human rights

### *Summary*

The digital welfare state is either already a reality or emerging in many countries across the globe. In these states, systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. In the present report, the irresistible attractions for Governments to move in this direction are acknowledged, but the grave risk of stumbling, zombie-like, into a digital welfare dystopia is highlighted. It is argued that big technology companies (frequently referred to as “big tech”) operate in an almost human rights-free zone, and that this is especially problematic when the private sector is taking a leading role in designing, constructing and even operating significant parts of the digital welfare state. It is recommended in the report that, instead of obsessing about fraud, cost savings, sanctions, and market-driven definitions of efficiency, the starting point should be on how welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged.

---

## Contents

	<i>Page</i>
I. Introduction .....	4
II. Uses of digital technologies in the welfare state .....	6
A. Identity verification .....	6
B. Eligibility assessment .....	9
C. Welfare benefit calculation and payments .....	9
D. Fraud prevention and detection .....	10
E. Risk scoring and need classification .....	10
F. Communication between welfare authorities and beneficiaries .....	11
III. Making digital technologies work for social protection .....	12
A. Taking human rights seriously and regulating accordingly .....	12
B. Ensuring legality and transparency .....	14
C. Promoting digital equality .....	15
D. Protecting economic and social rights in the digital welfare state .....	16
E. Protecting civil and political rights in the digital welfare state .....	18
F. Resisting the inevitability of a digital-only future .....	19
G. Role of the private sector .....	20
H. Accountability mechanisms .....	21
IV. Conclusions .....	21

## I. Introduction<sup>1</sup>

1. The era of digital governance is upon us. In high- and middle-income countries, electronic voting, technology-driven surveillance and control, including through facial recognition programmes, algorithm-based predictive policing, the digitization of justice and immigration systems, online submission of tax returns and payments and many other forms of electronic interactions between citizens and different levels of government are becoming the norm. In lower-income countries, national systems of biometric identification are laying the foundations for comparable developments, especially in systems to provide social protection, or “welfare”, to use a shorthand term.<sup>2</sup>

2. Invariably, improved welfare provision, along with enhanced security, is one of the principal goals invoked to justify the deep societal transformations and vast expenditure that are involved in moving the entire population of a country not just on to a national unique biometric identity card system but also into linked centralized systems providing a wide array of government services and goods ranging from food and education to health care and special services for the ageing and for persons with disabilities.

3. The result is the emergence of the “digital welfare state” in many countries across the globe.<sup>3</sup> In these countries, systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. The process is commonly referred to as “digital transformation”, but this somewhat neutral term should not be permitted to conceal the revolutionary, politically driven character of many such innovations. Commentators have predicted “a future in which government agencies could effectively make law by robot”,<sup>4</sup> and it is clear that new forms of governance are emerging which rely significantly on the processing of vast quantities of digital data from all available sources, use predictive analytics to foresee risk, automate decision-making and remove discretion from human decision makers. In such a world, citizens become ever more visible to their Governments, but not the other way around.<sup>5</sup>

4. Welfare is an attractive entry point not just because it takes up a major share of the national budget or affects such a large proportion of the population but because digitization can be presented as an essentially benign initiative. Thus, for example, the Government Transformation Strategy of the United Kingdom of Great Britain and Northern Ireland proclaims that it is intended to transform the relationship between citizens and the State, putting more power in the hands of citizens and being more responsive to their needs. The core values of the Unique Identification Authority of India include facilitating good governance, integrity, inclusive nation-building, a collaborative approach, excellence in services and transparency and openness.

5. In other words, the embrace of the digital welfare state is presented as an altruistic and noble enterprise designed to ensure that citizens benefit from new

---

<sup>1</sup> The present report has been prepared in close collaboration with Christiaan van Veen, Director of the Digital Welfare States and Human Rights Project at New York University School of Law.

<sup>2</sup> While “welfare” is often used as a pejorative term, it is used in a positive sense in the present report and is synonymous with the goal of social protection as reflected in the Social Protection Floor Initiative and comparable approaches. See David Garland, *The Welfare State: A Very Short Introduction* (Oxford, Oxford University Press, 2016).

<sup>3</sup> Philip Alston and Christiaan van Veen, “How Britain’s welfare state has been taken over by shadowy tech consultants”, *Guardian*, 27 June 2019.

<sup>4</sup> Cary Coglianese and David Lehr, “Regulating by robot: administrative decision making in the machine-learning era”, *Georgetown Law Journal*, vol. 105, No. 5 (July 2017), p. 1147.

<sup>5</sup> See Foucault’s description of panoptic systems, in which those put under surveillance are “seen, without ever seeing” (Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York, Pantheon Books, 1977), p. 202).

technologies, experience more efficient governance and enjoy higher levels of well-being. Often, however, the digitization of welfare systems has been accompanied by deep reductions in the overall welfare budget, a narrowing of the beneficiary pool, the elimination of some services, the introduction of demanding and intrusive forms of conditionality, the pursuit of behavioural modification goals, the imposition of stronger sanctions regimes and a complete reversal of the traditional notion that the State should be accountable to the individual.

6. These other outcomes are promoted in the name of efficiency, targeting, incentivizing work, rooting out fraud, strengthening responsibility, encouraging individual autonomy and responding to the imperatives of fiscal consolidation. Through the invocation of what are often ideologically charged terms, neoliberal economic policies are seamlessly blended into what are presented as cutting-edge welfare reforms, which in turn are often facilitated, justified and shielded by new digital technologies. Although the latter are presented as being “scientific” and neutral, they can reflect values and assumptions that are far removed from, and may be antithetical to, the principles of human rights. In addition, because of the relative deprivation and powerlessness of many welfare recipients, conditions, demands and forms of intrusiveness are imposed that would never be accepted if they were piloted in programmes applicable to better-off members of the community instead.

7. Despite the enormous stakes involved, not just for millions of individuals but for societies as a whole, these issues have, with a few notable exceptions,<sup>6</sup> garnered remarkably little attention. The mainstream technology community has been guided by official preoccupations with efficiency, budget savings and fraud detection. The welfare community has tended to see the technological dimensions as separate from policy developments, rather than as being integrally linked. Lastly, those in the human rights community concerned with technology have understandably been focused instead on concerns such as the emergence of the surveillance state, the potentially fatal undermining of privacy, the highly discriminatory impact of many algorithms and the consequences of the emerging regime of surveillance capitalism.

8. However, the threat of a digital dystopia is especially significant in relation to the emerging digital welfare state. The present report is aimed at redressing the neglect of these issues to date by providing a systematic account of the ways in which digital technologies are used in the welfare state and of their implications for human rights. It concludes with a call for the regulation of digital technologies, including artificial intelligence, to ensure compliance with human rights and for a rethinking of the positive ways in which the digital welfare state could be a force for the achievement of vastly improved systems of social protection.

9. The report builds in part on reports by the Special Rapporteur on visits to the United States of America in 2017 ([A/HRC/38/33/Add.1](#)) and the United Kingdom in 2018 ([A/HRC/41/39/Add.1](#)), in which attention was drawn to the increasing use of digital technologies in social protection systems. In preparing the present report, the Special Rapporteur consulted representatives of various digital rights groups, leading scholars and other stakeholders, first in a meeting hosted by the Digital Freedom Fund in Berlin in February 2019, and then at a meeting sponsored by the Center for Information Technology Policy at Princeton University, United States, in April 2019. In addition, a formal call for contributions resulted in some 60 submissions from 22 Governments, as well as international and national civil society organizations,

---

<sup>6</sup> For pioneering work on the impact of digital technologies on the welfare state in the United States, especially on the poorest individuals in the system, see Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York, St Martin’s Press, 2018). See also Cathy O’Neil, *Weapons of Math Destruction* (New York, Crown, 2016); and Khiara Bridges, *The Poverty of Privacy Rights* (Stanford, California, Stanford University Press, 2017).



national human rights institutions, academics and individuals in 34 countries.<sup>7</sup> While it is impossible to do justice to these rich and detailed submissions in such a necessarily brief report, the Special Rapporteur has made them available electronically<sup>8</sup> and will continue analysing them in the context of his team's ongoing work on the digital welfare state.<sup>9</sup>

## II. Uses of digital technologies in the welfare state

10. From the many submissions received, and on the basis of various case studies addressed in the literature, it is possible to distinguish various ways, and different stages in the welfare context, in which digital innovation has been used most prominently.

### A. Identity verification

11. Establishing every person's legal identity, including through birth registration, by 2030 is target 16.9 of the Sustainable Development Goals. A verifiable identity is essential for applying for benefits, establishing entitlements, receiving benefits and appealing against denial of benefits. For the Government or other provider, a verifiable identity avoids duplication and fraud, facilitates accurate targeting and enhances efficiency. Traditionally, paper and/or plastic documents have been used in forms such as birth certificates, identity cards and passports. These systems function reasonably well in most of the global North, although 21 million adults in the United States do not have government-issued photo identification.<sup>10</sup> In the global South, 502 million people in sub-Saharan Africa and 357 million people in South Asia lack official identification.<sup>11</sup> In Liberia, for example, birth registration stands at only 5 per cent and national identity cards were not introduced until 2015.<sup>12</sup>

12. In response, the World Bank, regional development organizations and bilateral donors have launched new programmes to promote access to identity documents. In particular, the World Bank's Identification for Development (ID4D) campaign has focused heavily on promoting digital technologies. The role of digital technology in identity documents is set out in the "Principles on identification for sustainable development: toward the digital age", which were facilitated by the World Bank and the Center for Global Development and have been widely endorsed, including by MasterCard.

13. It is acknowledged in the Principles that both advantages and disadvantages are involved. On the positive side, it is claimed that digital technology can create huge savings for citizens, Governments and businesses by reducing transaction costs, increasing efficiency and driving innovation in service delivery, particularly to the poorest and most disadvantaged groups in society. It is also noted that digital identity systems can also improve governance, boost financial inclusion, reduce gender

<sup>7</sup> Argentina, Australia, Austria, Azerbaijan, Brazil, Chile, Croatia, Egypt, El Salvador, Estonia, Germany, Greece, Guatemala, India, Italy, Ireland, Kazakhstan, Lebanon, Mexico, Nicaragua, Nigeria, Netherlands, New Zealand, Oman, Pakistan, Philippines, Poland, Qatar, Russian Federation, Senegal, South Africa, Switzerland, United Kingdom and United States.

<sup>8</sup> [www.ohchr.org/EN/Issues/Poverty/Pages/SubmissionsGADigitalTechnology.aspx](http://www.ohchr.org/EN/Issues/Poverty/Pages/SubmissionsGADigitalTechnology.aspx).

<sup>9</sup> <https://chrgj.org/people/christiaan-van-veen/>.

<sup>10</sup> Wendy R. Weiser and Lawrence Norden, *Voting Law Changes in 2012* (New York, Brennan Center for Justice at New York University School of Law, 2011), p. 2.

<sup>11</sup> United States Agency for International Development, *Identity in a Digital Age: Infrastructure for Inclusive Development* (2017), p. 8.

<sup>12</sup> Bronwen Manby, *Citizenship in Africa: The Law of Belonging* (Oxford, Hart Publishing, 2018), p. 3.

inequalities by empowering women and girls, and increase access to health services and social safety nets for the poor (p. 5).

14. However, in addition to this impressive and by now familiar sales pitch, possible risks are recognized in the Principles, and similar documents.<sup>13</sup> Those risks range from political backlash to concerns over privacy, security and cybersecurity. Solutions for dealing with those risks are often technological or take the form of soft law norms. The United States Agency for International Development has called for open source solutions and the development of good practices for data privacy to resolve the relevant problems.<sup>14</sup> While the “Principles on identification for sustainable development” contain references to human rights principles such as article 7 of the Convention on the Rights of the Child, emphasis is placed primarily on the need to create an interoperable platform using open standards, and protecting privacy through system design.

15. The world’s largest biometric identification system is Aadhaar in India. Residents are issued a 12-digit unique identifying number and the system contains both demographic and biometric information, including an iris scan, a photograph and fingerprints. It is used to verify the identity of recipients of benefits and subsidies and is now mandatory to access those social rights. It was first introduced in 2009 and now covers more than 1.2 billion people.<sup>15</sup> It has been enthusiastically endorsed by the international development community.<sup>16</sup> The World Bank has praised it for overcoming complex information problems, thereby helping willing Governments to promote the inclusion of disadvantaged groups,<sup>17</sup> and has encouraged other Governments to learn from the experience.<sup>18</sup> Over 20 countries are reported to have expressed an interest in emulating Aadhaar.<sup>19</sup>

16. It nevertheless remains controversial domestically. Critics of Aadhaar have reportedly been harassed and surveilled,<sup>20</sup> and the scheme has been criticized for collecting biometric information unnecessarily, severe shortcomings in legislative oversight, function creep, facilitating surveillance and other intrusions into privacy, exacerbating cybersecurity issues and creating barriers to accessing a range of social rights.<sup>21</sup>

17. In 2018, the Supreme Court of India, in a 1,448-page landmark ruling, upheld the constitutionality of Aadhaar, albeit with some caveats. The court appeared to view the use of biometric identification technology in the context of providing welfare benefits as being legitimate, proportional and even inevitable. In a welfare state, Aadhaar’s aim of ensuring that benefits reach the intended beneficiary was “naturally a legitimate State aim”.<sup>22</sup> In balancing the rights to social security and privacy, the

<sup>13</sup> *Identity in a Digital Age*; and McKinsey Global Institute, “Digital identification: a key to inclusive growth” (January 2019).

<sup>14</sup> *Identity in a Digital Age*.

<sup>15</sup> Rahul Tripathi, “National population register to include Aadhaar details”, *Economic Times*, 5 August 2019.

<sup>16</sup> Jeanette Rodrigues, “India ID program wins World Bank praise despite ‘Big Brother’ fears”, *Bloomberg*, 16 March 2017.

<sup>17</sup> World Bank, *World Development Report 2016: Digital Dividends* (Washington, D.C., 2016), p. 2.

<sup>18</sup> Amrit Raj and Upasana Jain, “Aadhaar goes global, finds takers in Russia and Africa”, *Live Mint*, 9 July 2016.

<sup>19</sup> Jayadevan PK, “India’s latest export: 20 countries interested in Aadhaar, India Stack”, *Factory Daily*, 10 January 2018.

<sup>20</sup> Rahul Bhatia, “Critics of India’s ID card project say they have been harassed, put under surveillance”, *Reuters*, 13 February 2018.

<sup>21</sup> Submission to the Special Rapporteur by the Centre for Communication Governance at the National Law University, Delhi.

<sup>22</sup> Supreme Court of India, *Justice K.S. Puttaswamy and Another v. Union of India and Others*, Writ Petition (Civil) No. 494 of 2012, p. 341.

Court held that registering biometric data represented a minimal inroad into privacy rights<sup>23</sup> and went so far as to characterize Aadhaar as a vital tool for ensuring good governance in a social welfare state.<sup>24</sup> However, the Supreme Court's ruling has apparently not put an end to the controversy surrounding the scheme.<sup>25</sup>

18. In 2019, Kenya required all of its citizens, including those living abroad, and all foreign nationals and refugees in the country above the age of 6 to obtain a national identification card in order to access government services, including welfare benefits. This involved providing biometric data including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA in digital form. In response to a case claiming that the National Integrated Identity Management System (NIIMS), also known as Huduma Namba (Swahili for "service number"), violated the rights to privacy, equality, non-discrimination and public participation, the High Court issued an interim order allowing the registration process to continue, but on a voluntary basis and on the basis that the disbursement of government services and benefits could not be made conditional on participation. Subsequently, registration has proceeded apace: nearly two thirds of the population has been registered,<sup>26</sup> and the Government is reportedly threatening to withdraw unregistered individuals' access to benefits and the right to vote.<sup>27</sup>

19. In South Africa, the South African Social Security Agency distributes non-contributory and means-tested social grants, including grants for child support, for pensioners and for persons with disabilities, to about one third of the population.<sup>28</sup> In 2012, the Agency contracted the company Cash Paymaster Services, a subsidiary of Net1, to deliver the grants.<sup>29</sup> Cash Paymaster Services registered beneficiaries by collecting their biometric information (fingerprints and, originally, voice recordings) and beneficiaries were issued MasterCard debit cards with biometric functionality and a linked bank account by Net1 and Grindrod Bank in association with the Agency.<sup>30</sup> After much controversy surrounding the tender to Cash Paymaster Services, the fees charged by the company, deductions made to social grants on these accounts and privacy concerns surrounding the processing of cardholder data, the Agency changed providers in 2018 by entering into a partnership with the South African Post Office. The Agency and the Post Office will provide new biometric cards. The change from Cash Paymaster Services to the Post Office has been complex and has led to questions about effective access to social grants by beneficiaries in South Africa.<sup>31</sup>

---

<sup>23</sup> Ibid., p. 377.

<sup>24</sup> Ibid., p. 553.

<sup>25</sup> Vindu Goel, "India's top court limits sweep of biometric ID programme", *New York Times*, 26 September 2018.

<sup>26</sup> Submission to the Special Rapporteur by Amnesty International.

<sup>27</sup> Moses Nyamori, "No healthcare, voting without Huduma Namba, bill proposes", *Standard Digital*, 18 July 2019.

<sup>28</sup> Mary Jan Mphahlele, "#BUDGET2019: social grants to increase", *Diamond Fields Advertiser*, 20 February 2019.

<sup>29</sup> Submission to the Special Rapporteur by Black Sash.

<sup>30</sup> Mastercard, "More than 2.5 million Mastercard debit cards issued to social welfare beneficiaries in South Africa", press release, 30 July 2012.

<sup>31</sup> Ray Mahlaka, "Post office set to take over cash payments from CPS", *The Citizen*, 4 June 2018.

20. Many other examples could be given of countries using or exploring digital identity systems, including Argentina,<sup>32</sup> Bangladesh,<sup>33</sup> Chile,<sup>34</sup> Ireland,<sup>35</sup> Jamaica,<sup>36</sup> Malaysia,<sup>37</sup> the Philippines<sup>38</sup> and the United States.<sup>39</sup>

## B. Eligibility assessment

21. Automated programmes are increasingly used to assess eligibility in many countries. An especially instructive case was the automation of eligibility decisions in Ontario, Canada, in 2014 through the Social Assistance Management System, which was based on Cúram, a customizable, off-the-shelf IBM software package also used in welfare programmes in Australia, Germany, New Zealand and the United States.<sup>40</sup>

22. In 2015, the Auditor-General of Ontario reported on 1,132 cases of errors with eligibility determinations and payment amounts under the Social Assistance Management System, involving about 140 million Canadian dollars. The total expenditure on the System by late 2015 was 290 million Canadian dollars.<sup>41</sup> The new system reportedly led caseworkers to resort to subterfuge to ensure that beneficiaries were fairly treated; it also made decisions very difficult to understand and created significant additional work for staff.<sup>42</sup>

## C. Welfare benefit calculation and payments

23. The calculation and payment of benefits is increasingly done using digital technologies without the involvement of caseworkers and other human decision makers. While such systems offer many potential advantages, the Special Rapporteur also received information about prominent examples of system errors or failures that had generated major problems for large numbers of beneficiaries. These included the automated debt-raising and recovery system (“robo-debt”) in Australia,<sup>43</sup> the Real Time Information system in the United Kingdom<sup>44</sup> and the Social Assistance Management System in Canada.

24. Electronic payment cards or debit cards are increasingly being issued to welfare recipients. Information provided to the Special Rapporteur in relation to such programmes in Australia, New Zealand and South Africa reveal very similar

<sup>32</sup> Submission to the Special Rapporteur by the Government of Argentina.

<sup>33</sup> Privacy International, “Bangladesh: biometrics needed to access welfare payment”, 2 May 2017.

<sup>34</sup> In Chile, facial recognition technology is used to deliver school meals (submission to the Special Rapporteur by Privacy International).

<sup>35</sup> Submission to the Special Rapporteur by the Government of Ireland.

<sup>36</sup> See the National Identification System webpage (<https://opm.gov.jm/portfolios/national-identification-system>).

<sup>37</sup> Alita Sharon, “Malaysia’s digital ID project to be finalized by 2019”, Open Gov, 10 June 2019.

<sup>38</sup> See the Philippine Identification System webpage (<https://psa.gov.ph/philsys>).

<sup>39</sup> For example, the use of digital technologies in the CalWORKs programme in California (submission to the Special Rapporteur by Human Rights Watch).

<sup>40</sup> Submission to the Special Rapporteur by Human Rights Watch.

<sup>41</sup> Canada, Office of the Auditor General of Ontario, *Annual Report 2015* (Toronto, Ontario, Queen’s Printer for Ontario, 2015), p. 475.

<sup>42</sup> Jennifer Raso, “Displacement as regulation: new regulatory technologies and front-line decision-making in Ontario works”, *Canadian Journal of Law and Society*, vol. 32, No. 1 (2017), pp. 75–95.

<sup>43</sup> Terry Carney, “The new digital future for welfare: debts without legal proofs or moral authority?”, UNSW Law Journal Forum (March 2018); Richard Glenn, *Centrelink’s Automated Debt Raising and Recovery System* (2017), pp. 7–8; and submission to the Special Rapporteur by the Castan Centre for Human Rights Law at Monash University.

<sup>44</sup> Philip Alston, Special Rapporteur on extreme poverty and human rights, statement on visit to the United Kingdom of Great Britain and Northern Ireland, 16 November 2018.

problems. First, beneficiaries often face difficulties accessing and fully utilizing their right to social security.<sup>45</sup> Second, when such cards are clearly recognizable as welfare-related, users have expressed feelings of disempowerment, embarrassment and shame,<sup>46</sup> a problem exacerbated when the users come from communities long accustomed to exclusion.<sup>47</sup> Third, electronic cards enable monitoring and surveillance of behavioural data by welfare authorities and private actors, thus raising important human rights concerns.<sup>48</sup>

25. Moreover, the outsourcing of the issuance and administration of electronic cards to private companies has led to problems such as users being encouraged to pay for commercial financial products and the imposition of user fees.<sup>49</sup> More generally, the ethos surrounding such cards has often reflected stereotypes such as the financial untrustworthiness and irrationality of those living in poverty.

#### D. Fraud prevention and detection

26. Fraud and error in welfare systems can potentially involve very large sums of money and have long been a major concern for Governments. It is thus unsurprising that many of the digital welfare systems that have been introduced have been designed with a particular emphasis on the capacity to match data from different sources in order to expose deception and irregularities on the part of welfare applicants. Nevertheless, evidence from country missions undertaken by the Special Rapporteur,<sup>50</sup> along with other cases examined,<sup>51</sup> suggests that the magnitude of these problems is frequently overstated and that there is sometimes a wholly disproportionate focus on this particular dimension of the complex welfare equation. Images of supposedly wholly undeserving individuals receiving large government welfare payments, such as Ronald Reagan's "welfare queen" trope, have long been used by conservative politicians to discredit the very concept of social protection. The risk is that the digital welfare state provides endless possibilities for taking surveillance and intrusion to new and deeply problematic heights.

#### E. Risk scoring and need classification

27. Risk calculation is inevitably at the heart of the design of welfare systems, and digital technologies can achieve very high levels of sophistication in this regard. In addition to fraud detection and prevention, child protection has been a major focus in this area, as illustrated by examples from countries such as Denmark,<sup>52</sup> New Zealand,<sup>53</sup>

<sup>45</sup> Submission to the Special Rapporteur by Shelley Bielefeld (Griffith University).

<sup>46</sup> Submission to the Special Rapporteur by Nijole Naujokas.

<sup>47</sup> Melissa Davey, "'Ration days again': cashless welfare card ignites shame", *Guardian*, 8 January 2017.

<sup>48</sup> Submission to the Special Rapporteur by Louise Humpage (University of Auckland).

<sup>49</sup> Andries du Toit, "The real risks behind South Africa's social grant payment crisis", *The Conversation*, 20 February 2017.

<sup>50</sup> See, for example, Alston, statement on visit to the United Kingdom.

<sup>51</sup> For example, the case on system risk indication from the Netherlands (see Philip Alston, Special Rapporteur on extreme poverty and human rights, brief as amicus curiae before the District Court of the Hague on the case of *NJCM c.s./De Staat der Nederlanden (SyRI)*, case No. C/09/550982/HA ZA 18/388, September 2019).

<sup>52</sup> Jacob Mchangama and Hin-Yan Liu, "The welfare state is committing suicide by artificial intelligence", *Foreign Policy*, 25 December 2018.

<sup>53</sup> Philip Gillingham, "Predictive risk modelling to prevent child maltreatment: insights and implications from Aotearoa/New Zealand", *Journal of Public Child Welfare*, vol. 11, No. 2 (2017).

the United Kingdom<sup>54</sup> and the United States.<sup>55</sup> Governments have also applied these techniques to determine whether unemployment assistance will be provided and at what level. A prominent such scheme in Poland was held unconstitutional,<sup>56</sup> but an algorithm-based system in Austria continues to categorize unemployed jobseekers to determine the support they will receive from government job centres.<sup>57</sup>

28. Many other areas of the welfare state will also be affected by new technologies used to score risks and classify needs.<sup>58</sup> While such approaches offer many advantages, it is also important to take into account the problems that can arise. First, there are many issues raised by determining an individual's rights on the basis of predictions derived from the behaviour of a general population group.<sup>59</sup> Second, the functioning of the technologies and how they arrive at a certain score or classification are often secret, thus making it difficult to hold Governments and private actors to account for potential rights violations.<sup>60</sup> Third, risk-scoring and need categorization can reinforce or exacerbate existing inequalities and discrimination.<sup>61</sup>

## F. Communication between welfare authorities and beneficiaries

29. Communication that previously took place in person, by phone or by letter is increasingly being replaced by online applications and interactions. In various submissions to the Special Rapporteur, problems were cited with the Universal Credit system in the United Kingdom, including difficulties linked to a lack of Internet access and/or digital skills<sup>62</sup> and the extent to which online portals can create confusion and obfuscate legal decisions, thereby undermining the right of claimants to understand and appeal decisions affecting their social rights.<sup>63</sup> Similar issues have also been raised in relation to other countries, including Australia<sup>64</sup> and Greece.<sup>65</sup>

30. Another problem is the likelihood, once the entire process of applying and maintaining benefits is moved online, of the situation inviting further digital

<sup>54</sup> Niamh McIntryre and David Pegg, "Councils use 377,000 people's data in efforts to predict child abuse", *Guardian*, 16 September 2018; and Alex Turner, "County becomes latest authority to trial predictive algorithms in children's social work", *Community Care*, 14 June 2019.

<sup>55</sup> Eubanks, *Automating Inequality*; Alexandra Chouldechova and others, "A case study of algorithm-assisted decision making in child maltreatment hotline screening decisions", *Proceedings of Machine Learning Research*, vol. 81 (2018), pp. 1–5; and Dan Hurley, "Can an algorithm tell when kids are in danger?", *New York Times*, 2 January 2018.

<sup>56</sup> Supreme Court of Poland, case No. K 53/16, 6 June 2018.

<sup>57</sup> Submission to the Special Rapporteur by EpicenterWorks.

<sup>58</sup> See, for example, Lina Dencik and others, *Data Scores as Governance: Investigating Uses of Citizen Scoring in Public Services* (Data Justice Lab, Cardiff University, and Open Society Foundations, 2018).

<sup>59</sup> Household-level and individual-level data rely on a fundamental personalization of risk, attaching risk factors to individual characteristics and behaviour that can lead to individualized responses to social ills being privileged over collective and structural responses, such as issues of inequality, poverty or racism (submission to the Special Rapporteur by the Data Justice Lab at Cardiff University); and submission to the Special Rapporteur by Paul Henman (University of Queensland).

<sup>60</sup> Submission to the Special Rapporteur by Jędrzej Niklas and Seeta Peña Gangadharan (London School of Economics and Political Science).

<sup>61</sup> "Human bias is built in to the predictive risk model." (Virginia Eubanks, "A child abuse prediction model fails poor families", *Wired*, 15 January 2018).

<sup>62</sup> Submissions to the Special Rapporteur by the Scottish Council for Voluntary Organisations and Citizens Advice Scotland.

<sup>63</sup> Submission to the Special Rapporteur by the Child Poverty Action Group.

<sup>64</sup> Australia, Senate Community Affairs References Committee, *Design, Scope, Cost-Benefit Analysis, Contracts Awarded and Implementation Associated with the Better Management of the Social Welfare System Initiative* (Canberra, 2017), p. 60.

<sup>65</sup> Submission to the Special Rapporteur by the Government of Greece.

innovation. In 2018, Sweden was forced to reverse a complex digital system used by the Employment Service to communicate with jobseekers because of problems that led to as many as 15 per cent of the system's decisions likely being incorrect.<sup>66</sup>

31. In Australia, the Targeted Compliance Framework requires jobseekers to use a digital dashboard to report mandatory activities and to check their compliance status. Failure to meet a "mutual obligation" can automatically, without the involvement of a human decision maker, lead to the suspension of payments or the imposition of financial penalties. Problems have been highlighted that result from a lack of Internet access and digital literacy and to the rigidity of an automated system which fails to take real-life situations into account.<sup>67</sup>

### **III. Making digital technologies work for social protection**

32. Digital technologies, including artificial intelligence, have huge potential to promote the many benefits that are consistently cited by their proponents. They are already doing so for those who are economically secure and can afford to pay for the new services. They could also make an immense positive difference by improving the well-being of the less well-off members of society, but this will require deep changes in existing policies. The leading role in any such effort will have to be played by Governments through appropriate fiscal policies and incentives, regulatory initiatives and a genuine commitment to designing the digital welfare state not as a Trojan Horse for neoliberal hostility towards welfare and regulation but as a way to ensure a decent standard of living for everyone in society.

33. In the present report, problems that are specific to the ways in which the digital welfare state has been envisioned and implemented have been highlighted. However, many of the changes required to avoid a digital dystopia will need to range more broadly. In addressing the General Assembly on 24 September 2019, the Prime Minister of the United Kingdom warned of the dangers of the digital age, singling out: (a) the risk of round-the-clock surveillance; (b) the perils of algorithmic decision-making; (c) the difficulty of appealing against computer-generated determinations; and (d) the inability to plead extenuating circumstances when the decision maker is an algorithm. He concluded rather ominously by suggesting that digital authoritarianism was an emerging reality.<sup>68</sup>

34. His comments resonate strongly in the context of the digital welfare state, including in relation to the Universal Credit system of the United Kingdom. There is no magic recipe for avoiding the pitfalls of which he warned, but the steps set out in the following subsections could help to make the digital welfare state a force for enhancing rather than undermining human rights.

#### **A. Taking human rights seriously and regulating accordingly**

35. The Prime Minister of the United Kingdom concluded his statement to the General Assembly by warning that, unless new technology reflected the rights contained in the Universal Declaration of Human Rights, that Declaration would mean

---

<sup>66</sup> Tom Wills, "Sweden: rogue algorithm stops welfare payments for up to 70,000 unemployed", Algorithm Watch, 19 February 2019.

<sup>67</sup> Submission to the Special Rapporteur by the Human Rights Law Centre; and Simone Casey, "The targeted compliance framework: implications for job seekers", National Social Security Rights Network, 25 July 2019.

<sup>68</sup> Boris Johnson, Prime Minister, United Kingdom, statement to the General Assembly, New York, 24 September 2019.

nothing.<sup>69</sup> The reality is that Governments have certainly not regulated the technology industry as if human rights were at stake, and the technology sector remains a virtually human rights-free zone. The big technology companies (frequently referred to as “big tech”) and their governmental supporters have worked hard to keep it that way. Their approach can be summed up for present purposes in four propositions, as set out below.

36. The first proposition is that the ability to innovate requires freedom, especially from regulation. The early call by the founder of Facebook for the industry to “move fast and break things” epitomizes the importance attached to minimizing legal and governmental constraints. However, this argument leads inexorably to a handful of powerful executives replacing Governments and legislators in determining the directions in which societies will move and the values and assumptions which will drive those developments. The accumulation of vast amounts of capital in the hands of very small elites and the rapid growth in extreme inequality have gone hand in hand with the ascendancy of this approach so far.<sup>70</sup>

37. The second proposition is that there are no universal values. In a recent book, the President of Microsoft asked, rhetorically: “How can the world converge on a singular approach to ethics for computers when it cannot agree on philosophical issues for people?”<sup>71</sup> Even non-discrimination standards are sometimes presented as being too vague and contested to be useful in regulating artificial intelligence.<sup>72</sup> However, these arguments are self-serving and ill-informed. Governments worldwide have accepted universal human rights standards, including in the form of binding legal obligations. Over the past half century or more, these standards have been exhaustively developed and applied by courts and a wide range of expert and community-based bodies. There remains plenty of room for philosophical disagreements, but there is no absence of agreement on core human values.

38. The third proposition is that Governments are inherently slow and clumsy and tend to respond to yesterday’s challenges rather than tomorrow’s. The Republican minority leader of the United States House of Representatives recently argued that the bureaucratic leviathan does not have what it takes to develop or enforce nimble responses to rapid change in the technology industry.<sup>73</sup> While such claims might also be put forward by the proponents of unfettered discretion for the finance, aviation, defence, pharmaceutical and other industries, it is solely in relation to big tech that Governments have been prepared to abandon their regulatory responsibilities and acquiesce in a self-regulatory approach to such an extreme degree. There is no justification for such exceptionalism and no empirical evidence to support the claim that there is a fundamental incompatibility between innovation and regulation.

39. The fourth proposition is that public accountability is unnecessary because the free market is the best regulator.<sup>74</sup> Leaving aside the powerful arguments that big tech is deeply anti-competitive and thus immune to many currents of the free market, the great scandals of recent years that have led to the backlash against big tech (the so-called techlash) provide compelling evidence that public accountability is indispensable.

<sup>69</sup> Ibid.

<sup>70</sup> See Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York, Public Affairs, 2019); and Emmanuel Saez and Gabriel Zucman, *The Triumph of Injustice: How the Rich Dodge Taxes and How to Make Them Pay* (New York, W. W. Norton and Company, 2019).

<sup>71</sup> Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York, Penguin Press, 2019), p. 207.

<sup>72</sup> Aaron Rieke, Miranda Bogen and David G. Robinson, “Public scrutiny of automated decisions: early lessons and emerging methods” (Upturn and Omidyar Network, 2018), p. 25.

<sup>73</sup> Kevin McCarthy, “Don’t count on Government to protect your privacy”, *New York Times*, 14 June 2019.

<sup>74</sup> See Julie Cohen, “Law for the platform economy”, *U.C. Davis Law Review*, vol. 51, No. 1 (November 2017).



40. In response to growing calls for effective governmental regulation, the industry has gone into high gear in producing, influencing and embracing codes of ethics and other non-binding standards purporting to regulate digital technologies and their developers.<sup>75</sup> Most, but by no means all, of these codes contain a reference to human rights, but the substance of human rights law is invariably lacking. Instead, the token reference to human rights serves only to enhance claims of legitimacy and universality. Meanwhile, the relevant discussions of ethics are based on almost entirely open-ended notions that are not necessarily grounded in legal or even philosophical arguments and can be shaped to suit the needs of the industry. As a result, there are serious problems of conceptual incoherence, conflicts among norms are rarely acknowledged, meaningful input is rarely sought from stakeholders and accountability mechanisms are absent.<sup>76</sup> Even industry-employed ethicists acknowledge that “if ethics is simply absorbed within the logics of market fundamentalism, meritocracy, and technological solutionism, it is unlikely that the tech sector will be able to offer a meaningful response to the desire for a more just and values-driven tech ecosystem.”<sup>77</sup> Against this background, it is unsurprising that there are few public or scholarly discussions of the human rights implications of digital welfare states.

41. The human rights community has thus far done a very poor job of persuading industry, Government or, seemingly, society at large of the fact that a technologically driven future will be disastrous if it is not guided by respect for human rights that is in turn grounded in law.

## B. Ensuring legality and transparency

42. One of the most surprising characteristics of too many important digital welfare state initiatives is a lack of attention to the importance of ensuring legality. Many such examples have been drawn to the Special Rapporteur’s attention, including: the online compliance intervention system of the Government of Australia, which used automated data-matching as the basis for sending out vast numbers of debt notices with very high error rates;<sup>78</sup> allegedly unlawful information provided to claimants over the online Universal Credit portal in the United Kingdom;<sup>79</sup> the contested legality of the Irish Public Services Card for some of the purposes for which it has been used;<sup>80</sup> the System Risk Indication system in the Netherlands, which initially

<sup>75</sup> These include industry standards, civil society initiatives and public frameworks. To give a few examples: IBM, “Everyday ethics for artificial intelligence” (September 2018); Google, “Artificial intelligence at Google: our principles” (2019); Microsoft, *The Future Computed* (2018); Institute of Electrical and Electronics Engineers, Global Initiative on Ethics of Autonomous and Intelligent Systems; Software and Information Industry Association, “Ethical principles for artificial intelligence and data analytics” (2017); Future of Life Institute, “Asilomar artificial intelligence principles” (2017); and Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, “Ethics guidelines for trustworthy AI” (Brussels, European Commission, April 2019).

<sup>76</sup> Karen Yeung, Andrew Howes and Ganna Pogrebna, “AI governance by human rights-centred design, deliberation and oversight: an end to ethics washing”, in M. Dubber and F. Pasquale, eds., *The Oxford Handbook of AI Ethics* (forthcoming).

<sup>77</sup> Jacob Metcalf, Emanuel Moss and danah boyd [sic], “Owning ethics: corporate logics, Silicon Valley, and the institutionalization of ethics”, *Social Research*, vol. 86, No. 2 (Summer 2019), p. 473.

<sup>78</sup> Carney, “The new digital future for welfare”.

<sup>79</sup> Submission to the Special Rapporteur by the Child Poverty Action Group.

<sup>80</sup> Data Protection Commission, *Final Investigation Report: An Investigation by the Data Protection Commission in Respect of the Processing of Personal Data by the Department of Employment Affairs and Social Protection in relation to the Public Services Card (“PSC”) – Examining Compliance with the Obligations in Relation to Legal Basis and Transparency* (Dublin, 2019).

lacked a legal basis and remains subject to court challenge;<sup>81</sup> and the Aadhaar system in India, which was originally implemented without a legal framework.<sup>82</sup>

43. While the lack of a legal basis is deeply problematic per se, it also means that opportunities for legislative debate and for public inputs to shape the relevant systems are also lacking. This has potentially major negative implications for transparency, design, legitimacy and the likelihood of acceptance.

### C. Promoting digital equality

44. Egalitarianism is a consistent theme of the technology industry, as exemplified by Facebook's aim "to give people the power to build community and bring the world closer together".<sup>83</sup> At the macro level, however, big tech has been a driver of growing inequality<sup>84</sup> and has facilitated the creation of a "vast digital underclass".<sup>85</sup>

45. For its part, the digital welfare state sometimes gives beneficiaries the choice to go digital or to continue using more traditional techniques. In reality, however, policies such as "digital by default" or "digital by choice" are usually transformed into "digital only" in practice. This in turn exacerbates or creates major disparities among different groups. A lack of digital literacy leads to an inability to use basic digital tools at all, let alone effectively and efficiently. Limited or no access to the Internet poses huge problems for a great many people. Additional barriers arise for individuals who have to pay high prices to obtain Internet access, travel long distances or absent themselves from work to do so, visit public facilities such as libraries in order to get access, or obtain assistance from staff or friends to navigate the systems. Moreover, while the well-off might have instant access to up-to-date and easy-to-use computers and other hardware, as well as fast and efficient broadband speeds, the least well-off are far more likely to be severely disadvantaged by out-of-date equipment and time-consuming and unreliable digital connections.

46. In submissions to the Special Rapporteur from a wide range of countries, the salience of these different problems was emphasized. In both the global North and the global South, many individuals, especially those living in poverty, do not have a reliable Internet connection at home,<sup>86</sup> cannot afford such a connection,<sup>87</sup> are not digitally skilled or confident<sup>88</sup> or are otherwise inhibited from communicating with authorities online. In the various submissions, it was emphasized how those problems impede the ability of would-be claimants to realize their human rights.

<sup>81</sup> Alston, brief as amicus curiae before the District Court of the Hague on the case of *NJCM c.s./ De Staat der Nederlanden (SyRI)*.

<sup>82</sup> Submission to the Special Rapporteur by the Centre for Communication Governance at the National Law University, Delhi.

<sup>83</sup> Kevin Munger, "The rise and fall of the Palo Alto consensus", *New York Times*, 10 June 2019.

<sup>84</sup> Isobel Asher Hamilton, "A definitive list of the 13 richest tech billionaires in the world", *Business Insider*, 9 March 2019.

<sup>85</sup> Farhad Manjoo, "The tech industry is building a vast digital underclass", *New York Times*, 24 July 2019.

<sup>86</sup> Emily Dreyfuss, "Global Internet access is even worse than dire reports suggest", *Wired*, 23 October 2018; Organization for Economic Cooperation and Development (OECD), Internet Access database, available at <https://data.oecd.org/ict/internet-access.htm>; and OECD, "OECD toolkit aims to spur high-speed Internet use in Latin America and the Caribbean", 21 June 2016.

<sup>87</sup> Alliance for Affordable Internet, "2018 affordability report" (Washington, D.C., 2018); and World Wide Web Foundation, "New mobile broadband pricing data shows uneven progress on affordability", 21 March 2019. In the United States, 27 per cent of the population does not use high-speed broadband Internet at home, and that figure is as high as 44 per cent for people with an income below \$30,000 (Pew Research Centre, "Internet/broadband fact sheet", 12 June 2019).

<sup>88</sup> European Commission, "Human capital: digital inclusion and skills", 2019.

47. The United Kingdom provides an example of a wealthy country in which, even in 2019, 11.9 million people (22 per cent of the population) do not have the essential digital skills needed for day-to-day life. An additional 19 per cent cannot perform fundamental tasks such as turning on a device or opening an application. In addition, 4.1 million adults (8 per cent) are offline because of fears that the Internet is an insecure environment; proportionately, almost half of those are from a low-income household and almost half are under 60 years of age.<sup>89</sup>

48. These problems are compounded by the fact that, when digital technologies are introduced into the welfare state, their distributive impact is often not a significant focus of Governments.<sup>90</sup> In addition, vulnerable individuals are not commonly involved in the development of information technology systems and information technology professionals are often ill-equipped to anticipate the sort of problems that are likely to arise.<sup>91</sup> It is often assumed, without justification, that individuals will have ready access to official documents and be able to upload them, that they will have a credit history or broader digital financial footprint, or even that their fingerprints will be readable, which is often not the case for those whose working lives have involved unremitting manual labour.

49. In terms of digital welfare policy, several conclusions emerge. First, there should always be a genuine, non-digital option available.<sup>92</sup> Second, programmes aimed at digitizing welfare arrangements should be accompanied by programmes designed to promote and teach the digital skills needed and to ensure reasonable access to the necessary equipment, as well as effective online access. Third, in order to reduce the harm caused by incorrect assumptions and mistaken design choices, digital welfare systems should be co-designed by their intended users and evaluated in a participatory manner.

#### **D. Protecting economic and social rights in the digital welfare state**

50. The processes of digitization and the increasing role played by automated decision-making through the use of algorithms and artificial intelligence have, in at least some respects, facilitated a move towards a bureaucratic process and away from one premised on the right to social security or the right to social protection. Rather than the ideal of the State being accountable to the citizen to ensure that the latter is able to enjoy an adequate standard of living, the burden of accountability has in many ways been reversed. To a greater degree than has often been the case in the past, today's digital welfare state is often underpinned by the starting assumption that individuals are not rights holders but rather applicants. In that capacity, people must convince the decision-makers that they are deserving, that they satisfy the eligibility criteria, that they have fulfilled the often onerous obligations prescribed and that they have no other means of subsistence. In addition, much of this must be done electronically, regardless of applicants' skills in that domain.

<sup>89</sup> "The digitally disadvantaged", in Lloyds Bank, *UK Consumer Digital Index 2019 – Key Findings* (London, 2019).

<sup>90</sup> Mary Madden, "The devastating consequences of being poor in the digital age", *New York Times*, 25 April 2019.

<sup>91</sup> Submission to the Special Rapporteur by Norbert Jansen (ICTU, the Netherlands).

<sup>92</sup> Submissions to the Special Rapporteur by the Association for Progressive Communications, Derechos Digitales and Media Matters for Democracy; Citizens Advice Scotland; and the National Social Security Rights Network.

51. The right to social security<sup>93</sup> encompasses the right to access and maintain benefits, whether in cash or in kind, without discrimination.<sup>94</sup> The imposition of technological requirements can make it impossible or very difficult for individuals to effectively access that right.<sup>95</sup>

52. The right to social protection is integrally linked to what the Human Rights Committee refers to as the right to life with dignity, which must be protected, where necessary, through measures designed to ensure access without delay by individuals to essential goods and services such as food, water, shelter, health care, electricity and sanitation, and other measures designed to promote and facilitate adequate general conditions.<sup>96</sup> Various other rights are also implicated, including the right to an adequate standard of living, the right to mental health and the right to be treated with dignity.

53. While social protection in general should be designed to protect those rights, the dignity dimension is at particular risk in the context of the digital welfare state. The potential risks arise in various contexts.

54. First, the process for determining eligibility may easily be transformed into an electronic question-and-answer process that almost inevitably puts already vulnerable individuals at even greater disadvantage.

55. Second, the way in which determinations are framed and communicated may be dehumanized and allow no room for meaningful questioning or clarification.

56. Third, the digital welfare state often seems to involve various forms of rigidity and the robotic application of rules. As a result, extenuating circumstances, such as being late for an appointment because of urgent caring obligations or being unable to understand a written communication because of a disability or a personal crisis, are often not taken into account in a predominantly digital context.

57. Fourth, digital systems are often not designed to respond rapidly either to serious emergencies or to daily challenges, such as those that may be experienced by an older person whose entitlement has suddenly and inexplicably been electronically reduced or cancelled or by a single parent unable to take a child to a local day care because the digital identification card will not function.

58. Fifth, the ways in which services are provided can easily have degrading connotations, such as unnecessarily exposure to a broader audience the fact that a person is reliant on benefits, or requiring extended waiting periods or the navigation of lengthy queues.

59. Sixth, the introduction of various new technologies that eliminate the human provider can enhance efficiency and provide other advantages but might not necessarily be satisfactory for individuals who are in situations of particular vulnerability. New technologies often operate on the law of averages, in the interests of majorities and on the basis of predicted outcomes or likelihoods.

60. Seventh, digital services risk eliminating, almost entirely, much of the human interaction and compassion that are likely to be indispensable components in providing at least some welfare recipients with the care and assistance they need. The assumption that there is always a technological fix for any problem is highly likely to be misplaced in various aspects of a humane and effective system of social protection.

---

<sup>93</sup> International Covenant on Economic, Social and Cultural Rights, art. 9.

<sup>94</sup> Committee on Economic, Social and Cultural Rights, general comment No. 19 (2007) on the right to social security, para. 2.

<sup>95</sup> *Ibid.*, paras. 24–27.

<sup>96</sup> Human Rights Committee, general comment No. 36 (2018) on the right to life, para. 26.

## E. Protecting civil and political rights in the digital welfare state

61. That the poor suffer from more intense levels of scrutiny, monitoring and surveillance is hardly an original observation. In the 1960s, Charles Reich wrote that welfare recipients in the United States had been subjected to many forms of procedure and control not imposed on other citizens and were all too easily regulated.<sup>97</sup> In 1975, Michel Foucault wrote about the “coercive technologies of behaviour” used in modern society to discipline and punish the poorer classes.<sup>98</sup>

62. By way of explaining why these lessons have not been learned in the digital welfare state, Shoshana Zuboff writes that the system of “surveillance capitalism” that prevails today is unprecedented, which has enabled it to elude systematic contest because it cannot be adequately grasped with our existing concepts.<sup>99</sup> This private surveillance is being reinforced by trends in government surveillance. Jack Balkin has described the “national surveillance state” as a permanent feature of governance that will become as ubiquitous in time as the familiar devices of the regulatory and welfare states.<sup>100</sup>

63. Digital technologies are employed in the welfare state to surveil, target, harass and punish beneficiaries, especially the poorest and most vulnerable among them. Once again, many of the submissions received by the Special Rapporteur serve to illustrate and reinforce this point. A number of human rights concerns are highlighted in them.

64. A first concern, in the context of social security benefits and assistance, is that there is a real risk of beneficiaries being effectively forced to give up their right to privacy and data protection to receive their right to social security, as well as other social rights.<sup>101</sup>

65. A second concern is the blurring of the lines between public and private surveillance. Welfare state authorities increasingly rely, either actively or passively, on private corporations for the surveillance and targeting of beneficiaries. Private entities have different motives for their involvement in benefit and social assistance systems and this may lead to conflicts between the public interests that these systems ought to serve and the private interests of corporations and their owners.

66. A third concern is the potential for deliberate targeting and harassment of the poor through new technologies in the welfare state. As highlighted in one submission to the Special Rapporteur, fraud in the welfare state is often the result of confusion, complexity and the inability to correct the resulting errors.<sup>102</sup> However, by deliberately using the power of new technologies to identify fraud or violations of “conditionalities” imposed on beneficiaries, Governments are likely to find inconsistencies that they can hold against claimants. It is relevant here that new technologies are enabling what Jack Balkin described as the “death of amnesia”: new abilities to collect information and store it digitally for an undefined period of time create a future in which a wealth of information can be held against someone indefinitely.<sup>103</sup>

<sup>97</sup> Charles A. Reich, “Individual rights and social welfare: the emerging legal issues”, *Yale Law Journal*, vol. 74, No. 7 (1965), p. 1245.

<sup>98</sup> Foucault, *Discipline and Punish*, p. 222.

<sup>99</sup> Zuboff, *The Age of Surveillance Capitalism*, p. 14.

<sup>100</sup> Jack M. Balkin, “The constitution in the national surveillance state”, *Minnesota Law Review* (vol. 93, No. 1 (2008)).

<sup>101</sup> Submission to the Special Rapporteur by the Government of Mexico; and Philip Alston, Special Rapporteur on extreme poverty and human rights, statement on visit to the United States, 15 December 2017, para. 57.

<sup>102</sup> Submission to the Special Rapporteur by Norbert Jansen (ICTU, the Netherlands).

<sup>103</sup> Balkin, “The constitution in the national surveillance state”, p. 13.

67. Additional concerns that warrant greater consideration than can be provided in the present report include: (a) the human rights consequences of the move to predicting risk instead of the ex post enforcement of rules violations;<sup>104</sup> (b) the dangers of connecting Government data silos, which is more readily contemplated in the welfare context than elsewhere in the field of digital governance;<sup>105</sup> (c) the psychological and societal cost of constant monitoring and surveillance;<sup>106</sup> and (d) the growing tendency of some Governments to use the opportunities provided by the digital welfare state to try to alter social behaviours, such as sexual activity or preferences, approaches to cohabitation, the use of alcohol or drugs and the decision to have children.<sup>107</sup>

## F. Resisting the inevitability of a digital-only future

68. Digital technologies in general, and especially those central to the digital welfare state, are often presented as being both unavoidable and irresistible. If a country wants to be seen to be at the technological cutting edge, if its Government wants to have the most efficient, economical and flexible welfare system available and if its citizenry wants all of the convenience that comes from not having to provide identification in order to undertake various transactions, then a transition to a digital welfare state must be pursued. However, quite apart from the choices that citizens and Governments might make if they were fully informed and adequately consulted, the reality is that such decisions are all too often taken in the absence of sophisticated cost-benefit analyses. When such analyses are undertaken, they consist of financial balance sheets that ignore what might be termed the fiscally invisible intangibles that underpin human rights. Values such as dignity, choice, self-respect, autonomy, self-determination and privacy are all traded off without being factored into the overall equation, all but guaranteeing that insufficient steps will be taken to ensure their role in the new digital systems.

69. It is often assumed that at least some of these trade-offs can be justified on the grounds that the bargain is just a matter between the individual and a particular government agency. However, such an image is increasingly very far from the truth as cross-matching, data-sharing and cross-verification systematically enlarge the pools of data potentially available across the spectrum of governance. To the extent that assurances are given that leakage from one silo to the next will not occur, such guarantees are largely illusory as a change of Government or a real or imagined emergency situation is all that is required to trigger a partial or comprehensive breaking down of the partitions, quite apart from the risks of electronic data breaches resulting from hacking or normal system breakdowns. In addition, the assumption that the relationship is only between Government and citizen is also anachronistic. Corporate actors now play a central role in large parts of the welfare system and, when taken together with the ever-expanding reach of other forms of surveillance capitalism, intangible human rights values can be assumed to be worth as much as the shares of a bankrupt corporation.

<sup>104</sup> Ibid., p. 11.

<sup>105</sup> Reetika Khera, "These digital IDs have cost people their privacy – and their lives", *Washington Post*, 9 August 2018.

<sup>106</sup> Research with civil society groups has shown that concerns about stigmatization and feelings of being targeted are more prominent than privacy concerns per se (submission to the Special Rapporteur by the Data Justice Lab at Cardiff University).

<sup>107</sup> See Foucault's analysis of panoptic systems that could be used as a machine to carry out experiments, to alter behaviour, to train and correct individuals (Foucault, *Discipline and Punish*, p. 203).

70. The Special Rapporteur has learned of situations in which crucial decisions to go digital have been taken by government ministers without consultation, or even by departmental officials without any significant policy discussions taking place, on the grounds that the move is essentially an administrative matter, rather than one involving a potentially game-changing approach to a large swathe of official policy. Sometimes, there seems to be a presumption that, even if the move to digital is not currently necessary, it surely will be one day and it is better to move in advance. Support for such pre-emptive moves may come from corporate interests, as well as from the security and counter-terrorism sectors, albeit for quite different reasons. Careful and transparent consideration should always be given to the questions of why, for whom, when and how transitions to digital systems take place.

71. Even where detailed cost estimates are provided, accuracy seems difficult to achieve. Helen Margetts has observed that, in the United Kingdom, for example, technology and the public sector have rarely been happy bedfellows and every government technology project seems doomed to arrive late, underperform and come in over budget.<sup>108</sup> Another example is the Aadhaar system in India, which is said to have lacked a proper cost-benefit analysis prior to implementation<sup>109</sup> and in relation to which there has been great disagreement as to the post hoc assessment of costs and benefits.<sup>110</sup>

## G. Role of the private sector

72. Two consistent themes of the present report have been the reluctance of many Governments to regulate the activities of technology companies and the strong resistance of those companies to taking any systematic account of human rights considerations. The fact that this leads to many large technology corporations operating in an almost human rights-free zone is further exacerbated by the extent to which the private sector is taking a leading role in designing, constructing and even operating significant parts of the digital welfare state.<sup>111</sup>

73. Among well-known examples are the involvement of the Net1 subsidiary Cash Paymaster Services, MasterCard and Grindrod Bank in the distribution of social grants linked to the biometric identification system of South Africa, the roles played by Indue and Visa in the cashless debit card trials in Australia and the involvement of IBM in the Social Assistance Management System in Ontario, Canada. In submissions to the Special Rapporteur, attention was also drawn to the increasing role of the private sector in Germany for public administration software used for unemployment services and social and youth welfare;<sup>112</sup> and outsourcing by local authorities in the United Kingdom to private companies in the area of social protection.<sup>113</sup> In contrast,

<sup>108</sup> Helen Margetts, “Back to the bad old days, as civil service infighting threatens United Kingdom’s only hope for digital government”, *The Conversation*, 9 August 2016.

<sup>109</sup> Submission to the Special Rapporteur by the Centre for Communication Governance at the National Law University, Delhi.

<sup>110</sup> Reetika Khera, “A ‘cost-benefit’ analysis of UID”, *Economic and Political Weekly*, vol. 48, No. 5 (February, 2013); Kieran Clarke, “Estimating the impact of India’s Aadhaar scheme on liquid petroleum gas subsidy expenditure”, International Institute for Sustainable Development, 16 March 2016; Jean Drèze and Reetika Khera, “Aadhaar’s \$11-billion question”, *Economic Times*, blog, 17 February 2018; Anand Venkatanarayanan, “The curious case of the World Bank and Aadhaar savings”, *The Wire*, 3 October 2017; and Aria Thaker, “Emails from a World Bank official reveal why India shouldn’t brag about \$11 billion Aadhaar savings”, *Quartz India*, 10 January 2019.

<sup>111</sup> Submissions to the Special Rapporteur by the Government of Croatia, the Government of Estonia and the Government of Ireland.

<sup>112</sup> Submissions to the Special Rapporteur by AlgorithmWatch.

<sup>113</sup> Submission to the Special Rapporteur by the Data Justice Lab at Cardiff University.

the deliberate choice by some Governments not to rely on private actors to play key roles in the welfare state was pointed out in some submissions.<sup>114</sup>

74. The Special Rapporteur has addressed elsewhere the issues arising out of the privatization of public services more generally (A/73/396). However, in relation to social protection services, there is a deeply problematic lack of information about the precise role and responsibility of private actors in proposing, developing and operating digital technologies in welfare states around the world. This lack of transparency has a range of causes, from gaps in freedom of information laws, confidentiality clauses and intellectual property protections to a failure on the part of legislatures and executives to require transparency and a general lack of investigation of these practices by oversight bodies and the media.<sup>115</sup> The absence of information seriously impedes efforts to hold Governments and private actors accountable.

## H. Accountability mechanisms

75. Many of the programmes used to promote the digital welfare state have been designed by the very same companies that are so deeply resistant to abiding by human rights standards. Moreover, those companies and their affiliates are increasingly relied upon to design and implement key parts of the welfare programmes themselves. It is thus evident that the starting point for efforts to ensure human rights-compatible digital welfare state outcomes is to ensure, through governmental regulation, that technology companies are legally required to respect applicable international human rights standards.<sup>116</sup>

## IV. Conclusions

**76. There is no shortage of analyses warning of the dangers for human rights of various manifestations of digital technology and, especially, artificial intelligence. However, these studies are overwhelmingly focused on traditional civil and political rights such as the right to privacy, non-discrimination, a fair trial and freedom of expression and information. Few studies have adequately captured the full array of threats represented by the emergence of the digital welfare state. The vast majority of States spend very large amounts of money on different forms of social protection, or welfare, and the allure of digital systems that offer major cost savings along with personnel reductions, greater efficiency and fraud reduction, not to mention the kudos associated with being at the technological cutting edge, is irresistible. There is little doubt that the future of welfare will be integrally linked to digitization and the application of artificial intelligence.**

**77. However, as humankind moves, perhaps inexorably, towards the digital welfare future, it needs to alter course significantly and rapidly to avoid stumbling, zombie-like, into a digital welfare dystopia. Such a future would be one in which unrestricted data-matching is used to expose and punish the**

<sup>114</sup> Submissions to the Special Rapporteur by the Government of Argentina, the Government of Greece and Louise Humpage (University of Auckland).

<sup>115</sup> Submissions to the Special Rapporteur by AlgorithmWatch, Privacy International and the Irish Council for Civil Liberties.

<sup>116</sup> See Yeung, Howes and Pogrebna, "Artificial intelligence governance by human rights-centred design"; Paul Nemitz, "Constitutional democracy and technology in the age of artificial intelligence", *Philosophical Transactions A*, vol. 376, No. 2133 (2018); and Karen Yeung, *A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework*, MSI-AUT(2018)05 rev (Council of Europe, 22 May 2019).



slightest irregularities in the record of welfare beneficiaries (while assiduously avoiding such measures in relation to the well-off); evermore refined surveillance options enable around-the-clock monitoring of beneficiaries; conditions are imposed on recipients that undermine individual autonomy and choice in relation to sexual and reproductive choices and choices in relation to food, alcohol, drugs and much else; and highly punitive sanctions are able to be imposed on those who step out of line.

78. It will be argued that the present report is unbalanced, or one-sided, because the dominant focus is on the risks rather than on the many advantages potentially flowing from the digital welfare state. The justification is simple. There are a great many cheerleaders extolling the benefits, but all too few counselling sober reflection on the downsides. Rather than seeking to summarize the analysis above, a number of additional observations are in order.

79. First, digital welfare state technologies are not the inevitable result of scientific progress, but instead reflect political choices made by humans. Assuming that technology reflects preordained or objectively rational and efficient outcomes risks abandoning human rights principles along with democratic decision-making.

80. Second, if the logic of the market is consistently permitted to prevail, it inevitably disregards human rights considerations and imposes externalities on society, for example when artificial intelligence systems engage in bias and discrimination and increasingly reduce human autonomy.<sup>117</sup>

81. Third, the values underpinning and shaping the new technologies are unavoidably skewed by the fact that there is a diversity crisis in the artificial intelligence sector across gender and race.<sup>118</sup> Those designing artificial intelligence systems in general, as well as those focused on the welfare state, are overwhelmingly white, male, well-off and from the global North. No matter how committed they might be to certain values, the assumptions and choices made in shaping the digital welfare state will reflect certain perspectives and life experiences. The way to counteract these biases and to ensure that human rights considerations are adequately taken into account is to ensure that the practices underlying the creation, auditing and maintenance of data are subjected to very careful scrutiny.<sup>119</sup>

82. Fourth, predictive analytics, algorithms and other forms of artificial intelligence are highly likely to reproduce and exacerbate biases reflected in existing data and policies. In-built forms of discrimination can fatally undermine the right to social protection for key groups and individuals. There therefore needs to be a concerted effort to identify and counteract such biases in designing the digital welfare state. This in turn requires transparency and broad-based inputs into policymaking processes. The public, and especially those directly affected by the welfare system, need to be able to understand and evaluate the policies that are buried deep within the algorithms.

---

<sup>117</sup> Anton Korinek, "Integrating ethical values and economic value to steer progress in artificial intelligence", National Bureau of Economic Research Working Paper, No. 26130 (Cambridge, Massachusetts, 2019), p. 2.

<sup>118</sup> Women make up 15 per cent of artificial intelligence research staff at Facebook and 10 per cent at Google; only 2.5 per cent of Google's workforce is black, while Facebook and Microsoft are each at 4 per cent (Sarah West, Meredith Whittaker and Kate Crawford, "Discriminating systems: gender, race and power in AI" (AI Now Institute, 2019)).

<sup>119</sup> Rashida Richardson, Jason M. Schultz, and Kate Crawford, "Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice", *New York University Law Review* (May 2019).

83. Fifth, especially, but not only, in the Global North, the technology industry is heavily oriented towards designing and selling gadgets for the well-off, such as driverless and flying cars and electronic personal assistants for multitasking businesspeople. In the absence of fiscal incentives, government regulation and political pressures, it will devote all too little attention to facilitating the creation of a welfare state that takes full account of the humanity and concerns of the less well-off in any society.

84. Sixth, to date, astonishingly little attention has been paid to the ways in which new technologies might transform the welfare state for the better. Instead of obsessing about fraud, cost savings, sanctions and market-driven definitions of efficiency, the starting point should be how existing or even expanded welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged and to devise new ways of caring for those who have been left behind and more effective techniques for addressing the needs of those who are struggling to enter or re-enter the labour market. That would be the real digital welfare state revolution.

---

Public Disclosure Authorized

Public Disclosure Authorized

Public Disclosure Authorized

Public Disclosure Authorized



# PRINCIPLES ON IDENTIFICATION

FOR SUSTAINABLE DEVELOPMENT



# PRINCIPLES ON IDENTIFICATION FOR SUSTAINABLE DEVELOPMENT: TOWARD THE DIGITAL AGE

## ENDORISING ORGANIZATIONS

African Development Bank

Asian Development Bank (ADB)

Bill & Melinda Gates Foundation (BMGF)

Center for Global Development (CGD)

Digital Impact Alliance (DIAL)

Digital Nations

FHI 360

ID4Africa

International Organization for Migration (IOM)

International Telecommunication Union (ITU)

International Union of Notaries

Mastercard

Norwegian Agency for Development Cooperation (Norad)

Omidyar Network

Open Identity Exchange UK/Europe

Organization of American States

OSCE Office for Democratic Institutions and Human Rights (ODIHR)

Plan International

Privacy and Consumer Advisory Group to the Government Digital Service and GOV.UK

Secure Identity Alliance (SIA)

Smart Africa

The GSMA

UN World Food Programme

UNHCR, The UN Refugee Agency

United Nations Capital Development Fund (UNCDF)

United Nations Children's Fund (UNICEF)

United Nations Development Programme (UNDP)

United Nations Economic Commission for Africa (ECA)

Women in Identity

World Bank Group

# PRINCIPLES

## INCLUSION

- 1 Ensure universal access for individuals, free from discrimination.
- 2 Remove barriers to access and use.

## DESIGN

- 3 Establish a trusted—unique, secure, and accurate—identity.
- 4 Create a responsive and interoperable platform.
- 5 Use open standards and prevent vendor and technology lock-in.
- 6 Protect privacy and agency through system design.
- 7 Plan for financial and operational sustainability.

## GOVERNANCE

- 8 Protect personal data, maintain cyber security, and safeguard people's rights through a comprehensive legal and regulatory framework.
- 9 Establish clear institutional mandates and accountability.
- 10 Enforce legal and trust frameworks through independent oversight and adjudication of grievances.



# PURPOSE

*Every person has the right to participate fully in their society and economy and to be recognized as a person before the law.<sup>1</sup> Yet, as many as 1 billion people across the world do not have basic proof of identity, which is essential for protecting their rights and enabling access to services and opportunities.<sup>2</sup> Many more have forms of identification that are insecure or untrusted by service providers, or live in countries where identification systems are weak and unsuited for the digital era, or fail to safeguard people’s rights and data. Addressing this “identification gap”—by improving the coverage, quality, and governance of identification systems that protect rights and facilitate access to services—is, therefore, critical to the development agenda.*

**The organizations endorsing these Principles are committed to a shared set of values, with the goal of ensuring that identification systems are inclusive, protective of individuals’ data and rights, and designed to support development outcomes.**

Building on existing international norms,<sup>3</sup> the Principles were first developed and published in 2017 by a group of organizations committed to supporting the development of identification systems that are inclusive, trusted, accountable, and used to enhance people’s lives and the achievement of the Sustainable Development Goals (SDGs). Given the quickly evolving nature of the identification sector, the original signatories to the Principles committed to revisiting them to incorporate new perspectives and lessons learned. This second edition reflects inputs from this process and from broader public consultations.

The endorsing organizations—consistent with their respective mandates, operational policies, and rules—use these Principles to promote a common understanding of key issues and good practices; improve stakeholder alignment; guide support and funding decisions; facilitate discussions at country, regional, and/or global levels; and work together to support identification systems that advance economic and social development, protect individual and human rights, and leave no one behind. We hope that a progressively wider range of stakeholders—including governments, intergovernmental organizations, development partners, local and international civil society and nongovernmental organizations, and private sector actors—will join us in endorsing the Principles and putting them into practice.

---

1 The right to recognition before the law is enshrined in Article 6 of the Universal Declaration on Human Rights (UDHR) and Article 16 of the International Covenant on Civil and Political Rights (ICCPR). The right to birth registration is enshrined in several international conventions, including Article 7 of the Convention on the Rights of the Child (CRC).

2 Estimates from the 2018 World Bank Global ID4D Dataset are available at <http://id4d.worldbank.org/global-dataset>

3 This includes, among others, the UN Principles and recommendations on Civil Registration and Vital Statistics (CRVS), international norms on data protection (such as the European General Data Protection Regulation and Council of Europe Convention 108+), global and regional standards and trust frameworks for identification, and the Principles on Digital Development.

## Definitions and Scope

These Principles are intended to apply broadly to the creation and use of identification systems<sup>4</sup> to advance development goals. Because of their central role in realizing individual rights and facilitating access to basic services and entitlements in the physical and digital worlds, **the focus of the Principles is on “official” identification systems provided by, on behalf of, or recognized by governments.**<sup>5</sup>

While each country typically has a unique constellation of official identification systems that can differ greatly in their purpose, provider, technology, architecture, use, and governance arrangements, these systems can be broadly categorized as “legal” or “functional” identification systems. **Legal identification systems** provide recognition before the law and proof of legal identity. The name and nature of legal identification systems varies under national law, but typically includes civil registration systems, national identification systems, population registries, and other foundational identification systems.<sup>6</sup> **Functional identification systems** provide official proof of identity and authorization for particular purposes or sectors. This typically includes identification systems that provide voter identification, ration cards, social security numbers, health cards, tax numbers, and more; in some cases these credentials may also be recognized as proof of identity for other purposes or sectors.<sup>7</sup>

Given the overwhelming trend toward digitalization of economies and societies, the Principles reflect the increasingly digital nature of official identification systems. For example, many provide official **digital credentials** and services (such as mobile IDs, digital certificates, e-signatures, etc.) that enable automated and remote authentication for access to services and entitlements, both in person and online. In some cases, governments have built these systems themselves. In others, countries have developed ecosystems of digital identity providers that rely on existing official identification systems for identity proofing and enrollment. Under a federated ecosystem model, for example, multiple public and/or private entities operating within a trust framework can issue officially recognized digital identity credentials. Emerging decentralized identity architectures and standards are also creating possibilities to store and verify official digital credentials on personal devices.

**For the remainder of this document, the term “identification system” is used to refer to the analog and digital versions of the official identification systems described above.**

---

4 Broadly speaking, identification systems collect and validate identity data through a registration process and then provide people with credentials—such as certificates, cards, or other identity documents—they can use to authenticate themselves or verify specific identity attributes to a third party that needs to rely on their identity or attribute claims.

5 Government recognized ID systems are enabled by and adhere to a country’s legal framework, and are based on an identity proofing process that involves validating the holder against government-issued credentials and/or authoritative source registries such as civil registration systems, national identification systems, or population registers.

6 Governments retain ultimate responsibility for legal identification (see, for example, the Official UN Operational Definition of Legal Identity, ECOSOC resolution E/CN.3/2020/15). Although proof of legal identity—particularly birth and/or marriage registration—is frequently a requirement for acquiring a nationality, legal identification need not be linked to nationality and should not be equated with legal or national status. While some legal identification systems (e.g., national identification systems) require or constitute proof of nationality, others do not.

7 In the case of asylum seekers and refugees, although host states are primarily responsible for providing proof of a legal identity for refugees who do not have valid travel documents, the credentials issued by the UN Refugee Agency under its mandate on behalf of the host state can be recognized as proof of legal or official identity (1951 Convention on the Status of Refugees, Articles 25 and 27; 1950 Statute of the Office of the United Nations High Commissioner for Refugees).



## Why identification matters for development

**For people, identification is a right, an instrument of protection, and a gateway to access services, benefits, and opportunities.**

The importance of identification for people's rights and for development was recognized by the international community through adoption of the Sustainable Development Goal (SDG) Target 16.9: "by 2030, provide legal identity for all, including birth registration." The right to an identity starting from birth—as guaranteed in Articles 7 and 8 of the Convention on the Rights of the Child (CRC)—and to be recognized as a person before the law are critical first steps in ensuring lifelong protection and are a prerequisite for exercising other rights. A legal identity is the basis on which children can establish a nationality, avoid the risk of statelessness, and seek protection from violence and exploitation. For example, proof of age is needed to help prevent child labor, child marriage, and underage recruitment into the armed forces.

Furthermore, having an official way to prove one's identity may be required for many formal interactions, transactions, and services across the public and private sector. For example, verifying a person's identity against an official credential or registry is often required to open a bank account, vote in an election, obtain formal employment, acquire a nationality, register for school, enroll in health insurance, receive a social transfer, buy a SIM card, register property, cross borders, or seek legal redress. The acceleration toward online services and digital transformation across governments and firms means that people also increasingly need a secure and accessible means to prove their identities remotely, such as over the internet.<sup>8</sup>

**For governments, private sector actors, and other stakeholders, being able to reliably identify people or verify certain attributes is critical for delivering programs and services efficiently, effectively, and accountably.**

The ability to know who people are is essential for a number of government responsibilities, including targeting social programs and ensuring that the correct people receive benefits; responding to emergencies, disasters, and epidemics that require rapid direct assistance; collecting taxes; reducing fraud in public wages; facilitating safe and orderly migration; and, in the case of civil registration, producing vital statistics for planning and monitoring development progress. For certain private entities, verifying customers' identities to a particular level of assurance for certain services—such as opening or allowing access to an account—is necessary to mitigate risk, comply with customer due diligence (CDD) or know your customer (KYC) requirements or

---

8 For these reasons, identification is a key enabler of numerous SDG targets in addition to 16.9, including 1.3 (implementing social protection systems), 1.4 (ensuring that the poor and vulnerable have control over land, property, and financial assets), 5a (giving poor women equal access to economic resources, including finance), 5b (enhancing the use of technology, including ICT to promote women's empowerment), 8.10 (universal access to banking, insurance, and financial services), 10.7 (safe and responsible migration and mobility), 10c (reducing the cost of remittance transfer), 12c (phasing out harmful fuel subsidies), 16a (strengthening the capacity to fight terrorism and crime), 16.5 (reducing corruption), and many others.



other regulations, and protect clients against identity fraud and theft. When identification systems provide digital mechanisms for individuals to authenticate themselves remotely in online contexts, they are also important enablers of an inclusive digital economy and underpin digital platforms across sectors, including for online services and digital payment systems.<sup>9</sup>

**When designed and used appropriately, identification systems have the potential to help countries accelerate inclusive development.**

This includes improving governance and service delivery, increasing financial inclusion, reducing gender inequalities by empowering women and girls, and increasing access to health services and social safety nets for the poor. Compared to paper-based registries, the adoption of digital technologies has the potential to increase the accuracy and reliability of identity data and credentials, automate processes to save money and increase convenience, and provide new platforms for innovations in service delivery. Although there are risks to digital technology, digitalization also presents the opportunity to intentionally design identification systems to be more inclusive, user-friendly, and protective of people's rights and data than ever before through the development of new standards, models, and tools to exercise personal oversight and control over how data are used.

---

<sup>9</sup> See, for example, FATF. 2020. *Guidance on Digital Identity*. Financial Action Task Force (FATF), Paris; World Bank. 2018. "Private Sector Economic Impacts from Identification Systems." Washington, DC; Gelb, A., and Metz, A. 2018. *Identification Revolution: Can Digital ID Be Harnessed for Development?* Washington, DC. Center for Global Development; Gelb, A., and Clark, J. 2013. "Identification for Development: The Biometrics Revolution," *Center for Global Development Working Paper 315*.

## Why building “good” identification systems is essential to mitigating risks

**Despite the opportunities that come with improving identification, identification systems that are poorly implemented or inappropriately used can create a number of risks; these risks disproportionately affect already disadvantaged groups and can be amplified by digital technology.**

*Key risks include those related to exclusion or discrimination, data protection and privacy, and poorly designed and implemented identification systems that waste resources while offering few benefits.* Vulnerable and marginalized groups are often the least likely to have proof of their identity, but also the most in need of the protection and services linked to identification.<sup>10</sup> People who are unable to obtain or easily use identification are therefore at greater risk of being left behind when strict identification requirements must be met to access services. Without proactive mitigation measures, new or upgraded identification systems may reinforce or perpetuate existing inequalities, discriminatory practices, and structural biases. Like other systems that process personal data, identification systems may also undermine individual data protection and privacy rights in the absence of appropriate laws and regulations, oversight, and technical controls and safeguards. Data breaches, unauthorized use or surveillance, identity fraud, and function creep can put people—especially vulnerable groups—at serious risk of harm. Furthermore, identification systems are often built with a “top-down” approach and little transparency. Together with poor procurement practices and design choices that inflate costs and lead to vendor or technology lock-in, this can result in systems that are operationally or financially unsustainable and that do not serve people’s needs or development goals.

*While these risks are present in any identification system, they may be amplified by digitization.* With digital technologies, the potential scale and harm of the mismanagement or misuse of personal data are much greater than with paper-based systems. Similarly, the adoption of technologies that depend on internet connectivity and expensive devices has the potential to widen the digital divide and create new obstacles for already marginalized groups to reliably obtain or use identification. The speed of innovation can also create incentives to focus on obtaining the latest technology rather than building systems that are fit for current purposes and flexible for future needs. Furthermore, even if identification systems are successfully digitized, they are unlikely to reach their potential without full digitalization—transforming and rethinking processes for the digital medium—and complementary investments in internet connectivity, online services, payment platforms, and other digital systems.

---

<sup>10</sup> The particular groups most at risk of being excluded by identification systems vary by context, but often include people living in poverty, women and children, migrant populations, refugees and asylum seekers, remote and rural residents, ethnic, linguistic, or religious minorities, sexual and gender minorities, persons with disabilities, the internally displaced, stateless persons, conflict-affected persons, informal sector workers, and other marginalized or minority groups. See, for example, World Bank. 2019. *Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Findex Survey*, Washington, DC: World Bank Group.



**To harness the benefits of identification systems in the digital era, these risks must be proactively, comprehensively, and continuously addressed by stakeholders.**

*Building an identification system that meets development goals requires a multifaceted, multi-stakeholder approach. This requires clearly defining the purposes and intended uses of the system; adopting and resourcing adequate legal and regulatory frameworks that remove barriers to access and provide sufficient safeguards and oversight; implementing inclusive policies and practices for identification system enrollment and use; following a people-centric and data privacy-protecting approach for design and risk assessment; and selecting context-appropriate, equitable, and accessible technologies that ensure the quality, security, and utility of the system now and in the future. Continuous and transparent engagement with the public and a diverse set of stakeholders throughout these processes are essential for fostering trust and accountability, and ensuring that identification systems are built to be useful for people and support sustainable development outcomes.*

## Key Stakeholders and Roles

**In practice, applying the Principles requires a coordinated, sustained effort by multiple stakeholders who play essential roles in providing, using, overseeing, and funding official identification systems:**

- **Individuals.** People are the center of identification systems, both as the data subjects of these systems and the end-users who rely on identification to protect and claim their rights and to access services. They have the right to know and exercise appropriate oversight and control over how—and for what purpose—their personal data are collected, used, stored, shared, and otherwise processed by public and private bodies. Understanding and responding to people’s identification-related needs and concerns, protecting their personal data and privacy, and ensuring their participation in the design and implementation of identification systems that affect their lives are essential.
- **Governments.** National and local government agencies are typically the identity providers for legal identification systems—e.g., civil registration and vital statistics (CRVS), national identification systems, population registries, foundational ID credentials, and so forth—as well as many functional systems, such as voter IDs, tax identifiers, and drivers’ licenses. Other government agencies and service providers are frequently relying parties for these systems, using them to identify or authenticate the people they interact with or serve. Government institutions, including legislatures and oversight bodies, also play a critical role in creating and enforcing legal and regulatory frameworks to enable and safeguard identification systems provided by both the public and private sectors. Finally, government agencies are typically involved in setting standards and developing and supervising trust and assurance frameworks for identity providers, relying parties, and other stakeholders in centralized, federated, or decentralized digital identity ecosystems.
- **Private sector.** Private companies are frequent developers, innovators, and suppliers of identification system components and infrastructure, and may also be providers of identity verification and authentication services. Many private companies are also relying parties who depend on legal or other identification systems to verify or authenticate the identities of their customers (e.g., to open bank or mobile money accounts). In some cases, private sector entities are identity providers within a federated or decentralized ecosystem that use government-issued credentials and authoritative source registries (e.g., civil registries and national identification systems) to create digital credentials or authentication services that are accepted for online government (and private sector) services.

- **Nongovernmental, community-based, and civil society organizations.** Nongovernmental organizations (NGOs), civil society and community-based organizations (CSOs and CBOs) can play vital roles in the design and implementation of identification systems, including through advocacy activities, providing protection and legal assistance, spreading awareness, facilitating community consultations, empowering people to access identification or grievance redress mechanisms, and holding identity providers accountable.
- **International organizations, regional bodies, and development partners.** International inter-governmental bodies, development and humanitarian agencies, foundations, and other donors often provide support for identification systems in the form of funding and technical assistance, and support the establishment of normative standards. Other international and regional bodies are also involved in setting standards related to identification, including those for cross-border interoperability and mutual recognition of credentials. In certain cases, development and humanitarian actors may also be identity providers or administer identification systems for specific programs or activities. In the case of refugees and asylum seekers, UNHCR may provide proof of legal or official identity on behalf of the host state under its mandate.



# PRINCIPLES

# INCLUSION

## 1

### Ensure universal access for individuals, free from discrimination.

- *Legal identity for all.* Everyone should be able to prove their legal identity. Countries must fulfill their obligations and commitments to provide legal identification to all residents<sup>11</sup>—not just citizens<sup>12</sup>—from birth to death, as reflected in international and domestic laws.<sup>13</sup> This includes the obligation of universal birth registration for all children,<sup>14</sup> which is essential for providing proof of legal identity from birth, and the timely registration of other vital events, such as marriages and deaths. It also includes the obligations and commitments to provide proof of legal identity to refugees, stateless persons, and migrants who do not have a valid credential or cannot otherwise prove their legal identity.
- *Nondiscrimination.* All identification systems should be free from discrimination in policy, in practice, and by design. This includes ensuring that legal frameworks; requirements and procedures to register, obtain, or use identification; and the data that are collected or displayed on credentials do not enable or reinforce discrimination against particular groups, such as those who may face increased risks of exclusion for cultural, political, economic or other reasons. Such groups include people living in poverty; women; children; rural populations; racial, ethnic, linguistic, and religious minorities; persons with disabilities; sexual and gender minorities; migrants; asylum seekers, refugees, and the forcibly displaced; and stateless persons among others. Furthermore, identification systems and data should never be used as a tool for discrimination or to infringe on or deny individual or collective rights.

11 While states have the sovereign right to determine eligibility for citizenship and issue proof of citizenship in accordance with international law, they also have the obligation to provide proof of legal identity—or recognize legal identification issued by another state or international organization—to all persons resident on their territory, including birth registration. For example, the 1951 Convention on the Status of Refugees, Article 27 provides that States “shall issue identity papers to any refugee in their territory who does not possess a valid travel document,” and a similar provision for stateless persons is contained in the 1954 Convention on the Status of Stateless Persons, Article 27. Providing everyone with proof of legal identity is critical to the prevention of statelessness (see [www.unhcr.org/ibelong](http://www.unhcr.org/ibelong)).

12 States should provide proof of citizenship to all persons entitled to it without discrimination of any kind.

13 The obligation of states to provide proof of legal identity does not necessarily mean that enrollment in identification systems should be legally mandatory.

14 For example, Article 7 of the Convention on the Rights of the Child (CRC) states: “The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.” The CRC has been ratified by every Member State of the UN except for the United States, which has signed but not ratified the treaty. In practice, however, virtually all births in the United States are registered.



## 2

### Remove barriers to access and use.

- *Direct and indirect costs.* Costs to the individual must never be a barrier to obtain identity credentials required to fulfill rights or access basic services or entitlements. For example, civil registration and the initial issuance of birth and death certificates and other legal identity credentials should be free of charge for the individual. If fees are charged for certain additional services (such as reissuance of lost credentials), rates should be reasonable, proportional to costs incurred, and transparent to the public. The indirect costs of obtaining identification—including fees for supporting documents, travel costs, and cumbersome administrative procedures—must also be minimized.
- *Information asymmetries.* Stakeholders must work to reduce information and knowledge barriers and disparities that might prevent individuals—such as linguistic minorities, people with low literacy levels, persons with disabilities, and others—from accessing or using identification and foster a culture of trust and accountability by increasing literacy and sensitization around the system. Information and education campaigns and other materials must be inclusive and accessible to ensure that everyone has the knowledge, capacity, and tools they need to participate in the identification system and exercise their rights to oversight and control.
- *Technology gaps.* While technology is a key enabler of identification systems, no one should be denied identification or associated services and rights because they lack mobile or internet connectivity, electronic devices, digital literacy or digital skills, the comfort or ability to use certain technology, or because of technology biases or failures. Stakeholders should therefore work together to ensure that identification and authentication services are available and usable for everyone, regardless of digital resources, skills, or connectivity. Furthermore, accessible exception-handling procedures and grievance redress mechanisms are necessary to avoid denial of services or rights and in the case of technical difficulties.
- *Inclusion by design.* Identification systems should prioritize the needs and address the concerns of marginalized and vulnerable groups who are most at risk of being excluded and who are the most in need of the protections and benefits identification can provide. This requires working with communities to proactively identify legal, procedural, social, and economic barriers faced by particular groups, risks and impacts specific to these groups, and adopting appropriate technologies and mitigation measures to ensure that new or updated identification systems do not reinforce or deepen existing inequalities.



## DESIGN

### 3

#### Establish a trusted—unique, secure, and accurate—identity.

- *Uniqueness.* An identification system provides a mechanism to establish and authenticate a unique identity when—within that system—each person has only one identity and no two people share the same identity. Uniqueness is particularly important within legal identification systems and others that support use cases requiring high levels of assurance,<sup>15</sup> such as government-to-person (G2P) payments and voting. Importantly, uniqueness *within* a given system does **not** imply that there must be only one identity provider or system or a single permanent identifier (e.g., a unique ID number) used for all purposes in a country or jurisdiction.
- *Security.* Identification systems must have adequate and effective safeguards against unauthorized access, tampering (alteration or other unauthorized changes to data or credentials), identity theft, misuse of data, cybercrime, and other threats occurring throughout the identification life cycle. Data must be protected at rest and in transit, including when people use their credentials, or including on personal devices. Security measures must include systems to raise awareness about safe utilization of the system and to notify data subjects in the case of data breaches, as well as recourse for identities that have been stolen or compromised and need to be reissued.
- *Accuracy.* Ensuring that identity data are accurate and up-to-date is one of the core principles of data protection and a right of data subjects, and is also essential for the trustworthiness of the system. Identification systems should be designed to ensure accurate data collection and have user-friendly procedures for people to view and update their data and correct errors to ensure accuracy over time.

<sup>15</sup> Generally speaking, a “level of assurance” (LOA) represents the amount of trust a given identification system or credential provides to a third party that an identity claimed by a person or entity is actually their “true” identity. This is a function of multiple factors, including the strength of the identity proofing process when people are enrolled in an identification system and issued credentials (the identity assurance level or IAL), the strength of the authentication process and technology (authentication assurance level or AAL), and—if using a federated model—the assertion protocol used by the federation to communicate authentication and attribute information (federation assurance level or FAL) (adapted from NIST 800-63:2017).

## 4

### Create a responsive and interoperable platform.

- *Responsiveness.* Identification and authentication services should be designed to meet people’s real needs and concerns. In addition, they should be flexible, scalable, and useful for the public agencies and private sector entities that rely on them for identification or authentication. This requires broad stakeholder consultation and a people-centric, participatory approach—including civil society, the public at large, service providers, and other relying parties—beginning with the design process and continuing throughout implementation.
- *Interoperability.* Subject to laws and regulations on data sharing and appropriate technical safeguards, including “privacy-by design” principles, the ability of identification systems to communicate with other systems (e.g., civil registration systems and services providers) and exchange queries or information facilitates services such as identity verification or attestations, eKYC, other permissioned data sharing, and mutual recognition of identification systems across borders.<sup>16</sup>

## 5

### Use open standards and prevent vendor and technology lock-in.

- *Open standards.* Designs based on open standards enable market-based competition and innovation.<sup>17</sup> Open standards are essential for greater efficiency, improved functionality, and adaptability of identification systems, both within countries and across borders.
- *Preventing vendor and technology lock-in.* Good procurement processes facilitate competition, promote innovation, and prevent technology and vendor “lock-in,” which can increase costs and reduce flexibility to accommodate changes over time. Procurement processes should emphasize value for money, economy, integrity, fitness for purpose, efficiency, transparency, and fairness. Effective contract management will ensure that these benefits are sustained throughout implementation.

---

<sup>16</sup> Cross-border interoperability can facilitate migration and trade, but controls should be put in place to protect the security of vulnerable groups, such as refugees, whose personal data must often be shielded from their home country.

<sup>17</sup> For example, ISO/IEC has developed standards covering many aspects of identification systems. For more, see World Bank. 2016. “Technical Standards for Digital Identity Systems: Formulating a Strategic Approach.”

## 6

**Protect privacy and agency through system design.**

- *Privacy by design approach.* Identification systems must be designed to prioritize and protect data and privacy as the default setting without requiring any additional special action on the part of an individual. Personal data, including any data that are linked or linkable to an individual, must be protected from improper use proactively and by default through a robust legal and regulatory framework, system design, and the adoption of technical standards and operational controls.<sup>18</sup>
- *Data protection principles in practice.* The design, policies, and technology used by identification systems should comply with global norms for data protection, including data minimization and proportionality, purpose specification, lawful processing, strict limits on data retention, data accuracy, security, accountability, and transparency, among others.<sup>19</sup> For example, identification systems should limit the collection and exposure of data—particularly sensitive personal information<sup>20</sup>—including in credentials and the structure of identification numbers. Authentication protocols must disclose only the minimum data necessary to ensure appropriate levels of assurance and retain data only for as long as required for the purposes for which the data may lawfully be used, or for which consent has been given. These levels and the method of authentication should reflect an assessment of the level of risk in the transactions and should preferably be based on recognized international standards.<sup>21</sup> Data rules and policies should be transparent and made available to people in a user-friendly format to facilitate knowledge of their rights and the processes available to exercise control or oversight of their data.

18 On the “privacy-by-design” approach, see, for example, Cavoukian, A. 2011. “Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices.” [https://iab.org/wp-content/uploads/2011/03/fred\\_carter.pdf](https://iab.org/wp-content/uploads/2011/03/fred_carter.pdf).

19 Commonly referenced examples of standards include the Fair Information Practices (FIPs), the OECD’s Privacy Guidelines, the EU’s General Data Protection Regulation, the UN Principles on Data Privacy and Protection, and Convention 108+, among others.

20 “Sensitive personal information” can vary by context but commonly includes data that could be used to create fraudulent identities and/or to profile or target individuals. This includes biometric data and identifying numbers, such as permanent or unique identity numbers (UINs), as well as attributes such as religion, ethnicity, caste, political affiliation, and so forth. The disclosure of identifying information may involve particularly serious risks to certain people, for example, asylum seekers and refugees. Therefore, specific considerations apply to ID systems used primarily or exclusively for humanitarian purposes, particularly in settings affected by conflict, violence, and fragility. See, for example, the International Committee of the Red Cross “Policy on the Processing of Biometric Data by the ICRC.” 2019. Available at: [https://www.icrc.org/en/download/file/106620/icrc\\_biometrics\\_policy\\_adopted\\_29\\_august\\_2019\\_.pdf](https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf), and the ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action, 2nd Edition, 2020.

21 Such risk impact assessments should be carried out by the responsible entity that creates, collects, shares, or uses data for authentication and identification purposes linked to the specific use case. Examples of existing standards for levels of assurance for identity proofing include ISO/IEC 29115 and those issued by eIDAS, the UK Cabinet Office, the U.S. National Institute of Standards and Technology (NIST), and others.

## 7

### Plan for financial and operational sustainability.

- *Sustainability.* Identification systems should be designed for long-term fiscal and operational sustainability. This requires a transparent and outcomes-based approach to design to ensure that the system is fit-for-purpose and makes sustainable management and technical choices, and the adoption of business models that ensure the longevity of the system without compromising other Principles. Fees for identification services can create barriers to access, inclusion for individuals, and adoption for service providers. Efforts to recuperate costs through efficiency gains and reduced leakages must also weigh fiscal savings goals against the potential for increasing exclusion errors. Identification systems should be designed to incentivize high standards of performance for all parties involved.



# GOVERNANCE

## 8

### **Protect personal data, maintain cyber security, and safeguard people's rights through a comprehensive legal and regulatory framework.**

- *Legal and regulatory frameworks.* Identification systems must be underpinned by legitimate, comprehensive, and enforceable legal and regulatory frameworks and strong policies that promote trust in the system; ensure data protection and privacy (including cybersecurity); mitigate abuse such as unauthorized surveillance in violation of due process; are free from discrimination and promote inclusion, particularly for vulnerable or marginalized groups; and ensure accountability. Legal frameworks should be clear in delineating liability and recourse for individuals and should be overseen by independent regulatory bodies with appropriate powers and consistent funding. They should also protect people against inappropriate access and use of their data for undue surveillance or unlawful profiling. Frameworks require a balance between regulatory and self-regulatory models that does not stifle competition, innovation, or investment. Appropriate legal and regulatory frameworks are also required for cross-border interoperability or mutual recognition.<sup>22</sup>
- *Rights of data subjects.* Identification services should provide people with genuine choice and control over the collection and use of their data, including the ability to selectively disclose only those attributes that are required for a particular transaction. People should be given a simple means to have inaccurate data corrected free-of-charge and to obtain a copy of their personal data. Personal data should not be used for secondary, unconnected purposes without a person's informed consent, unless otherwise required or authorized under law (for example, as may be necessary and proportionate).<sup>23</sup> Identity providers and other stakeholders should be transparent about identity management; develop appropriate resources to raise people's awareness of how their data will be used; and provide accessible and user-friendly tools to manage their data, provide informed consent, and address grievances. Identity providers should ensure that the initial process to correct errors is administrative rather than judicial in order to increase speed of resolution and reduce costs. Data sharing arrangements should also be transparent and fully documented.

---

<sup>22</sup> For example, asylum seekers and refugees must be given special consideration; see *UNHCR Advisory Opinion on the Rules of Confidentiality Regarding Asylum Information* at <https://www.refworld.org/docid/42b9190e4.html>

<sup>23</sup> See, for example, Convention 108+, Articles 5, 10, and 11.

## 9

### Establish clear institutional mandates and accountability.

- *Institutional mandates.* Legislation, regulation, and trust frameworks must establish and regulate comprehensive governance arrangements for identification systems and providers domestically and—if applicable—internationally. This should include specifying the terms and conditions governing the institutional relations among participating parties, so that the rights and responsibilities of each are clear to all.
- *Accountability.* There should be clear accountability and transparency around the roles and responsibilities of all entities involved in building, operating, managing, and overseeing identification systems.

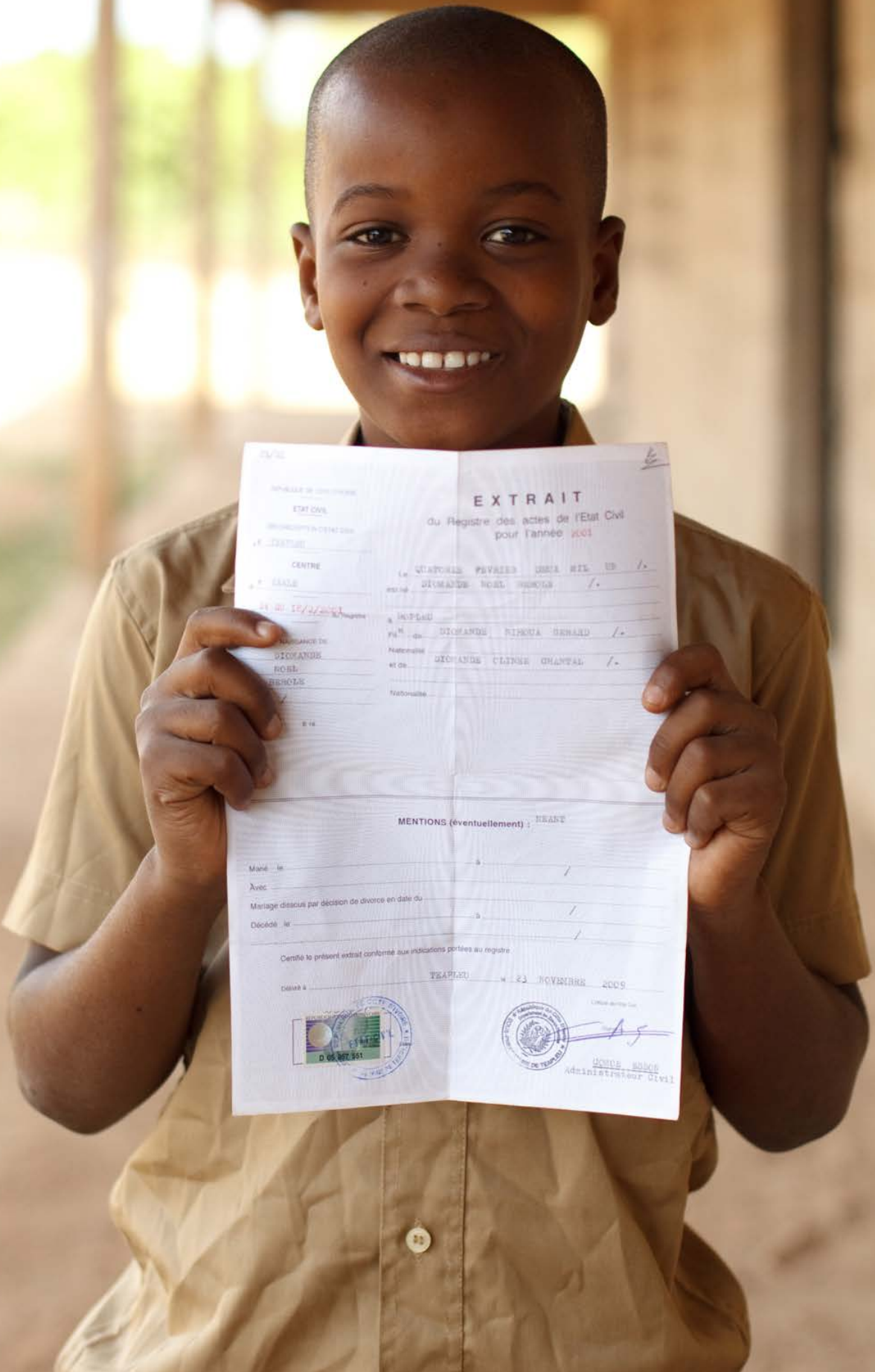


## 10

**Enforce legal and trust frameworks through independent oversight and adjudication of grievances.**

- *Oversight.* the use of identification systems should be independently monitored (for efficiency, transparency, exclusion, misuse, etc.) to ensure that all stakeholders comply with applicable laws and regulations, appropriately use identification systems to fulfill their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding the processing of personal data. Regulators should be sufficiently resourced and empowered to discharge their statutory responsibilities.
- *Adjudication.* Disputes regarding identification and the use of personal data—for example, refusal to register a person or to correct data, or an unfavorable determination of a person’s legal status—that are not satisfactorily resolved by identity providers should be subject to a rapid and low-cost review by independent administrative and judicial authorities with the authority to provide suitable redress without adding barriers for the individual.





## ENDORISING ORGANIZATIONS



Empowered lives.  
Resilient nations.



We welcome additional organizations to join us in endorsing these Principles

February 2021

# Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes



## Acknowledgments

This Guidance was developed by Nina Sun, Joseph Amon and Kenechukwu Esom under the guidance of Ludo Bok and Mandeep Dhaliwal.

We would like to extend our special appreciation to the follow individuals for their invaluable insights and for sharing their knowledge and experience: Caitlin Bishop, Miguel Blanco, Saudamini Dabak, Sabyasachi Das, Sara 'Meg' Davis, Emma Day, Claudia Lopes, Allan Maleche, Rohit Malpani, Naveen Narale, Alexandrine Pirlot de Corbion, Sally Shackleton, Waruguru Wanjau, Daniel Wolfe, Chris Wright and Nida Yamin. The guidance document also benefited from insights from participants at three expert consultations and an online, multilingual e-discussion. These participants included government officials, people living with HIV and representatives from research institutions, universities, digital technology companies, United Nations entities and civil society organizations. Any views expressed in this document are not necessarily those of these individuals or of any organizations or institutions with which they may be affiliated.

Thanks also go to Tenu Avafia, Fatima Bashir, Nicolas Booth, Tracey Burton, Elba Fuster Figerola, Calum Handforth, Serge Kpto, Boyan Konstantinov, Carolin Frankenhauser, Yolanda Jinxin Ma, Camilla Malakasuka, Niall McCann, Peace Kuteesa Nassanga, Samuel Ng, Senelisiwe Ntshangase, Robert Opp, David Owolabi, Cecilia Oh, Leslie Ong, Manish Pant, Sarah Rattray, Sophia Robele, Amitrajit Saha, Aroa Santiago, and Alexandra Wilde of United Nations Development Programme (UNDP); and Emily Christie and Mianko Ramaroson of the Joint United Nations Programme on HIV/AIDS (UNAIDS).

We thank Paul Derrick for expert graphics and design, and Barbara Hall for skillful editing.

This guidance document benefited from the support of the UNDP-led Access and Delivery Partnership (ADP). ADP works with low- and middle-income countries to ensure that health technologies for tuberculosis, malaria and neglected tropical diseases reach people in need. It supports countries to strengthen and harmonize policies and systems, and build the capacities of institutions to drive the necessary reforms for sustainable, country-led progress towards universal health coverage. The Partnership is supported by the Government of Japan and led by UNDP, in collaboration with the World Health Organization, the Special Programme for Research and Training in Tropical Diseases, and PATH.

The views expressed in this publication are those of the author(s) and do not necessarily represent those of the United Nations, including UNDP, or the United Nations Member States.

Guidance on the  
rights-based and  
ethical use of  
digital technologies  
in HIV and health  
programmes

For more information, contact:  
Kenechukwu Esom at  
[kenechukwu.esom@undp.org](mailto:kenechukwu.esom@undp.org).

## Contents

<b>1</b>	<b>Introduction</b>	<b>6</b>
<b>2</b>	<b>Key ethical, technical and social considerations for the adoption of digital health technologies</b>	<b>8</b>
2.1	Ethics and the use of digital technologies	8
2.2	Technical considerations	9
2.2.1	Health technology assessments	10
2.2.2	Incentivizing interoperability	10
2.3	Social considerations – Building trust	11
2.4	Integrating ethical, technical and social considerations into the adoption and use of digital interventions for HIV and health	12
2.4.1	National digital health strategies	12
2.4.2	Digital literacy	12
2.4.3	Biometric and digital identify	13
2.4.4	Advancing accountability and justice	13
2.4.5	Tackling corruption in the health sector	13
<b>3</b>	<b>The rights-based legal and regulatory framework</b>	<b>14</b>
3.1	Human rights risks and digital technologies	14
3.1.1	Data breach	14
3.1.2	Bias	14
3.1.3	Function creep	15
3.2	International human rights standards for States	15
3.2.1	Right to health	15
3.2.2	Right to non-discrimination	17
3.2.3	Right to enjoy the benefits from scientific progress	18
3.2.4	Right to privacy	18
3.2.5	The role of courts in upholding human rights in the digital age	19
3.3	Human rights obligations in relation to private businesses	19
3.4	Legal principles from regional and United Nations agreements on data privacy and security	20
3.4.1	Rights of the data subject	20
3.4.2	Data collection and processing	20
3.4.3	Data security and confidentiality	21
3.5	Looking forward: Opportunities to advance human rights standards for digital health technologies	21

<b>4</b>	<b>Practical checklist for assessing key ethical and rights considerations in adopting digital technologies for HIV and health</b>	<b>22</b>
<b>5</b>	<b>Recommendations for the ethical and rights-based adoption of digital technologies for HIV and health</b>	<b>25</b>
5.1	Recommendations for governments	25
5.1.1	The right to health	25
5.1.2	The right to non-discrimination	25
5.1.3	The right to privacy	25
5.1.4	Access to justice	26
5.1.5	Cross-cutting human rights obligations	26
5.1.6	Country strategies that support adherence to human rights and ethical obligations	26
5.2	Recommendations for the private sector and technology companies	26
5.3	Recommendations to donor agencies	27
	<b>Annex: Overview of common digital technologies</b>	<b>28</b>
1	Individuals	28
1.1	eHealth technologies	28
1.2	Wearables	28
1.3	Point-of-care diagnostics	29
2	Health-care providers	30
2.1	Electronic medical records	30
2.2	Health informatics	31
2.3	Telemedicine	32
3	Health systems management	33
3.1	Digital identifications	33
3.2	Supply chain innovations	34
4	Cross-cutting digital health technologies	34
4.1	Genomics and molecular surveillance	35
4.2	Big data and algorithms	35
4.3	Artificial intelligence and machine learning	35
5	Digital health technologies to advance drug research and development	36
6	Use of digital technologies during the COVID-19 pandemic	36

## Introduction

Unleashing the transformative power of science, technology and innovation is vital to achieving the 2030 Agenda for Sustainable Development, including the commitment to leave no one behind. Advances in digital technologies offer new means of addressing complex global challenges to unlock more equitable and sustainable development, be it is drone-supported climate solutions, user-friendly applications for vaccine cold chain management, digitization of health information systems, or blockchain for financial inclusion.

The United Nations – through the Secretary-General’s Strategy for New Technologies (2018), the High-level Panel for Digital Cooperation (2018–2019), and most recently, the Secretary-General’s Roadmap for Digital Cooperation (2020) – has acknowledged that digital technologies provide great opportunities to promote health and wellbeing. It has also recognized the challenges that they might pose to security, privacy, human rights, and the norms and standards of international law.<sup>1</sup> UNDP’s *Strategic Plan 2018–2021* and *Digital Strategy* highlight the importance of harnessing the positive potential of technologies to drive progress on sustainable development and the organizational commitment to “continually seek out and embrace existing and emerging digital technology in all aspects of its work to better serve its partners in their efforts to achieve the SDGs”.<sup>2</sup> *UNDP’s HIV, Health and Development Strategy 2016–2021: Connecting the Dots* highlights using digital technologies to increase access to HIV and health services as one of the promising opportunities for innovation and acceleration of progress towards the health-related Sustainable Development Goal (SGD) targets, and for building more resilient systems for health.<sup>3</sup>

COVID-19 has highlighted systemic weaknesses in health systems across the world and exposed deep-rooted inequalities across societies, with a disproportionate impact on vulnerable and marginalized groups. The pandemic has also demonstrated that health systems globally, whether robust and well-resourced, or weak and fragile, struggle with affordability, inequitable health care access, uneven outcomes and increasing demands for services.<sup>4</sup> The pandemic accelerated the use of digital technologies to support the public health response including for population surveillance, case identification, contact tracing, testing, the provision of health services and the implementation of quarantine measures.<sup>5</sup> Digital technologies facilitated pandemic strategies and responses in ways that would have been difficult to achieve manually.<sup>6</sup> Digital health technologies (i.e. ‘digital health’)<sup>7</sup> can help address health system challenges and achieve universal health coverage.

The World Health Organization (WHO) *Global Strategy on Digital Health 2020–2025* recognizes that digital technologies are an essential component and an enabler of sustainable health systems and universal health coverage.<sup>8</sup> Its vision of digital health technologies is to:

“improve health for everyone, everywhere by accelerating the development and adoption of appropriate, accessible, affordable, scalable and sustainable person centric digital health solutions to prevent, detect and respond to epidemics and pandemics, developing infrastructure and applications that enable countries to use health data to promote health and wellbeing.”<sup>9</sup>



As countries work towards achieving the SDG 3 – *Ensure healthy lives and promote well-being for all at all ages*, including the targets on ending the AIDS epidemic as a public health threat and achieving universal health coverage by 2030, digital technologies offer clear opportunities to improve service delivery and health systems. For instance, they can facilitate the provision of a more coordinated and higher quality care, increase access to specialized medical expertise, as well as support better patient engagement and access to quality health services at lower costs.<sup>10</sup> Nevertheless, the application of these technologies is most successful when informed by ethics and human rights, and nestled within broader, comprehensive approaches to addressing health outcomes. When there is the appropriate ethical, technical and legal infrastructure, including accountability mechanisms, that safeguard against rights violations, digital technologies can be invaluable in enabling HIV and health programming to become more people-centred, supporting individuals and systems to overcome barriers to access and realize the right to health for all.

The Global Commission on HIV and the Law noted that digital health technologies have the potential to support people living with HIV and its co-infections to reliably make more informed decisions with less stigma, and take control of their health care.<sup>11</sup> However, new and emerging digital technologies can also face challenges in realizing these opportunities while protecting human rights. The Commission cautioned that governments should establish legal protections to safeguard the privacy and confidentiality of users of digital health technologies, ensuring that online health-care records, electronic medical records and communications with health-care providers are protected. To guarantee that the most vulnerable are not excluded, it is necessary that strong measures be taken to protect their privacy when technology is used in HIV programmes.<sup>12</sup> Violations in privacy and confidentiality, particularly where groups are subject to punitive or criminal laws, may lead to human rights violations such as unjust detention, violence or death for people living with HIV and key populations, including sex workers, people who use drugs, lesbian, gay, bisexual, transgender and intersex (LGBTI) people, prisoners and people in closed settings, as well as other vulnerable populations such as migrants and women and girls.

Digital health technologies may also exacerbate health inequities. For example, the digital divide – i.e. the gap between demographics and regions that have access to modern information and communications technology, and those that have restricted access or do not access – still disadvantages millions of people. Additionally, electronic medical records and mHealth interventions (i.e. the use of mobile and wireless technologies to support the achievement of health objectives) can unintentionally reinforce or amplify legal, economic, social and cultural inequalities embedded in health systems based on citizenship, language, or income. Designing and implementing digital health technologies for HIV and health with attention to ethical principles and rights-based obligations help ensure that everyone, everywhere, has access to and benefits from health care enhanced by appropriate digital interventions.

Building on the work of the Global Commission on HIV and the Law, as well as the July 2019 UNDP Expert Consultation on *Digital Technologies and Data for HIV and Health: A Rights-*

*Based Approach*, and taking note of the new *Global AIDS Strategy 2021–2026: Ending Inequalities, Ending AIDS*,<sup>13</sup> this Guidance provides key ethical, human rights and technical considerations for countries looking to adopt digital technologies for health. It outlines key considerations from ethical, technical and social perspectives, and the human rights risks, norms and standards relevant to the use of digital technologies for HIV and health. It provides a practical checklist for assessing key ethical and rights considerations in adopting digital technologies; and finally, provides recommendations to various stakeholders.

## ..... section 2

### Key ethical, technical and social considerations for the adoption of digital health technologies

The key step in considering the adoption of digital technologies for HIV and health should be to assess whether the digital technology is needed to resolve an issue or barrier within the HIV response or health system, and whether there is evidence of the effectiveness of the proposed technological solution. Digital health technologies work best when used as a tool within a broader system to facilitate more effective HIV and health responses. Moreover, digital interventions that are built on systems whose flaws have not yet been addressed can replicate inefficiencies, exacerbate inequity, and hinder effective responses.

This section covers critical ethical, technical and social factors that countries should consider when thinking about adopting digital technologies for HIV and other health programmes. It starts with the ethical foundations and then presents other key considerations such as technical components (health technology assessments, incentivization of interoperability) and the social component of building trust.

#### 2.1

One strategy for integrating ethical, technical and social considerations is to include them in national digital health strategies together with digital literacy and workforce training, and to adopt a holistic approach to advancing accountability and justice via digital health technologies. Addressing these elements is critical to both mitigate risks of digital health interventions and to ensure their efficiency, safety and uptake.

#### Ethics and the use of digital technologies

The development, adoption and implementation of digital technologies for HIV and health should adhere to ethical standards. Various groups, such as the Institute of Electrical and Electronics Engineers, the World Economic Forum and the European Commission's High-Level Expert Group on Artificial Intelligence, have developed resources related to ethics and digital technologies.<sup>14</sup> Based on these resources, as well as on established principles in bioethics and HIV responses, key ethical considerations for digital health include:

- **Beneficence and well-being** – Digital health technologies should 'do no harm', and include an obligation to be aware of, and mitigate, harms that may occur. In addition to minimizing harmful effects, technologies should also maximize the benefits for humanity.<sup>15</sup> Benefiting human well-being must be a central tenant of digital health technologies.

- **Autonomy, informed consent, and privacy** – All individuals should be recognized as having agency over themselves and their personal information. This protection not only applies to the data collected from specific technologies, but also to data exchange mechanisms between various technologies. When personal information and/or data are collected with full informed consent, there should be safeguards to protect their integrity and security, including ‘purpose limitation’ (see Section 3 on ‘rights-based legal and regulatory framework’ below).
- **Participation and inclusion** – Technologies should be co-designed with people whose personal information and rights will be impacted by them (participatory design). Moreover, they should be involved in the implementation, monitoring and evaluation of digital health tools. Technologies should be inclusive of all within society, including the most marginalized and those most left behind.
- **Transparency** – Digital health technologies should be developed, adopted and implemented in an open and accessible manner that allows for public feedback, consultation and monitoring. This entails ensuring algorithmic transparency – i.e. the principle that factors that influence the decisions made by algorithms should be visible to the people who use, regulate and are affected by the systems that use these algorithms.
- **Non-discrimination and equity** – Digital health technologies should not deliberately or unintentionally discriminate against individuals. Moreover, to ensure equity in implementation, these technologies should account for the needs of vulnerable and marginalized groups, including women, children, racial and ethnic minorities, migrants, people living with HIV and other key populations. Effective, non-digital options should also be available and accessible to all.
- **Accountability** – Remedies should be provided for rights violations related to digital health technologies, and accountability and oversight mechanisms put in place. To this end, a variety of approaches can be taken, including fostering enabling legal and regulatory environments (i.e. litigation, complaints/user feedback mechanisms, etc.).

## 2.2 Technical considerations

Adopting and implementing digital technologies for HIV and health must consider user accessibility and their availability. This includes considering infrastructure needs, such as availability and strength of internet access and cell phone coverage. Decision makers should also consider the availability, accessibility and cost of the hardware (e.g. computer, cell phone) and software needed to use specific digital technologies. To ensure equity in the use of digital technologies, these considerations should emphasize their availability and accessibility for marginalized populations, including persons of low socio-economic status, and account for gender, race and other statuses, such as membership of a key population affected by HIV. Since new digital technologies are tools that should be used to support health systems and health outcomes, it is critical for countries to provide support services to facilitate their adoption where the infrastructure permits. Countries should also provide effective, non-digital options for end users who may otherwise be unable to access or use digital technologies.

### 2.2.1 Health technology assessments

The regulation of digital technologies is complex given the rapid pace of innovation. A health technology assessment (HTA) is a specific tool that may support the regulation of digital technologies for HIV and health. An HTA is a multi-disciplinary process that evaluates the “value of health technology at different points in its lifecycle”, including the technology’s properties, effects and impacts.<sup>16</sup> It aims to inform policymakers and influence decision-making in health care, with a focus on how best to allocate funding for health programmes and technologies. Components of an HTA include validation of technical aspects (i.e. accuracy of the product or system), clinical considerations (i.e. contribution towards improving or maintaining a specific health condition) and systems compatibility (i.e. connection and/or integration into health service provision and health systems, including medical records).<sup>17</sup> HTAs can be applied to different types of interventions, such as piloting tests, medicines, vaccines, procedures and programmes.

Applying HTAs to digital technologies provides an opportunity for governments to assess their ethical and human rights risks, including those related to equity and community acceptability. Also, HTAs may be applied to digital health interventions that involve the use of protected, personal health information or other criteria that raises human rights risks. However, there are challenges in HTAs as digital health technologies evolve rapidly. Furthermore, the technology sector’s ethos of ‘moving fast and breaking things’ is in contrast with the conventional process of health technology development and testing for patient safety and clinical efficiency, which upholds a ‘do no harm’ approach.<sup>18</sup>

To better tailor HTAs to digital health technologies with a focus on ensuring equity in availability and access, there are several key considerations. In addition to assessing the traditional technical, clinical and systems elements, integrating a strong focus on usability and human-centred design is critical. Digital technologies should be co-designed with end users and people whose personal information and rights will be impacted by them (i.e. healthcare providers, systems administrators, patients, communities). There should be subsequent, effective mechanisms for feedback and iteration; this is in line with a cornerstone of product design, that the needs of the affected communities must be met. These mechanisms also facilitate uptake and effectiveness of digital technologies, and fulfil the key ethical and human rights principle of meaningful participation and engagement. HTAs should also assess the risks for bias or discrimination as a result of access to and use of the digital health intervention. This includes reviewing a digital technology’s accessibility and availability for all users, including those left furthest behind.

### 2.2.2 Incentivizing interoperability

Interoperability is the “ability of a system or product to transfer meaning of information within and between systems or products without special effort on the part of the user”.<sup>19</sup> This data sharing can apply across organizations as well as geographic boundaries. To achieve interoperability, there must be industry-wide standards that are adopted by all relevant entities that need to share information. Within the context of health systems, interoperability is important because sharing information about the health of patients and populations in

a seamless, timely manner can improve health outcomes. Importantly, when implemented with appropriate security measures, interoperability ensures effective data portability, which allows users to transfer their data from one system to another. The standards and systems for interoperability should include safeguards that protect the autonomy and privacy of users, with their central tenants focused on efficiency and effectiveness, as well as individual and population well-being. Interoperability must also have strict limitations to protect against ‘function creep’ – i.e. the use of collected data for purposes beyond its original intent. This is especially important in a context where information may be collected on criminalized or highly stigmatized populations.

Interoperability, while desirable within the HIV response and health-care sector, may require some incentivization. Digital technology developers and health-care entities may have economic incentives to make data sharing more difficult or expensive. Other challenges include lack of coordination among various entities within the health sector, as well as the fact that different institutions have differing policies related to data privacy and security.<sup>20</sup> To encourage interoperability, some countries have established incentivization programmes that provide funding for entities that adopt such technologies. These initiatives could also be offered to promote interoperability of systems that encompass strong privacy and data protections in order to address ethics and human rights considerations.

### 2.3 Social considerations – building trust

A core component of successful HIV responses, trust is also a key element in the adoption and success of digital technologies for health. Without trust, the implementation and uptake of digital health will be weak, even if all other aspects of infrastructure, as well as legal and regulatory frameworks, are effective. Trust must be built for all types of relationships related to digital health – between patients and health-care providers; within the health sector institutions; between the State and its residents; and between a State, its residents and the private sector. Strategies to foster trust that will enable the adoption and use of digital health technologies include:<sup>21</sup>

- being consultative and transparent in decision-making related to governance and management of digital technologies – this includes being transparent about and accountable for the factors that influence algorithmic decisions;
- establishing impartial, effective accountability and oversight mechanisms for breaches of data privacy and other rights violations;
- co-designing digital technologies and systems with affected communities, and creating monitoring and evaluation systems that allow the technologies to adapt based on feedback, where possible;
- investing in creating opportunities for digital rights literacy for communities and individuals to understand their rights and take ownership of their data, including the right to withdraw their data from use and to data portability;
- creating spaces for dialogue between various key stakeholders, such as the State, the private sector, civil society and communities.

## 2.4 Integrating ethical, technical and social considerations into the adoption and use of digital interventions for HIV and health

### 2.4.1 National digital health strategies

One way to avoid the ad hoc development of digital health technologies is the adoption of a national digital health strategy. Digital health strategies can facilitate coordination, set standards for interoperability, and establish policies related to digital health.<sup>22</sup> A country-wide strategy is also helpful for identifying gaps and opportunities where digital technologies can be best leveraged to improve health outcomes. The 2019 report of the Global Digital Health Index (GDHI) indicates that, out of the 22 current GDHI countries, Bangladesh, Jordan, Malaysia, Portugal, Thailand and the Philippines have the most advanced processes, policies and practices for digital health.<sup>23</sup>

One of the strategic objectives of the new WHO Global Strategy on Digital Health 2020–2025 aims to “stimulate and support every country to own, adapt and strengthen its strategy on digital health”.<sup>24</sup> There are some key characteristics for effective national digital health strategies. They should be developed in a consultative and transparent manner that accounts for the needs of vulnerable and marginalized communities and those living in urban, rural, as well as crisis and conflict settings. They should also have political support from a variety of different entities, including the government sectors that deal with health, communications, economics and data protection, human rights, and corruption, civil society organizations, communities and the private sector.<sup>25</sup> National digital health strategies should be coordinated and coherent with other relevant policies, including broader national digital transformation strategies. They should undergo periodic reviews to ensure relevance and recognize the rapid evolution of digital health technologies.

### 2.4.2 Digital literacy

For national digital health strategies to succeed, individuals and health professionals must be digitally literate and aware of the human rights protections relevant to digital health. Accordingly, the WHO *Global Strategy on Digital Health, 2020–2025* recognizes that advancing digital literacy, including through investments in the education, training and continued professional development of the health workforce, is critically important.<sup>26,27</sup> A global framework for measuring digital literacy is still underway. However, the challenge of digital literacy is particularly acute in low- and middle-income countries given the global disparities between developed and developing countries in access to computing and information resources including the Internet and the opportunities derived from this access.<sup>28</sup> For example, most of the countries participating in the GDHI provide weak pre- and in-service training for health professionals: 20 of the 22 countries either do not provide digital health pre-service training to health-care personnel or only do so for less than 25 percent of their workforce.<sup>29</sup> Limited efforts have been made to engage HIV or tuberculosis (TB) key and vulnerable populations, who may have frequent contact with the health sector and experience stigma and discrimination,<sup>30</sup> in digital health literacy initiatives.

### 2.4.3 Biometric and digital identify

For people without an officially recognized legal identity (ID) document, accessing basic services, including HIV and health service, can be a major barrier.<sup>31</sup> Digital ID systems with unique biometric features are mediating this problem, and there has been an accelerated adoption of digital ID systems, especially in low- and middle-income countries.<sup>32</sup> While the goal of establishing national digital ID systems as the basis of public service delivery presents opportunities for improving access to service and reducing corruption and wastage, they also pose the risk of excluding already marginalized populations, such as people living with HIV and key populations in criminalized settings, if proper safeguards are not in place to mitigate these risks.<sup>33</sup>

### 2.4.4 Advancing accountability and justice

Within national digital health strategies, countries should consider how digital interventions can advance broader efforts to promote accountability and justice. For example, within the HIV response, eHealth apps may be used by community members to monitor medication stockouts<sup>34</sup> (e.g. antiretroviral therapy in the HIV response) or to address discriminatory treatment in health-care facilities.<sup>35</sup> They may also facilitate reports of abusive law enforcement practices against vulnerable and key populations. Regarding equity considerations for data and digital health interventions more broadly, governments should consider representational visibility of data, i.e. considering whose data are being collected (there must be a balance to ensure that the most marginalized are visible for critical services, but not targeted for discriminatory purposes), and how best to promote transparency and equity related to data and technological innovations (e.g. open source software and open data sets).

### 2.4.5 Tackling corruption in the health sector

Each year an estimated US\$7.5 trillion is spent worldwide on providing health services, yet as much as 6%, or approximately \$455 billion, is lost to corruption.<sup>36</sup> Corruption in the health sector undermines public trust, wastes resources, violates human rights, and negatively impacts health outcomes for the most vulnerable. Digital technology can serve as a powerful contributor to anti-corruption, transparency and accountability efforts, and can be leveraged to detect and deter corruption while promoting citizen trust and engagement. For instance, digital initiatives have included: open-contracting policies to correct information asymmetries among the multitude of actors involved in procurement processes;<sup>37</sup> electronic logistics management information system (eLMIS) that use smartphone and cloud-based technology to capture real-time data across the entire vaccine cold chain;<sup>38</sup> and digital payment platforms to reduce the risk of fraud and verify cash transfers.<sup>39</sup>

## The rights-based legal and regulatory framework

From their design to their adoption and implementation, digital technologies for HIV and health can raise human rights concerns. This section provides a short overview of some key human rights risks that have been identified in digital technologies for HIV and health. The section then discusses human rights obligations of States and private actors that arise from global, regional and national agreements, and norms and standards.

### 3.1 Human rights risks and digital technologies

Despite the opportunities that digital technologies can bring by creating more effective and efficient HIV and health responses, their adoption should take into account key human rights considerations, such as those related to privacy and non-discrimination. This is especially relevant in the HIV response, given the disproportionate impact of the disease on marginalized, stigmatized and criminalized communities.<sup>40</sup> Although there are many specific causes of human rights risks related to the use of digital technologies, focus will be placed here on the following three common causes – data breach, bias and function creep.

#### 3.1.1 Data breach

A ‘data breach’ refers to any breach of security that leads to the “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”.<sup>41</sup> Data breaches are common in the health sector and have a variety of causes – from malware and hacks, to accidental or purposeful disclosure of personal health information by health-care employees.<sup>42</sup> There have been several recorded incidents of protected health information data breaches globally, including the leak of the personal information of about 14,000 people living with HIV in one particular incident.<sup>43</sup> Data breaches violate an individual’s right to privacy and erode trust in the health-care system. As technology evolves and health systems become more complex, the likelihood of data breach occurrences increase. Health systems should invest in information security and keep up to date on the latest in data protection to prevent breaches.

#### 3.1.2 Bias

Discrimination resulting from biases present in algorithms of AI and other automated processes has been repeatedly documented across a wide range of applications. This phenomenon, also known as ‘algorithmic bias’, can amplify discrimination in criminal justice proceedings and predictive policing, facilitate discriminatory hiring decisions, and produce targeted online marketing campaigns with discriminatory effects.<sup>44</sup> Within health care, studies examining applications of AI have demonstrated that algorithms do not provide equally accurate predictions of health outcomes across race, gender, or socio-economic status. For example, one study that analysed AI predictions for intensive care unit mortality found that use of AI resulted in a higher error rate for female patients than for males.<sup>45</sup> These biases are reflective of the underlying bias in data used for the development of AI and machine learning applications, and the limited comprehensiveness of relevant variables in many existing datasets used to develop algorithms. This raises concerns over an individual’s right to non-discrimination. Additionally, certain types of algorithmic decisions



evade current non-discrimination laws,<sup>46</sup> leading to unfair differentiation that is technically legal (e.g. offering differing prices for the same product based on speed of internet access, etc.), but still counterproductive to health equity aims of digital technology application.

### 3.1.3 Function creep

'Function creep' refers to the "gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy".<sup>47</sup> Concretely, there is function creep when data collected for a specific purpose (e.g. as personal history information for HIV testing or treatment) are used for another purpose (e.g. to check immigration status). Concerns over function creep are present in all forms of digital technology application for health (e.g. molecular surveillance), but especially in relation to biometrics. Potential risks of biometric data include abuse of data for different purposes, such as forensics or criminal proceedings.<sup>48</sup> Function creep can also lead to data breaches, particularly among marketable technologies for health. For example, wearables are often produced and managed by private companies with greater interest in collecting and monetizing personal information than in protecting it, which poses a significant threat to the data privacy of individuals. Government partnerships with private companies, including big technology companies, have also raised alarms related to the exploitation of data for surveillance as well as commercial purposes.<sup>49</sup>

Good practices for data privacy to prevent function creep centre on the principle of 'purpose limitation', i.e. data can only be collected and used for an explicit and legitimate purpose. If a new purpose arises, informed consent must again be solicited and given for the data to be used in such a manner (for more information, see 3.4 below for more on data privacy and security protection).

## 3.2 International human rights standards for States

Human rights obligations apply to States in digital environments in the same manner that they apply in offline environments. While there is no specific global human rights agreement for digital technologies, many existing human rights obligations apply. The most relevant state obligations for the adoption of digital technologies for HIV and health are the rights to health, non-discrimination, benefits from scientific progress and privacy. Although States are primarily responsible for respecting, protecting and fulfilling human rights obligations, private companies that are domiciled or conduct business within a State's jurisdiction must also, at a minimum, respect human rights standards. Given that digital health technologies may be used across multiple countries and jurisdictions, international human rights law provides uniform standards for States' obligations, making it a strong foundation on which to build the governance framework for such technologies.

### 3.2.1 Right to health

The right to health is enshrined in various human rights treaties, including Article 12 of the International Covenant on Economic, Social and Cultural Rights.<sup>50</sup> The Committee on Economic, Social and Cultural Rights has noted that the right to health is interrelated and "indispensable for the exercise of other human rights. Every human being is entitled to the

enjoyment of the highest attainable standard of health conducive to living a life in dignity”.<sup>51</sup> The following four key elements comprise the right to health:

- Availability – Health facilities, goods and services must be available in adequate quantities within a country.
- Accessibility – Facilities, goods and services must be sufficiently accessible and provided in a non-discriminatory manner. ‘Accessibility’ refers to various form of access, including economic accessibility (affordability), physical accessibility (e.g. services are within reasonable travel distances and/or meet the needs of persons with disabilities) and information accessibility.
- Acceptability – Facilities, goods and services must be culturally appropriate, including for marginalized and vulnerable groups, and respect medical ethics, such as maintaining privacy and confidentiality.
- Quality – Facilities, goods and services must be of good quality, and based on scientific and medical evidence.<sup>52</sup>

Core obligations of the right to health include ensuring:

- access to health facilities, goods and services on a non-discriminatory basis, especially for vulnerable or marginalized groups;
- access to the minimum essential food that is nutritionally adequate and safe to ensure freedom from hunger to everyone;
- access to basic shelter, housing and sanitation, and an adequate supply of safe and potable water;
- the provision of essential drugs, as defined under the WHO Action Programme on Essential Drugs;
- equitable distribution of all health facilities, goods and services;
- the adoption and implementation of a national public health strategy and plan of action, based on epidemiological evidence, which address the health concerns of the whole population.<sup>53</sup>

While the right to health is subject to progressive realization, there are immediate state obligations that must be met, including executing the right in a non-discriminatory manner and recognizing that the country has a “specific and continuing obligation to move as expeditiously and effectively as possible towards the full realization” of the right to health.”<sup>54</sup>

The adoption of digital technologies for HIV and health must, at a minimum, satisfy the four key elements of the right to health (availability, accessibility, acceptability and quality). These key elements have also been recognized as elements of the right to enjoy the benefit of scientific progress and are applicable to digital technologies.<sup>55</sup> Indeed, addressing availability and accessibility of digital technologies for HIV and health supports efforts to bridge the digital divide. These obligations require governments to ensure the availability and accessibility of digital infrastructure throughout the country, both in terms of hardware (e.g. computers, mobile phones, mobile phone towers, internet, and broadband accessibility) and software (e.g. applications). This also includes providing digital literacy training for all users, such as those in leadership, health care and communities.<sup>56</sup> Digital

technologies for HIV and health should be a step towards supporting countries to realize the right to health; hence, they must be reasonably accessible to all communities, especially those that are left furthest behind. Moreover, with respect to the right to health, acceptability of digital technologies entails not only ensuring the right to privacy and confidentiality, but also meeting the needs of different populations.<sup>57</sup> Finally, digital health technologies must be of quality; for example, those that attempt to replace in-person care should be held to the same norms and standards.

### 3.2.2 Right to non-discrimination

The right to non-discrimination is found throughout various global treaties, beginning with the International Covenant on Civil and Political Rights (ICCPR).<sup>58</sup> States must uphold the right to non-discrimination both as a right in itself and as a principle that is inherent in the realization of other rights (e.g. entitlement to equal treatment before an impartial tribunal). Human rights law defines discrimination as:

“ [...] any distinction, exclusion, restriction or preference which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms”.<sup>59</sup>

‘Other status’ has been interpreted under human rights law to include HIV and other health status, as well as sexual orientation and gender identity.<sup>60</sup> Importantly, the right to non-discrimination does not imply identical treatment for all – some instances may necessitate differential treatment to ensure that individuals are on equal footing. Differential treatment does not constitute discrimination where the criteria for such differentiation are “reasonable and objective and if the aim is to achieve a purpose which is legitimate” under human rights law.<sup>61</sup>

Emerging and new technologies raise two main categories of concerns related to non-discrimination. The first focuses on their access and availability, while the second focuses on implicit biases within them. Relying on digital technologies as a primary system or strategy within the health sector may impact access and availability, and inadvertently exacerbate inequalities, contributing to the digital divide. This may be due to a myriad of reasons including limited technical infrastructure (e.g. broadband access, satellite towers), lack of digital literacy, expense, and lack of access to digital hardware (e.g. mobile smart phones, computers).<sup>62</sup> Human rights and technologies experts recognize that the design of various digital technologies may include implicit and inadvertent biases. Engineers and software developers tend to be based primarily in the Global North, and to design technologies with limited engagement and inputs from diverse communities, such as those that are inclusive of race, gender and socio-economic backgrounds.<sup>63</sup>

To realize the right to non-discrimination in the context of digital technologies, States must proactively identify risks to non-discrimination in access and availability of technologies, and hold private businesses to account in identifying, mitigating and redressing discriminatory outcomes.<sup>64</sup> States should also ensure transparency and accountability related to the

development, adoption and implementation of digital technologies for health, as well as provide access to justice where the right to non-discrimination or other rights have been violated. Finally, there should be an effective, non-digital option that achieves the same goal for those who are unwilling or unable to use digital technologies.<sup>65</sup>

### 3.2.3 Right to enjoy the benefits from scientific progress

Article 15 of the International Covenant on Economic, Social and Cultural Rights enshrines the right to enjoy the benefits from scientific progress.<sup>66</sup> Like the right to health, States must take deliberate, concrete steps towards the realization of their obligations within a reasonable time frame. Moreover, States are:

“under an immediate obligation to eliminate all forms of discrimination against individuals and groups in their enjoyment of economic, social and cultural rights. This duty is of particular importance in relation to the right to participate in and to enjoy the benefits of scientific progress and its applications because deep inequalities persist in the enjoyment of this right”.<sup>67</sup>

The Committee on Economic, Social and Cultural Rights recognizes that the right to participate in and enjoy the benefits from scientific progress are fundamental to achieving the right to health. States have a duty to ensure availability and accessibility to “all the best available applications of scientific progress necessary to enjoy the highest attainable standard of health” on a non-discriminatory basis, with a focus on the most marginalized.<sup>68</sup> States are obliged to fulfil this duty to the maximum of their available resources. The Committee notes that States must balance the benefits and risks, specifically of emerging and new technologies. It underscores that new technologies should be developed and used within an inclusive, rights-based framework, highlighting the principles of transparency, non-discrimination, accountability, and respect for human dignity. The Committee also emphasizes the importance of developing laws that impose an obligation of human rights due diligence on private and other non-state actors. States must also regulate the control and ownership of data collected through new technologies to prevent misuse and exploitation, as well as ensure informed consent and privacy.<sup>69</sup>

### 3.2.4 Right to privacy

Article 17 of the ICCPR recognizes everyone’s right to be free from arbitrary or unlawful interference with their privacy.<sup>70</sup> This requires States to adopt laws, policies and practices that realize this right. Any lawful interference with this right must be precisely outlined in relevant legislation.<sup>71</sup> Moreover, States must regulate the collection and storage of personal information – these measures must be effective to prevent unauthorized disclosure or use of personal information.<sup>72</sup> Such information can never be used for any purposes that are incompatible with the aims of the ICCPR. In addition, individuals have the right to know what personal data are stored in databases and the purposes of such storage. They also have the right to request rectification or elimination of files that contain incorrect personal information or “have been collected or processed contrary to the provisions of the law”.<sup>73</sup> Choice of technology is an important factor in realizing the right to privacy – digital health technologies should build on and utilize platforms and processes that minimize privacy

risks, for example, using blockchain technology or exploring Bluetooth-based apps as a less-intrusive alternative to GPS tracking for contact tracing. Governments should also be aware of the privacy and security concerns that are not only related to a digital technology, but also to any data exchange mechanisms that they may use. For further elaboration on the right to privacy in the context of digital technologies, see the section 3.4 below on legal principles from regional and United Nations agreements.

### 3.2.5 The role of courts in upholding human rights in the digital age

Courts have historically played a key role in protecting human rights, including the right to health. Within the HIV response, judicial decisions have advanced a range of rights and freedoms, notably access to antiretroviral treatment as part of the right to health.<sup>74</sup> It is important to note that the obligations of States provided in international human rights treaties apply online as well as offline, which include respect for human rights and fundamental freedoms in the use of information and communication technologies.<sup>75</sup> These obligations must inform actions and policies relating to digital cooperation and digital technology. For the use of digital technologies, judiciaries around the world have led the way in protecting rights. Court decisions from India, Jamaica and Mauritius have recognized the right to privacy, as well as the importance of data protection related to digital technologies.<sup>76</sup> In a similar vein, in January 2020, the Kenyan High Court held that the Government's proposed biometric identification system required stronger privacy and data protections before it could proceed. The Court prohibited the Government from collecting individuals' DNA and location data as part of this initiative.<sup>77</sup> Moreover, a court in the Netherlands noted concerns over algorithm-related discrimination, calling for the Government to ensure transparent use of digital technologies and privacy safeguards.<sup>78</sup>

## 3.3 Human rights obligations of private businesses

The private sector plays a dominant role in the field of digital technologies and can inadvertently contribute to human rights infringements from their deployment. States have several obligations related to the action of business enterprises: they must protect against human rights abuses within their jurisdictions by third parties, including by private actors. This includes providing access to justice when business-related human rights violations arise. Governments must also set expectations that businesses domiciled in or operating within their jurisdiction must respect human rights, including by conducting human rights due diligence and taking into account issues related to gender and marginalization.

Although only States can be party to human rights treaties, there have been legal and normative developments that recognize that businesses and private companies must also comply with laws and respect human rights.<sup>79</sup> Respecting human rights requires private companies to:

- “ (i) avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; and (ii) seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts”.<sup>80</sup>

In alignment with these principles, companies should develop and enact human rights policy commitments and conduct human rights due diligence. This due diligence comprises ongoing processes that involve assessing human rights impacts, acting to prevent or mitigate impacts, tracking to see how concerns are addressed, and remedying any violations that it caused or to which it contributed.<sup>81</sup> Business enterprises should treat the obligation to respect human rights as a legal compliance issue in all jurisdictions in which they operate or are domiciled.

### 3.4 Legal principles from regional and United Nations agreements on data privacy and security

While there is no global treaty on data security and protection, there are several regional agreements and principles that set standards on these issues, which include the African Union Convention on Cyber Security and Personal Data Protection,<sup>82</sup> the Asia-Pacific Economic Cooperation (APEC) Privacy Framework,<sup>83</sup> the European Union's General Data Protection Regulation<sup>84</sup> (EU GDPR) and the Standards for Personal Data Protection for Ibero-American States.<sup>85</sup> The Council of Europe (CoE) also has the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), which is open for accession by non-member States.<sup>86</sup> Moreover, the United Nations system has also developed strong ethical principles on data security and privacy that aligns with regional standards.<sup>87</sup> The following legal principles are drawn from these standards.

#### 3.4.1 Rights of the data subject

Data privacy and security agreements enshrine a set of rights for the individual whose data are being collected (i.e. the 'data subject'),<sup>88</sup> including:

- the right to be informed about where data are and are not collected;
- the right to access stored data;
- the right to rectification;
- the right to erasure (i.e. the 'right to be forgotten');
- the right to restriction of processing;
- the right to be notified of rectification or erasure or restriction of processing;
- the right to data portability (i.e. an individual's right to request and receive personal data provided to one data controller in a structured, commonly used and machine-readable format or to have it transmitted directly to another data controller);
- the right to object;
- the right related to automated decision-making and profiling.

#### 3.4.2 Data collection and processing

Data must be collected and processed in a manner that:

- fulfils the requirements of lawfulness, fairness and transparency to the data subject;
- aligns with a legitimate purpose that is clearly specified and agreed to by the data subject (i.e. purpose limitation);
- is the minimum necessary for the legitimate purpose (i.e. data minimization);
- for personal and identifiable data, are only stored for as long as necessary for the specified, legitimate purpose (i.e. storage limitation);

- ensures appropriate security, as well as data integrity and accuracy;
- ensures that the entity that controls the data demonstrates compliance with all principles of data processing (i.e. accountability of data controller).<sup>89</sup>

In addition, a data subject's informed consent to data collection and processing must be voluntarily given in an unambiguous agreement to a request that is presented in clear and plain language. The data subject has the right to withdraw consent at any time.<sup>90</sup>

### 3.4.3 Data security and confidentiality

- Entities that process data must implement safeguards to ensure data security,<sup>91</sup> including anonymization or pseudonymization (whichever is more appropriate for the data collected), as well as encryption of personal data.
- Entities must also ensure transparency in the processing of data so that the data subject can monitor data processing, and the data controller can create and improve security features.<sup>92</sup>
- Certain categories of sensitive data may only be processed where appropriate legal safeguards are met, most notably those that mitigate risks to the rights and fundamental freedoms of data subjects. Such categories include genetic data, personal data related to criminal offences, unique identifying biometric data, and personal data that reveal a person's racial or ethnic origins, political opinion, religious and other beliefs, health and sexual life.<sup>93</sup>

### 3.5 Looking forward: Opportunities to advance human rights standards for digital health technologies

While there are several human rights obligations that States must fulfil in relation to digital technologies, there are also various opportunities to build on and develop new standards for digital health interventions. The most directly relevant is the Special Rapporteur on the Right to Privacy's *Recommendation on the Protection and Use of Health-related Data*.<sup>94</sup> The Recommendation covers key topics such as rights of the data subject, security and interoperability, transborder data flow, as well as considerations related to data and gender, indigenous populations and persons with disabilities. Moreover, the Special Rapporteur on Contemporary Forms of Racism is developing a report on new information technologies, non-discrimination and racial equality.<sup>95</sup> The United Nations' Chief Executive Board is also developing a recommendation on the ethics of artificial intelligence (AI).<sup>96</sup> These developments, together with the standards established by human rights law and the guidance from rights-based principles and experts,<sup>97</sup> will facilitate more just, ethical and rights-respecting uses of digital health interventions.

Digital technologies have the potential to reduce inequities and barriers to accessing quality HIV and other health-care services. They have the potential to decrease health-care costs, transform health systems to provide more accurate and responsive care, and break down siloes between sectors. However, these opportunities must be developed, implemented and monitored in a way that respects, protects and fulfils ethics and human rights. The adoption of digital health technologies in this manner will truly protect and empower individuals, thereby helping countries fulfil their commitment to leaving no one behind.

## Checklist for assessing key ethical and rights considerations in adopting digital technologies for HIV and health

Aligned with the recommendations for the use of digital technologies for HIV and health, below is a checklist to support countries in their decision-making on the adoption of digital health interventions. The checklist focuses on whether the adoption of the technology will help countries realize the right to health, and whether appropriate safeguards are in place to protect users.<sup>98</sup>

Checklist to support countries in their decision-making on the adoption of digital health interventions	
Key considerations	<input checked="" type="checkbox"/>
<b>Threshold questions</b>	
Is this technology needed to address or resolve a critical issue or barrier within the HIV response or health system? Will it facilitate or streamline access and/or quality of facilities, goods and/or services (e.g. considerations of complementarity of systems, technology as a tool for good)?	<input type="checkbox"/>
Is there objective evidence on the clinical effectiveness of the proposed technological system or intervention for achieving the proposed HIV or health goal?	<input type="checkbox"/>
Is this technology reasonably accessible to the population that should benefit from its design and implementation (e.g. if the technology requires mobile smart phones, do most people have them)?	<input type="checkbox"/>
Has this technology been co-designed with users and/or has meaningful consultation with and input from communities been sought?	<input type="checkbox"/>
<b>Availability</b>	
Logistics support: Are there technological and other fundamental infrastructure in place to support the implementation and uptake of this technology to meet the HIV or health goal (e.g. access to internet and/or mobile phone coverage throughout the country, even in rural areas, etc.)?	<input type="checkbox"/>
<b>Accessibility</b>	
User access: Do end-users have the hardware (e.g. computers, mobile smart phones) and software necessary for accessing and using this technology?	<input type="checkbox"/>
Is the government able to provide access to hardware or software for users and/or areas where it is currently not available or accessible?	<input type="checkbox"/>
Will end-users incur any costs for using this technology, and if so, are they affordable and/or covered by insurance?	<input type="checkbox"/>
Is the technology accessible to specific requirements from people, such as persons with disabilities, the elderly and children?	<input type="checkbox"/>
Is the technology available to, and appropriate for, vulnerable communities, including but not limited to people in prisons and closed settings, people who are internally displaced and/or those in refugee or informal settlements?	<input type="checkbox"/>



## Checklist ... continued

Key considerations



### Acceptability

Is the technology available in the necessary languages? Are they tailored to take into account user experience based on gender, sex, ethnicity, or other major factors (such as membership to a key population group)?

Is the technology culturally appropriate within various communities?

Is training or are resources for training available in plain language and accessible formats to support digital literacy for a specific technology among health-care professionals and end users?

Has the specific digital technology been tested, piloted, or implemented to achieve the expected HIV or health goal?

### Data privacy and security

(Are there laws and regulations in place that outline clear legal standards on data privacy and security?)

Data collection:

- Are there clear informed consent requirements for data collection? Consent should be freely given, specific, informed and unambiguous, and the request presented should be in clear and plain language, with the purpose explicitly specified.
- Do the regulations specifically outline legitimate and lawful purposes for data collection?!
- Are there data minimization requirements (i.e. collecting the minimum necessary for the legitimate purpose)?

Storage and authorized use:

- Are there requirements for the data collected to be kept accurate, and if necessary, up-to-date?
- Are there standards that data processing methods ensure appropriate security and data integrity, including anonymization, where relevant, and rigorous processes to ensure authentication for authorized users and encryption?
- Are there mandates that personal, identifiable data can only be stored as long as necessary for the specified purpose (e.g. limited retention)?

Are there heightened protections for the collection and storage of special categories of data, including genetic data, personal data related to criminal offences, unique identifying biometric data, as well as personal data that reveal a person's racial or ethnic origins, political opinion, religious and other beliefs, health and sexual life?

Rights of the data subject: Do the applicable laws and policies include the following rights for individuals whose data are collected?

- the right to be informed of the use of their collected data;
- the right to access stored data;
- the right to rectification;
- the right to erasure;
- the right to restriction of processing;
- the right to be notified of rectification or erasure, or restriction of processing;
- the right to data portability;
- the right to object;
- rights related to automated decision-making and profiling.

### Checklist ... continued

Key considerations	<input checked="" type="checkbox"/>	
<b>Health-related surveillance<sup>100</sup></b> (including contact tracing)	Are the proposed surveillance measures lawful and for legitimate public health objectives?	<input type="checkbox"/>
	Are the measures strictly necessary and proportionate to the health objectives?	<input type="checkbox"/>
	Are there explicit measures in place to ensure transparency in the development and implementation of the technology, as well as the use of data collected (including any agreements with private actors)?	<input type="checkbox"/>
	Does the surveillance technology involve the meaningful and active engagement of key stakeholders, including civil society and communities, in its development, implementation and monitoring?	<input type="checkbox"/>
	Are there user notification requirements?	<input type="checkbox"/>
	Are there legal and regulatory protections for data privacy and security (in collection, storage and use), including the above-mentioned data and privacy requirements?	<input type="checkbox"/>
	Are there safeguards to mitigate risks of discrimination or other rights abuses for marginalized groups?	<input type="checkbox"/>
	Is there access to redress and justice for users who may have their rights violated through the use of the technology?	<input type="checkbox"/>
	Is there an institution or entity that can provide public oversight, review and accountability on the use of the technology?	<input type="checkbox"/>
	If the technology is for a specific, time-limited purpose (i.e. COVID-19 or any outbreaks), is its use time-bound?	<input type="checkbox"/>
<b>Non-discrimination</b>	Can pre-existing laws related to non-discrimination be applied to the impact and uptake of digital technologies?	<input type="checkbox"/>
	How well are private companies regulated in terms of legal compliance regarding human rights issues? Are there mandatory provisions for human rights due diligence?	<input type="checkbox"/>
<b>Accountability and access to justice</b>	Are private actors required to have policy commitments to human rights and to conduct human rights due diligence in order to be legally compliant with the business regulations within the country?	<input type="checkbox"/>
	Do individual and entities have the rights to bring cases related to potential discrimination as a result of digital technologies before courts (i.e. are technology-related discrimination claims justiciable)?	<input type="checkbox"/>
	Are there other mechanisms and or interventions available to support access to justice for technology-related human rights violations (e.g. impartial courts specializing in surveillance issues, training for judges and law enforcement on the use of digital technologies, etc.)?	<input type="checkbox"/>

## Recommendations for the ethical and rights-based adoption of digital technologies for HIV and health

The following recommendations emerge based on the ethical, technical, social and rights-based legal considerations of digital health technologies for HIV and health. These recommendations are for governments and other stakeholders, such as private sector companies and donor agencies.

### 5.1 Recommendations for governments

To ensure that the development and use of digital technologies for HIV and health are consistent with universal human rights obligations and ethical principles, governments should adopt the following:

#### 5.1.1 The right to health

Ensure that the use of digital technologies for HIV and health uphold – and are a step towards the progressive realization of – the right to health and the right to benefit from scientific progress. Specifically, uses of digital technologies for HIV and health must, at a minimum, advance equity within availability, accessibility, acceptability and quality.

#### 5.1.2 The right to non-discrimination

- a. Proactively identify and mitigate risks to non-discrimination in access and availability of technologies, as well as privacy and confidentiality. Where private actors are involved, hold businesses to account in identifying, mitigating and redressing discriminatory outcomes, as well as privacy and data security violations (human rights due diligence).
- b. Enact an effective, non-digital option that achieves the same HIV and/or other health goal for those who are unwilling or unable to use digital technologies.
- c. For accountability purposes, ensure that non-discrimination laws and policies can be applied to the development, implementation and use of digital technologies for HIV and health.

#### 5.1.3 The right to privacy

- a. Establish and implement laws, policies and regulations on informed consent for data collection and use of digital technologies for HIV and health.
- b. Update and/or enact privacy laws, policies and regulations to safeguard the integrity and security of personal information/data.
- c. Within privacy laws and regulations, recognize the rights of data subjects, including:
  - the right to be informed about where data are and are not collected;
  - the right to access stored data;
  - the right to rectification;
  - the right to erasure (i.e. the ‘right to be forgotten’);
  - the right to restriction of processing;
  - the right to be notified of rectification or erasure or restriction of processing;
  - the right to data portability;
  - the right to object;
  - rights related to automated decision-making and profiling.

- d. Guarantee heightened protections for special categories of data (e.g. genetic data, personal data related to criminal offences or racial or ethnic origin, and biometric data) with appropriate legal safeguards to mitigate risks to the rights and fundamental freedoms of data subjects.

#### 5.1.4 Access to justice

Ensure that there are legal, regulatory and other accountability mechanisms to facilitate access to justice and redress for violations of human rights as a result of the development, implementation or use of digital technologies for HIV and health.

#### 5.1.5 Cross-cutting human rights obligations

- a. Ensure that all digital technologies for HIV and health are aligned with ethical considerations including the obligations of: beneficence; lawfulness; autonomy, consent, and privacy; participation and inclusion; transparency; non-discrimination and equity; and accountability.
- b. Ensure meaningful participation of end users and affected communities in the design, implementation and monitoring of digital technologies for HIV and other health services.

#### 5.1.6 Country strategies that support adherence to human rights and ethical obligations:

- a. Conduct rigorous baseline assessments of the HIV or health needs in partnership with the communities who are targeted benefit from the technology, assessing the challenges and identifying potential, effective interventions, and then making a decision about whether the best intervention is based on digital technology, the improvement of analogue systems, or a combination of both.
- b. Ensure that there are robust, principles-based regulations, with accessible accountability mechanisms that digital health technologies must comply with, including HTAs tailored to review the technical, clinical, systems and ethical aspects of digital interventions.
- c. Develop, implement and institutionalize digital literacy training for health-care professionals, end users/communities and other relevant stakeholders to facilitate access and uptake of digital technologies.
- d. Maximize interoperability of digital health technologies and systems to facilitate more effective and efficient HIV and other health service access and provision. However, safeguards must be enacted to protect personal information from being modified or accessed beyond the specified health purposes, especially for criminalized or highly stigmatized groups.
- e. Enact and periodically update a national digital health strategy that governs a country's approach to the adoption and use of digital technologies for HIV and health. The development of the strategy should be a consultative process that includes meaningful participation of relevant stakeholders and communities.

#### 5.2 Recommendations for the private sector and technology companies

Ensure that the development and use of digital technologies for HIV and health are consistent with universal human rights obligations and ethical principles, as follows:

- a. In line with the Guiding Principles on Business and Human Rights, prevent or mitigate adverse human rights impacts that are directly linked to their operations, products, or services, even if they have not contributed to these impacts.
- b. Develop and enact human rights policy commitments and conduct human rights due diligence. This due diligence comprises ongoing processes that involve assessing human rights impacts, acting to prevent or mitigate impacts, tracking to see how concerns are addressed, and remedying any violations caused by digital technologies or to which they may have contributed.
- c. Ensure alignment with ethical standards related to the development, implementation, monitoring and overall use of digital technologies for HIV and other health issues.
- d. Establish and implement clear accountability systems for digital technologies that violate human rights.

### 5.3 Recommendations to donor agencies

To ensure that the development and use of digital technologies for HIV and health are consistent with universal human rights obligations and ethical principles, donors should adopt the following:

- a. Before funding or advocating for a digital health technology-focused project, conduct due diligence in assessing and understanding the gaps within a health system, which interventions may improve or address them, and how and if digital technologies may be used to support an effective intervention.
- b. Ensure that any digital technologies supported within projects or grants align with human rights and ethics principles, and that these interventions advance core elements of the right to health, including availability, accessibility, acceptability and quality. Technologies must also store data in a manner that safeguards privacy, confidentiality and security.
- c. Ensure that partnerships with the private sector and technology companies are thoroughly vetted so that they proceed in a manner that best protects and advances human rights, including the rights to health and non-discrimination.

## Annex: Overview of common digital technologies

Digital technologies are applied in numerous ways to support and enhance HIV and health programmes worldwide. This section highlights some examples of how they are currently used to support HIV interventions and health systems more generally.

Digital health interventions can be broadly categorized according to those that primarily target (i) individuals, (ii) health-care providers, or (iii) health systems management; as well as those that are (iv) cross-cutting and used in health research.<sup>101</sup> This section summarizes some common digital technologies currently used in HIV and other health responses, and highlights ethical and human rights concerns specific to individual technologies. However, since many digital health interventions share common concerns over data integrity, privacy and confidentiality, among other rights-related concerns, these cross-cutting risks are presented and addressed in section 4 as a part of a broader discussion of rights-based legal and regulatory frameworks.

### 1 Individuals

A range of digital health technologies have been developed specifically targeting the needs of individuals. This section provides an overview of eHealth interventions (including mHealth), wearables and point-of-care diagnostics.

#### 1.1 eHealth technologies

The World Health Organization (WHO) defines electronic health (eHealth) as “the use of information and communication technologies for health”.<sup>102</sup> Although eHealth can be defined broadly enough to include many of the other interventions covered in this section, basic eHealth technologies encompass the use of mobile phones (also known as mHealth) and websites to deliver medical or public health information. These technologies aim to facilitate the work of health providers and/or provide information or reminders to individuals. These interventions are low-cost and low-touch (i.e. minimal effort required by humans), and allow for customization of health information. Examples include: the use of mobile phone-based initiatives to deliver targeted health messages to pregnant and postpartum women,<sup>103</sup> the use of messaging applications (e.g. WhatsApp, Telegram) and internet outreach to facilitate access to harm reduction information for people who use drugs,<sup>104</sup> and the use of social media to address HIV-related stigma, encourage HIV testing and treatment<sup>105, 106</sup> and to disseminate verified information on COVID-19 and HIV to young people.<sup>107</sup>

#### 1.2 Wearables

Wearable technologies (or ‘wearables’) are electronic devices worn close to and/or on skin, designed to collect biometric health information (e.g. heart rate, glucose levels). Wearables, including smartwatches and fitness trackers, are increasing in popularity due to their ability to provide individuals with health information directly, without health providers as intermediaries. Cost and maintenance are unique barriers to widespread adoption of wearables, especially as concerns over obsolescence (i.e. the market-driven, artificially limited use of products) grow among consumers.<sup>108</sup>

### Using mobile phone-based SMS to support pre-exposure prophylaxis adherence in Thailand

From July 2015 to June 2020, the Thailand Ministry of Public Health and the Center for Disease Control (MoPH – CDC) partnered with Mahidol University, Johns Hopkins University and other organizations to track the uptake of pre-exposure prophylaxis (PrEP) with mobile phone-based SMS adherence support. The study focused on HIV-negative young men (aged 18–26 years) who have sex with men. Study participants were sent tailored SMS messages to encourage adherence to the PrEP regime, disseminate information on HIV testing and prevention, as well as provide feedback to researchers. The research aims to analyse medical and cost-effectiveness of encouraging PrEP uptake in key populations with mobile phone adherence support.

### Using social media to support HIV prevention for key populations

In Panama, UNDP and the Global Fund are working with partners to provide services to key populations, including Asociación de Hombre y Mujeres Nuevos de Panamá (AHMNP), Asociación Panameña de Persona Trans (APPT) and Asociación Viviendo Positivamente (AVP). Partners are utilizing digital communication platforms to minimize the impact of COVID-19 on HIV prevention services for key populations through their work with homosexual men and other men who have sex with men, transgender people and sex workers. Using social media platforms, including Instagram, Facebook, Twitter and WhatsApp, and various dating apps, partners are delivering preventive health messages. In addition, health promoters are establishing online conversations with those at risk and offering follow-up services in the form of local meetings where condom distributions and HIV testing can take place.

*Sources:* Adapted from “COPE4YMSM: Effectiveness and Cost-Effectiveness of a Combination HIV Preventive Intervention With and Without Daily Oral Truvada® PrEP among Young Men who have Sex with Men (YMSM) and Transgender Women (TGW) in Bangkok and Pattaya, Thailand”, Johns Hopkins University. Available from: [www.jhsph.edu/research/centers-and-institutes/center-for-public-health-and-human-rights/research/key-populations-program/current-projects/cope4ymsm-thai-ymsm-prevention-effectiveness-evaluation.html](http://www.jhsph.edu/research/centers-and-institutes/center-for-public-health-and-human-rights/research/key-populations-program/current-projects/cope4ymsm-thai-ymsm-prevention-effectiveness-evaluation.html). See also “Combating HIV Spread in Thailand One Text at a Time”. FrontlineSMS. Available from [www.frontlinesms.com/blog/2020/5/14/combating-hiv-spread-in-thailand-one-text-at-a-time](http://www.frontlinesms.com/blog/2020/5/14/combating-hiv-spread-in-thailand-one-text-at-a-time).

## 1.3 Point-of-care diagnostics

Point-of-care (PoC) diagnostics involve the use of technology to conduct biological tests for any disease or condition at the time and place of patient care instead of in a medical laboratory.<sup>109</sup> PoC diagnostics for HIV-related programmes is most notably applied in HIV rapid testing, which has the potential to address many barriers to accessing testing if scaled up and implemented systematically.<sup>110</sup> Another area where PoC diagnostics hold promise is for tuberculosis (TB) rapid testing and increasing access to treatment.<sup>111</sup>

The benefits of PoC diagnostics include: increased access to testing; improved diagnostic capabilities (both in accuracy and ability to detect diseases at earlier stages); faster decision-making (through the ability to diagnose on the spot); and improved health outcomes through the earlier start of treatment. PoC diagnostics can also be used directly by individuals (e.g. home-based testing), which can make this technology more easily accessible than having to go to a health facility or clinic.

### Innovation expands HIV testing for key populations

In the Western Pacific, people are scattered across a multitude of remote and small islands, many of which have scant clinical health services. It is harder still for key populations affected by HIV because they face stigma and discrimination. Now, however, with support from UNDP and the Global Fund, a new diagnostic test for HIV and syphilis can be performed in remote settings without sophisticated equipment—just a simple finger-prick. Testing among key populations has increased 10 times since the roll-out began.

*Source:* Adapted from UNDP Pacific Office in Fiji brief: Pacific-wide rollout of rapid HIV and syphilis test to improve sexual and reproductive health services for the most vulnerable (23 October 2018). Available from [www.pacific.undp.org/content/pacific/en/home/presscenter/articles/2018/pacific-wide-rollout-of-rapid-hiv-and-syphilis-test.html](http://www.pacific.undp.org/content/pacific/en/home/presscenter/articles/2018/pacific-wide-rollout-of-rapid-hiv-and-syphilis-test.html)

## 2 Health-care providers

Digital health innovations are facilitating more effective and efficient, and higher quality health-care service provision. This section looks at the following interventions: electronic medical records (EMRs), health informatics and telemedicine.

### 2.1 Electronic medical records

EMRs use “digitized record[s] to capture and store health information on clients in order to follow-up on their health status and services received”.<sup>112</sup> EMR implementation aims to support providers by integrating decision-making tools (e.g. checklists prompting for clinical protocols, scheduling of timely follow-up visits) to guide providers while delivering care to patients. Within the context of HIV, EMRs have the potential to improve HIV service delivery and care; for instance, electronically shared medical records have been shown to support adherence to antiretroviral treatment.<sup>113</sup> The benefits of widespread EMR use include the minimization of common human errors, improved accuracy of patient care records, and enhancement of the health system’s abilities to plan for the care of populations.<sup>114</sup> EMRs also allow for the creation and use of digital portals where patients can independently and directly access their medical information. Protecting personal health information and data is a fundamental requirement of transitioning to, and maintaining, EMRs.



### Ensuring that pregnant women receive timely care

In India, UNDP is working with the Ministry of Health and Family Welfare in the State of Maharashtra to pilot an innovative digital solution to address critical service delivery gaps in maternal health care. The Antenatal, Neonatal, Child Health Systems and Logistics Tracking Tool (ANCHAL) initiative aims to support pregnant women through a smartphone app to reduce maternal morbidity. Frontline health workers, health facilities and government ambulance services are linked through a digital platform that can track women during their pregnancy, and ensure that they deliver at the most appropriately equipped facility, at the right time. The app is currently being tested in Pune District, among 3 800 frontline health workers.

## 2.2 Health informatics

Health informatics uses computer-based information systems in health care for five primary functions: (i) management of day-to-day needs of a health-care institution or system, such as planning and budgeting; (ii) clinical support, such as diagnosis and treatment; (iii) surveillance and epidemiological information on the patterns and trends of health conditions and programmes; (iv) the preparation of formal publications and other documentation; and (v) additional technical information for a technical task not directly related to clinical support, such as conducting laboratory tests.<sup>115</sup>

Health informatics are applied to support HIV-related programmes in several ways, including analysis of health system EMRs to identify opportunities to scale up HIV treatment, creation of health information exchanges (patient information sharing across different providers or systems), and evaluation of public health programmes to improve treatment adherence.<sup>116</sup> Benefits of health informatics approaches include the improved ability of health systems to track and manage patient care more efficiently and increased efficiency in data analysis and reporting.

### Digitalization of Zimbabwe's national health management information system

The United Nations Development Programme (UNDP), with the support of the Global Fund, the US Government and other partners, has been working with Zimbabwe's Ministry of Health and Child Care to digitize its national health management information systems (HMIS). This process has required laying the groundwork for a unified central digital management system across four systems: the electronic Patient Management Information System (ePMS); the Macro Database for site-level ePMS data; the District Health Information System 2 (DHIS-2), a national system that collects aggregate data; and the weekly Disease Surveillance System.

*continued...*

...continued

Some of the key aspects of the project to date have been ensuring interoperability between systems, supporting enabling policy frameworks (including an information and communication technology [ICT] policy and an e-Health policy), facilitating strengthening of ICT infrastructure, and training of health-care professionals, data managers and policymakers in the HMIS systems. While the project is still ongoing, the work has already yielded positive results. For instance, improved interoperability between the ePMS and DHIS-2 has improved data accuracy and has enhanced the use and analysis of evidence at all levels of the health system. It has also improved coordination between various stakeholders who use the health data.

Source: Adapted from UNDP, *Zimbabwe Brief: UNDP and Global Fund support to strengthen the national health management information system* (7 July 2020). Available from [www.zw.undp.org/content/zimbabwe/en/home/library/hiv\\_aids/undp-and-global-fund-support-to-strengthen-the-national-health-m.html](http://www.zw.undp.org/content/zimbabwe/en/home/library/hiv_aids/undp-and-global-fund-support-to-strengthen-the-national-health-m.html)

### 2.3 Telemedicine

Telemedicine is broadly defined as:

“the delivery of health-care services, where distance is a critical factor, by all health-care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health-care providers, all in the interests of advancing the health of individuals and their communities”.<sup>117</sup>

Telemedicine can be and has been used in HIV-related programmes to support health-care workers in low-resource settings globally, consult on difficult HIV cases and deliver HIV case management remotely.<sup>118</sup> While the main benefit of telemedicine is overcoming geographical barriers to access, there are additional potential benefits for low-resource settings, such as connecting rural and remote sites to reverse the effects of ‘brain drain’ and the flight of human capital from these settings.

Restriction on movement during the COVID-19 pandemic resulted in an increased use of telemedicine in many countries, restricting in-person clinic appointments to medically necessary ones, and transitioning other appointments to newly scaled-up telemedicine services.<sup>119</sup> Telemedicine models were adopted for prescription re-fills;<sup>120</sup> and to access essential reproductive health-care services.<sup>121</sup> Some countries have also increased their administrative and/or financial support for telemedicine, for example: the Australian Government increased subsidies for telemedicine use; the Indonesian Government published a list of telemedicine providers on its COVID-19 website; and the Philippines announced a new national framework for telemedicine.<sup>122</sup>

### Telemedicine providing accessible health care in Libya

UNDP, in partnership with the Ministry of Health, the Government of Japan and a private sector start-up company, Speetar, launched the first telemedicine initiative in Libya. It addresses the shortage of doctors by connecting Libyans with physicians in diaspora communities who speak their language and understand the local context. It also reduces the burden of travel and mobility for people suffering from chronic diseases who require constant monitoring. This Telemedicine Initiative will engage with around 6,000 patients and 1,000 specialists, and will process 10,000 virtual consultations and E-prescriptions. The Libyan National Centre for Diseases Control also used the app to provide information and consultation on the COVID-19 pandemic.

*Sources: Adapted from UNDP (2020), UNDP, Japan, the startup Speetar, and the Ministry of Health launch the first telemedicine initiative in Libya (18 December 2020). Available from [www.ly.undp.org/content/libya/en/home/presscenter/pressreleases/UNDP-Japan-the-startup-Speetar-and-the-Ministry-of-Health-launch-the-first-Telemedicine-initiative-in-Libya.html](http://www.ly.undp.org/content/libya/en/home/presscenter/pressreleases/UNDP-Japan-the-startup-Speetar-and-the-Ministry-of-Health-launch-the-first-Telemedicine-initiative-in-Libya.html)*

## 3 Health systems management

Digital technologies have evolved to support improvements in various points in health systems management. Two examples highlighted in this section are digital identifications (IDs) and supply chain innovations.

### 3.1 Digital identifications

Digital IDs are electronic equivalents used to represent and prove a person's identity. Theoretically, digital IDs can improve access to high-quality health care and are used in numerous ways within the health sector, such as facilitating an individual's enrolment in insurance or social service programmes, and improving the ability to track health records across different providers.<sup>123</sup> A subset of digital IDs, biometrics, are biological markers of identity (e.g. from a blood sample, iris scan or fingerprint scan turned into a digital ID such as a number sequence). The benefits of biometric applications to HIV-related programmes include the reduction of patient misidentification inaccuracies and linking of biometrics to electronic health records to not only improve the quality of care delivered, but also to expand and improve the HIV surveillance capabilities of the system.<sup>124</sup> The use of biometrics, however, can pose significant rights-related risks, since it facilitates the identification of individuals, potentially exposing them to rights violations, especially when individuals belong to stigmatized, marginalized or criminalized groups.<sup>125</sup> Digital ID systems can also be built on analogue systems that are problematic in terms of access for specific communities, such as migrant or minority communities that already have difficulty accessing paperwork, among other shortcomings. Like other forms of digital technologies, the adoption of digital ID systems must be carefully considered to protect rights, as well as ensure equity in access and quality of care. To ensure this, risk assessments should be carried out at each stage of the planning and implementation of a digital ID system.

### 3.2 Supply chain innovations

Digital technologies can be used to support supply chain innovations in health systems; for example, effective digital interventions can improve the availability of critical health commodities such as medicines and vaccines. Innovations range from basic eHealth applications, such as the use of SMS and data dashboards in order to manage and report on supply levels, to the development of international surveillance tools in order to track entire supply chains and financing gaps of countries. WHO recommends the use of digital interventions to support supply chain innovations, noting that these technologies can improve allocation of health-care commodities and reduce wasted resources.<sup>126</sup> In turn, this leads to higher quality care and increased efficiency of service delivery.

#### Improving the immunization supply chain in India – the electronic Vaccine Intelligence Network

In India, UNDP, in partnership with the Ministry of Health and Family Welfare and GAVI, has supported the design and implementation of the electronic Vaccine Intelligence Network (eVIN) aiming to ensure equity in availability of immunizations. eVIN streamlines the vaccine flow network by relying on data-driven management of the immunization supply chain. The system digitalizes vaccine stocks at all 27,000 vaccine storage centres across all districts of 29 States and seven union territories of India, facilitating real-time monitoring of storage temperatures, building capacity of nearly 37,000 government personnel for vaccine and cold chain logistic management, and deploying vaccine and cold chain managers in every district for constant supportive supervision. Since its implementation, eVIN has reduced by over 80 percent the number of vaccine stock-outs and ensured improved availability of immunizations to its main beneficiaries: children and pregnant women. The eVIN system empowers its national and district-level managers as well as healthcare staff who can easily monitor and access the needed vaccines. Indonesia has also adopted the eVIN system, with strong results.

Sources: Ong, L. and Wee, M., *The Use of Digital Technology to Improve Vaccine Delivery in India and Indonesia*, Medium. (13 September 2020). Available from <https://medium.com/undp-in-asia-and-the-pacific/the-use-of-digital-technology-to-improve-vaccine-delivery-in-india-and-indonesia-cf024880fa0c>; UNDP, *Improving the efficiency of vaccinations systems in multiple States*. Available from [www.in.undp.org/content/india/en/home/projects/gavi1.html](http://www.in.undp.org/content/india/en/home/projects/gavi1.html)

## 4 Cross-cutting digital health technologies

‘Cross-cutting digital health technologies’ is a broad category that captures various forms of digital innovations that support research or technical building-blocks of digital interventions for individuals, healthcare providers and health systems. Specific examples highlighted in this section include genomics and molecular surveillance; big data and algorithms; and artificial intelligence and machine learning.

#### 4.1 Genomics and molecular surveillance

Genomics is the study of genes and their interrelations to identify their combined influence on human development.<sup>127</sup> Genome-editing technologies that can recognize specific DNA sequences hold much promise for curing HIV through the ability to systematically search the human genome (i.e. all the genetic information in a person) for common genetic variants that influence the human response to HIV acquisition. Identification of these variants can inform targets for intervention, whether through a preventative vaccine or antiretroviral treatment.<sup>128</sup> Benefits of these technologies include specificity to individuals, ease of use, and ability to be custom-designed for treating individuals.

Molecular surveillance is the aggregate use of an individual's HIV treatment resistance data to identify and respond to HIV transmission clusters, or a group of persons with diagnosed HIV infection who have genetically similar HIV strains.<sup>129</sup> Clusters are difficult to identify with epidemiological methods – molecular data are needed to identify areas of higher transmission. The aim of molecular surveillance is to track trends in HIV epidemiology by identifying social networks at high risk of HIV transmission in order to better target preventative interventions. This manner of tracking HIV cases and trends is controversial among communities of people living with HIV and other civil society groups, with particular concern over the use of phylogenetics and criminalization of HIV non-disclosure, exposure and transmission.<sup>130</sup>

#### 4.2 Big data and algorithms

'Big data' refers to the collection of a significantly large amount of data, often growing in three dimensions – volume, velocity and variety – that cannot be handled by traditional methods or data processing software packages.<sup>131</sup> Digital technologies collect and process massive amounts of data, potentially from various sources (e.g. government administrative data, social media, Internet searches) as well as metadata (e.g. data that describes other data). A related but distinct concept connected to big data is algorithms, which are a set of programmed rules or processes applied to analyse data for a specific purpose or output.<sup>132</sup>

Scientists posit that big data and algorithms have significant utility for addressing HIV among key populations due to the increased availability of an unprecedented amount of data including from individuals' mobile technologies.<sup>133</sup> There are numerous applications of big data and algorithms for HIV-related programmes. Examples include systems integration of different sectors to track HIV in the mining industry<sup>134</sup> and using web search engine data to predict new HIV cases.<sup>135</sup> Benefits of using big data and algorithms include: increased capacity to collect vital information to inform programme development to improve health outcomes, and promotion of cross-sectoral data sharing to increase provider coordination and collaboration.

#### 4.3 Artificial intelligence and machine learning

Artificial intelligence (AI) is "the development of computer systems to perform tasks that usually require human intelligence, such as visual perception, speech recognition, and decision-making".<sup>136</sup> AI, which also encompasses the subfields of machine learning, natural

language processing and robotics, has countless applications to public health sciences and the delivery of HIV-related programmes. For example, researchers have developed a machine learning model to identify patients at risk of dropping out in order to improve retention in HIV treatment and care.<sup>137</sup> This field also includes conversational AI, which can increase accessibility of services to people with lower literacy and physical disabilities. Benefits of AI use include: improved quality of care by supporting providers to more accurately diagnose patients and choose corresponding treatment plans, and enhanced ability to slow the spread of disease through modelling and predictive epidemiological efforts.<sup>138</sup> AI application provides the opportunity to significantly improve the efficiency of healthcare delivery and quality of patient care.

### Using artificial intelligence to provide health information to deaf and hearing-impaired persons

UNDP, Egypt's Ministry of Communication and Information Technology and Avaya developed an automated testing service which uses accessible chatbots and artificial intelligence technology in sign language to enable access to information for hearing impaired. The chatbot asks users several questions using sign language to determine whether they are experiencing COVID-19 symptoms and refers them to the responsible government agency to appropriate care.

Source: Adapted from UNDP Egypt brief: *Artificial intelligence is leaving no one behind: Accessible chatbot for deaf and hearing-impaired persons* (2 June 2020). Available from [www.eg.undp.org/content/egypt/en/home/stories/2020/artificial-intelligence-is-leaving-no-one-behind--accessible-cha.html](http://www.eg.undp.org/content/egypt/en/home/stories/2020/artificial-intelligence-is-leaving-no-one-behind--accessible-cha.html)

## 5 Digital health technologies to advance drug research and development

Technological applications in drug research and development are wide-ranging and include AI and machine learning, among other digital approaches. Benefits of digital technology-enabled drug product research and development include greater efficiency in screening drug candidates among existing drugs, and using machine learning approaches for the identification of prognostic biomarkers to determine the likelihood of disease occurrence for an individual.<sup>139</sup> AI and machine learning can also be used to rapidly analyse digital pathology data in clinical trials. Drug research and development also draws on genomic sequencing and developing nanotechnology for enhanced treatment.<sup>140</sup>

## 6 Use of digital technologies during the COVID-19 pandemic

The COVID-19 pandemic accelerated the use of digital health technologies. Since conventional public health methods are slow and subject to human error, many countries are turning to them to support their COVID-19 responses. Basic eHealth approaches, including online COVID-19 data dashboards and mobile phone apps for contact tracing and case management, have complemented new digital technologies such as infrared thermal screening cameras and wearables (e.g. smartwatches) that monitor temperature, pulse and sleep pattern data to screen for the disease.<sup>141</sup>

### Georgia's e-Learning Platform to enhance infection prevention and control

In the wake of the first wave of COVID-19, UNDP with the support of Sweden worked with the National Center for Disease Control (NCDC) in Georgia to build an e-learning platform that provides medical professionals and administrative staff with opportunities to receive training, communicate, exchange experiences, and receive practical advice from NCDC experts. The platform is available to 37 medical institutions and the NCDC's 60 regional centres across the country. 3,000 medical workers from the clinics designated for COVID-19 treatment and 1,000 medical staff from regular health-care institutions have been trained in health emergency response. Also, this training was also provided to operators of a specialized hotline for medical professionals who will be trained in infection prevention and control. The e-learning platform operates through desktop and mobile applications, with a built-in chatbot and search engine, allowing for real-time consultations and exchange.

Source: Adapted from UNDP (2020) "Boosting Georgia's public health care with digital solutions". New York. Available from [www.ge.undp.org/content/georgia/en/home/presscenter/pressreleases/2020/covid-health-care-elearning.html](http://www.ge.undp.org/content/georgia/en/home/presscenter/pressreleases/2020/covid-health-care-elearning.html).

New algorithms and AI, which includes analyses of big data collected in relation to COVID-19, have made it possible to develop digital health interventions for COVID-19. Digital technologies are playing an important part in vaccine rollouts, and harnessing the power of AI and data analytics will be crucial for increasing equitable access to COVID-19 vaccines.

### Indonesia's innovative technology supporting COVID-19 vaccination rollout

UNDP's Sistem Monitoring Imunisasi Logistik Secara Elektronik (SMILE), an innovative technological solution that aims to strengthen the immunization supply chain system in Indonesia, will be engaged to ensure the delivery of vaccines across the archipelago. Developed in 2018, SMILE aims to strengthen the health supply chain for Indonesia's immunization programme by managing vaccine stocks and quality. This has helped improve efficiency, especially in terms of reporting and monitoring real-time data of vaccine stocks. The SMILE app will be used to track delivery to COVID-19 health facilities.

Source: Adapted from UNDP (2020) "COVID-19 Immunization Drive provides opportunity for Indonesia to adopt UNDP's Digital Tracking System. New York. Available from [www.id.undp.org/content/indonesia/en/home/presscenter/articles/2020/Smile-Vaccine.html](http://www.id.undp.org/content/indonesia/en/home/presscenter/articles/2020/Smile-Vaccine.html).

While digital technologies may hold promise to support more effective public health responses, it is imperative to flag that such interventions may also be prone to error, perpetuate entrenched biases as well as present privacy and confidentiality risks, particularly where mass surveillance is involved. Thus, ensuring safeguards to protect individual rights, including through regulatory frameworks, is paramount when considering the adoption of digital health technologies.



## Endnotes

- 1 United Nations, *Secretary-General's Strategy on New Technologies* (2018). Available from [www.un.org/en/newtechnologies](http://www.un.org/en/newtechnologies); United Nations, High-Level Panel on Digital Cooperation, *The Age of Interdependence* (2019). Available from [www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf](http://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf); United Nations, *Secretary-General's Roadmap for Digital Cooperation* (2020). Available from [www.un.org/en/content/digital-cooperation-roadmap](http://www.un.org/en/content/digital-cooperation-roadmap)
- 2 UNDP, *Strategic Plan 2018–2021*. Available from <https://strategicplan.undp.org>; UNDP, *Digital Strategy 2019*. Available from <https://digitalstrategy.undp.org>
- 3 UNDP, *Connecting the Dot: HIV Health and Development 2016–2021*. Available from [www.undp.org/content/undp/en/home/librarypage/hiv-aids/hiv--health-and-development-strategy-2016-2021.html](http://www.undp.org/content/undp/en/home/librarypage/hiv-aids/hiv--health-and-development-strategy-2016-2021.html)
- 4 Deloitte Insights, *The essence of resilient leadership: Business recovery after COVID-19* (2020). Available from <https://documents.deloitte.com/insights/DeloitteReview27>
- 5 Budd, J, et al., Digital technologies in the public-health response to COVID-19. *Nat Med.* 26(8) (Aug. 2020). 1183–1192.
- 6 Whitelaw, S., Manas, M., Topol, E., Val Spall, H., *Lancet Digital Health*, Vol. 2, Issue 8, E435 – E.440 (Aug. 2020).
- 7 “Digital health” is a broad term encompassing diverse digital technologies, including ‘big data’, genomics and artificial intelligence (AI), applied to both clinical medicine and public health. World Health Organization resolution, *Digital health resolution – A71/VR/7*, (21 May 2018). Available from [http://apps.who.int/gb/ebwha/pdf\\_files/WHA71/A71\\_ACONF1-en.pdf](http://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_ACONF1-en.pdf). See also World Health Organization (WHO). Draft global digital health strategy, 2020–2024, (26 March 2019). Available from <https://extranet.who.int/dataform/upload/surveys/183439/files/Draft%20Global%20Strategy%20on%20Digital%20Health.pdf>
- 8 World Health Organization, *Global strategy on digital health, 2020–2025* (2019). Available from [www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5\\_58](http://www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_58)
- 9 Ibid.
- 10 Imison, C., Castle-Clarek, S., Watson, R., Edwards, N., *Delivering the Benefits of Digital Health Care*, Nuffield Trust (February 2016).
- 11 Global Commission on HIV and the Law, *Risks, rights and health – Supplement* (2018). Available from [www.hivlawcommission.org/supplement](http://www.hivlawcommission.org/supplement)
- 12 Ibid.
- 13 UNAIDS, *End Inequalities, End AIDS: Global AIDS Strategy 2021–2026*. Available from [www.unaids.org/en/Global-AIDS-Strategy-2021-2026](http://www.unaids.org/en/Global-AIDS-Strategy-2021-2026). The Strategy recognizes the potential of digital technologies to address structural and age-related barriers faced by adolescent and young key populations, and to advance the right to health and secure access to services without violating or undermining human rights.
- 14 See, IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition*. IEEE (2019). Available from <https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html>; Philbeck, T., Davis, N., Engtoft Larsen, A., Values, Ethics and Innovation Rethinking Technological Development in the Fourth Industrial Revolution, World Economic Forum White Paper (August 2018). Available from [www3.weforum.org/docs/WEF\\_WP\\_Values\\_Ethics\\_Innovation\\_2018.pdf](http://www3.weforum.org/docs/WEF_WP_Values_Ethics_Innovation_2018.pdf); European Commission, High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy Artificial Intelligence* (2019). Available from <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>; See also Principles for Digital Development. Available from <https://digitalprinciples.org/principles/>
- 15 See National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, U.S. Department of Health, Education and Welfare, *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research* (1979). Available from [www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html#xbenefit](http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html#xbenefit)
- 16 “About HTAI. Available from <https://htai.org/about-htai>. Accessed 3 September 2020; see also “Health Technology Assessment”, World Health Organization. Available from [www.who.int/medical\\_devices/assessment/en](http://www.who.int/medical_devices/assessment/en). Accessed 3 September 2020.
- 17 Mathews, S.C., McShea, M.J., Hanley, C.L. et al., Digital health: A path to validation. *npj Digit. Med.* 2, 38 (2019). Available from <https://doi.org/10.1038/s41746-019-0111-3>
- 18 Ibid.
- 19 “Interoperability”, Global Digital Health Partnership. Available from [www.gdhp.org/interoperability](http://www.gdhp.org/interoperability). Accessed 3 September 2020.
- 20 Powell, K., Alexander, G., *Mitigating Barriers to Interoperability in Health Care*. *Online Journal of Nursing Informatics (OJNI)*. 23(2) (Summer, 2019). Available from [www.himss.org/resources/mitigating-barriers-interoperability-health-care](http://www.himss.org/resources/mitigating-barriers-interoperability-health-care)
- 21 See also, United Nations, High-Level Panel on Digital Cooperation, *The Age of Interdependence* (2019). Available from [www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf](http://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf)

- 22 "Digital Health Strategies", Inter-Telecommunications Union. Available from [www.itu.int/en/ITU-D/ICT-Applications/Pages/e-health-strategies.aspx](http://www.itu.int/en/ITU-D/ICT-Applications/Pages/e-health-strategies.aspx). Accessed 03 September 2020.
- 23 Mechael, P., and Edelman, J.K., *The State of Digital Health: 2019*, Global Digital Health Index. (2019). Available from <https://static1.squarespace.com/static/5ace2d0c5cfd792078a05e5f/t/5d4dcb80a9b364000183a34/1565379490219/State+of+Digital+Health+2019.pdf>
- 24 World Health Organization, *Global strategy on digital health, 2020–2025* (2019). Available from [www.who.int/docs/default-source/documents/g54dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5\\_58](http://www.who.int/docs/default-source/documents/g54dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_58)
- 25 For guidance on developing a national strategy, including the importance of consultations, see WHO and ITU, *National eHealth Strategy Toolkit* (2012). Available from [www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-E\\_HEALTH.05-2012-PDF-E.pdf](http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-E.pdf). For concrete examples, see Australian Government, *Australian Digital Health Strategy*, p 16-18; *New Zealand Health Strategy: Future direction* (April 2016).
- 26 UNESCO is coordinating the Digital Literacy Global Framework (DLGF) project with the objective of developing a methodology that can serve as the foundation for Sustainable Development Goal (SDG) thematic Indicator 4.4.2: "Percentage of youth/adults who have achieved at least a minimum level of proficiency in digital literacy skills". Available from [www.uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf](http://www.uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf).
- 27 World Health Organization, *Global strategy on digital health, 2020–2025* (2019). Available from [www.who.int/docs/default-source/documents/g54dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5\\_58](http://www.who.int/docs/default-source/documents/g54dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_58)
- 28 West, D., *Digital divide: Improving Internet access in the developing world through affordable services and diverse content* (2015). Available from [www.brookings.edu/wp-content/uploads/2016/06/West\\_Internet-Access.pdf](http://www.brookings.edu/wp-content/uploads/2016/06/West_Internet-Access.pdf)
- 29 Participating States are: Benin, Ethiopia, Mali, Nigeria, Sierra Leone, Uganda, Afghanistan, Jordan, Kuwait, Pakistan, Portugal, Chile, Peru, Bangladesh, Indonesia, Sri Lanka, Thailand, Lao People's Democratic Republic, Malaysia, Mongolia, New Zealand, Philippines. Mechael, P., and Edelman, J.K., *The State of Digital Health: 2019*, Global Digital Health Index. (2019). Available from <https://static1.squarespace.com/static/5ace2d0c5cfd792078a05e5f/t/5d4dcb80a9b364000183a34/1565379490219/State+of+Digital+Health+2019.pdf>
- 30 Amon JJ., *Ending discrimination in health care*. *J Int AIDS Soc.* 23(2):e25471. doi:10.1002/jia2.25471 (2020).
- 31 A. Gleb, Clark, J., *Identification for development: The biometrics revolution* (2013). CGD Working Paper 315. Washington, DC: Center for Global Development. Available from [www.cgdev.org/content/publications/detail/1426862](http://www.cgdev.org/content/publications/detail/1426862).
- 32 Sullivan, C., *Digital Identity: An emergent legal concept: the role and legal nature of digital identity in commercial transactions* (2011). Adelaide: University of Adelaide. Available from [www.library.open.org/bitstream/handle/20.500.12657/33171/560114.pdf](http://www.library.open.org/bitstream/handle/20.500.12657/33171/560114.pdf)
- 33 Kavanagh, M., et al., *Biometrics and public health surveillance in criminalised and key populations: policy, ethics and human rights considerations* (2019). *Lancet HIV* 2019; 6: e51-59. Available from [www.thelancet.com/action/showPdf?pii=S2352-3018%2818%2930243-1](http://www.thelancet.com/action/showPdf?pii=S2352-3018%2818%2930243-1). Davis, S., Maleche, A., *Everyone said no: key populations and biometrics in Kenya*. July 4, 2018. *Health and Human Rights Journal*. Available from [www.hhrjournal.org/2018/07/everyone-said-no-key-populations-and-biometrics-in-kenya/](http://www.hhrjournal.org/2018/07/everyone-said-no-key-populations-and-biometrics-in-kenya/)
- 34 "Stop Stockouts", Stop Stockouts Project. Available from <https://stockouts.org>. Accessed 3 September 2020.
- 35 For an example of an access to justice reporting system in the HIV response, see Williamson, R.T., Wondergem, P., Amenyah, R., *Using a Reporting System to Protect the Human Rights of People living with HIV and Key Populations: A Conceptual Framework*, *Health and Human Rights Journal* 2014, 16. Available from [www.hhrjournal.org/2014/07/using-a-reporting-system-to-protect-the-human-rights-of-people-living-with-hiv-and-key-populations-a-conceptual-framework](http://www.hhrjournal.org/2014/07/using-a-reporting-system-to-protect-the-human-rights-of-people-living-with-hiv-and-key-populations-a-conceptual-framework)
- 36 Transparency International, *The ignored pandemic* (2019). Available from [www.ti-health.org/wp-content/uploads/2019/03/Ignored-Pandemic-WEB-v3.pdf](http://www.ti-health.org/wp-content/uploads/2019/03/Ignored-Pandemic-WEB-v3.pdf)
- 37 Open Contracting Partnership. Available from [www.open-contracting.org/impact-stories](http://www.open-contracting.org/impact-stories)
- 38 For more on eVIN in India. Available from [www.in.undp.org/content/india/en/home/projects/gavi1.html](http://www.in.undp.org/content/india/en/home/projects/gavi1.html)
- 39 Wald, T., *Governments can fight corruption by joining the digital payment revolution* (2018). Available from [www.weforum.org/agenda/2018/04/governments-join-digital-payment-revolution-fight-corruption](http://www.weforum.org/agenda/2018/04/governments-join-digital-payment-revolution-fight-corruption)
- 40 75 countries criminalize HIV non-disclosure, exposure and transmission ([www.hivjustice.net/wp-content/uploads/2019/05/AHJ3-Executive-Summary-EN.pdf](http://www.hivjustice.net/wp-content/uploads/2019/05/AHJ3-Executive-Summary-EN.pdf)); 36 countries criminalize selling sexual services, while 47 others criminalize some aspect of sex work (<http://lawsandpolicies.unaids.org/topicresult?i=212>). Seventy countries criminalize consensual same-sex conduct ([https://ilga.org/downloads/ILGA\\_State\\_Sponsored\\_Homophobia\\_2019.pdf](https://ilga.org/downloads/ILGA_State_Sponsored_Homophobia_2019.pdf)).

- Moreover, most countries criminalize some aspect of drug use or possession and at least 16 maintain the death penalty for drug-related crimes (<http://lawsandpolicies.unaids.org/topicresult?i=214>). In countries that criminalize adolescents through age of consent and service restriction laws, unauthorized access to, or disclosure of, adolescents' information related to access to HIV and other sexual and reproductive health services jeopardize their safety and autonomy.
- 41 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Article 4(12). Available from <http://data.europa.eu/eli/reg/2016/679/2016-05-04>
- 42 "Data Breaches: In the Healthcare Sector," Center for Internet Security. Available from [www.cisecurity.org/blog/data-breaches-in-the-health-care-sector](http://www.cisecurity.org/blog/data-breaches-in-the-health-care-sector). Accessed 3 September 2020.
- 43 Verizon, *Protected Health Information Data Breach Report: White Paper* (2018). Available from [https://enterprise.verizon.com/resources/reports/2018/protected\\_health\\_information\\_data\\_breach\\_report.pdf](https://enterprise.verizon.com/resources/reports/2018/protected_health_information_data_breach_report.pdf). Sharanjit Leyl, "Singapore HIV data leak shakes a vulnerable community". (22 February 2019), BBC News. [www.bbc.com/news/world-asia-47288219](http://www.bbc.com/news/world-asia-47288219)
- 44 Frederik J. Zuiderveen Borgesius, *Strengthening legal protection against discrimination by algorithms and artificial intelligence*. The International Journal of Human Rights. DOI: 10.1080/13642987.2020.1743976. For more information on AI biases and human rights (2020): see Latonero, M., *Governing Artificial Intelligence: Upholding Human Rights and Dignity* (2018). Available from [https://datasociety.net/wp-content/uploads/2018/10/DataSociety\\_Governing\\_Artificial\\_Intelligence\\_Upholding\\_Human\\_Rights.pdf](https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf)
- 45 Chen, I., Szolovits, P., Ghassemi, M., *Can AI Help Reduce Disparities in General Medical and Mental Health Care?* AMA J Ethics. 2019; 21(2):E167-179. doi: 10.1001/amajethics.2019.167.
- 46 Frederik J. Zuiderveen Borgesius, *Strengthening legal protection against discrimination by algorithms and artificial intelligence*. The International Journal of Human Rights. DOI: 10.1080/13642987.2020.1743976 (2020).
- 47 "Function Creep", Collins Dictionary. Available from [www.collinsdictionary.com/dictionary/english/function-creep](http://www.collinsdictionary.com/dictionary/english/function-creep). Accessed 3 September 2020.
- 48 Kavanagh, et al, *Biometrics and public health surveillance in criminalized and key populations: policy, ethics and human rights considerations*, Lancet HIV (7 Oct. 2018). Available from [http://dx.doi.org/10.1016/S2352-3018\(18\)30243-1](http://dx.doi.org/10.1016/S2352-3018(18)30243-1)
- 49 See, for instance, Amazon: "Alexa, what is hidden behind your contract with the NHS?"; Privacy International, 06 December 2019. Available from <https://privacyinternational.org/node/3298>. Accessed 3 September 2020; Palantir: "(Sort of) Trust but Verify: Palantir Responds to Questions about its work with NHS", Privacy International (6 May 2020). Available from <https://privacyinternational.org/long-read/3751/sort-trust-verify-palantir-responds-questions-about-its-work-nhs>. Accessed 3 September 2020; Google: "Give Google an inch and they'll take a mile!" Privacy International (13 November 2019). Available from <https://privacyinternational.org/node/3280>. Accessed 3 September 2020.
- 50 Other mentions include: *Convention on the Elimination of all Forms of Discrimination against Women* (Articles 11.1 and 12); *Convention on the Rights of the Child* (Article 24); *Convention on the Elimination of Racial Discrimination* (Article 5); *Convention on Persons with Disabilities* (Article 25); as well as various regional instruments such as the African Charter on Human and People's Rights (Article 16) and the *Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights* (Article 10). *Convention on the Elimination of All Forms of Discrimination against Women*. New York, (18 December 1979). Available from [www.ohchr.org/EN/ProfessionalInterest/Pages/CEDAW.aspx](http://www.ohchr.org/EN/ProfessionalInterest/Pages/CEDAW.aspx); *Convention on the Rights of the Child* (20 November 1989). Available from [www.ohchr.org/en/professionalinterest/pages/crc.aspx](http://www.ohchr.org/en/professionalinterest/pages/crc.aspx); *International Convention on the Elimination of All Forms of Racial* (21 December 1965). Available from [www.ohchr.org/en/professionalinterest/pages/cerd.aspx](http://www.ohchr.org/en/professionalinterest/pages/cerd.aspx); *Convention on the Rights of Persons with Disabilities* (13 December 2006). Available from [www.ohchr.org/EN/HRBodies/CRPD/Pages/ConventionRightsPersonsWithDisabilities.aspx](http://www.ohchr.org/EN/HRBodies/CRPD/Pages/ConventionRightsPersonsWithDisabilities.aspx); *African Charter on Human and People's Rights* (27 June 1981). Available from [www.achpr.org/legalinstruments/detail?id=49](http://www.achpr.org/legalinstruments/detail?id=49); *Additional Protocol to the American Convention on Human Rights in the Area of Economic, Social and Cultural Rights*. Available from [www.oas.org/juridico/english/treaties/a-52.html](http://www.oas.org/juridico/english/treaties/a-52.html)
- 51 United Nations Committee on Economic, Social and Cultural Rights, CESCR General Comment No. 14: Right to the highest attainable standard of health (Art. 12) (11 August 2000). Available from [www.refworld.org/pdfid/4538838d0.pdf](http://www.refworld.org/pdfid/4538838d0.pdf)
- 52 *Ibid*, para. 12.
- 53 *Ibid*, para.43.
- 54 *ibid.*, paras. 30-31, 11 August 2000. Available from [www.refworld.org/pdfid/4538838d0.pdf](http://www.refworld.org/pdfid/4538838d0.pdf)
- 55 *Ibid*, CESCR General Comment No. 25 on Science and economic, social and cultural rights, para. 70. Available from [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=9&DocTypeID=11](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=9&DocTypeID=11)

- 56 United Nations, Secretary-General's Roadmap for Digital Cooperation (2020). Available from [www.un.org/en/content/digital-cooperation-roadmap](http://www.un.org/en/content/digital-cooperation-roadmap)
- 57 United Nations Committee on Economic, Social and Cultural Rights, CESCR General Comment No. 25 on Science and economic, social and cultural rights, para.70. Available from [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=9&DocTypeID=11](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=9&DocTypeID=11)
- 58 International Covenant on Civil and Political Rights, Article 2 on non-discrimination, see also related Article 26 on equality before the law – *International Covenant on Civil and Political Rights* (16 December 1966). Available from [www.ohchr.org/en/professionalinterest/pages/ccpr.aspx](http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx); see also International Covenant on Economic, Social and Cultural Rights, Article 2 – *International Covenant on Economic, Social and Cultural Rights* (16 December 1966). Available from [www.ohchr.org/en/professionalinterest/pages/cescr.aspx](http://www.ohchr.org/en/professionalinterest/pages/cescr.aspx)
- 59 United Nations Human Rights Committee, CCPR General Comment No. 18: Non-discrimination, para. 7 (10 November 1989). Available from [www.refworld.org/docid/453883fa8.html](http://www.refworld.org/docid/453883fa8.html)
- 60 For HIV and health status, see United Nations Committee on Economic, Social and Cultural Rights, CESCR General Comment No. 14: Right to the highest attainable standard of health (Art. 12) (11 August 2000), Available from [www.refworld.org/pdfid/4538838d0.pdf](http://www.refworld.org/pdfid/4538838d0.pdf). For sexual orientation and gender identity, see "Fact Sheet: International Human Rights Law and Sexual Orientation and Gender Identity", Office of the High Commissioner for Human Rights. Available from [www.ohchr.org/Documents/Issues/Discrimination/LGBT/FactSheets/unfe-11-UN\\_Fact\\_Sheets\\_GenderIdentity\\_English.pdf](http://www.ohchr.org/Documents/Issues/Discrimination/LGBT/FactSheets/unfe-11-UN_Fact_Sheets_GenderIdentity_English.pdf)
- 61 United Nations Human Rights Committee, CCPR General Comment No. 18: Non-discrimination, para. 8, 10, 13 (10 November 1989). Available from [www.refworld.org/docid/453883fa8.html](http://www.refworld.org/docid/453883fa8.html)
- 62 See, for example, discussions on equality and the digital welfare state from the Special Rapporteur on Extreme Poverty's report, Alston, Philip, *Digital technology, social protection and human rights*, A/74/493, paras 44–49 (2019).
- 63 See *Toronto Declaration on the protecting the right to equality and non-discrimination in machine learning systems* (16 May 2018). Available from [www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems](http://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems). See also Alston, Philip, *Digital technology, social protection and human rights*, A/74/493, paras 48–49 (2019).
- 64 *Toronto Declaration on the protecting the right to equality and non-discrimination in machine learning systems* (16 May 2018). Available from [www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems](http://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems)
- 65 Alston, Philip, *Digital technology, social protection and human rights*, A/74/493, para 49 (2019).
- 66 International Covenant on Economic, Social and Cultural Rights, Article 15(1)(b) – *International Covenant on Economic, Social and Cultural Rights* (16 December 1966). Available from [www.ohchr.org/en/professionalinterest/pages/cescr.aspx](http://www.ohchr.org/en/professionalinterest/pages/cescr.aspx)
- 67 United Nations Committee on Economic, Social and Cultural Rights, CESCR General Comment No. 25 on Science and economic, social and cultural rights, paras 23–25. Available from [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=9&DocTypeID=11](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=9&DocTypeID=11)
- 68 *Ibid.* para. 70.
- 69 *Ibid.*, paras 75–76. See also para. 19 on privacy, informed consent and confidentiality.
- 70 *International Covenant on Civil and Political Rights* (16 December 1966). Available from [www.ohchr.org/en/professionalinterest/pages/ccpr.aspx](http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx); see also *Convention on the Rights of the Child*, Article 16, *Convention on the Rights of the Child* (20 November 1989). Available from [www.ohchr.org/en/professionalinterest/pages/crc.aspx](http://www.ohchr.org/en/professionalinterest/pages/crc.aspx); *Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, Article 14, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families* (18 December 1990). Available from [www.ohchr.org/Documents/ProfessionalInterest/cmw.pdf](http://www.ohchr.org/Documents/ProfessionalInterest/cmw.pdf)
- 71 United Nations Human Rights Committee (HRC). CCPR General Comment No. 16: Article 17 (Right to Privacy). The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988). Available from [www.refworld.org/docid/453883f922.html](http://www.refworld.org/docid/453883f922.html)
- 72 United Nations Human Rights Committee (HRC). CCPR General Comment No. 16: Article 17 (Right to Privacy). The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, para. 10 (8 April 1988).
- 73 United Nations Human Rights Committee (HRC). CCPR General Comment No. 16: Article 17 (Right to Privacy). The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988).
- 74 See, for example, the South African Constitutional Court case of *Minister of Health v. Treatment Action Campaign (TAC)* (2002) 5 SA 721. Available from [www.escri-net.org/caselaw/2006/minister-health-v-treatment-action-campaign-tac-2002-5-sa-721-cc](http://www.escri-net.org/caselaw/2006/minister-health-v-treatment-action-campaign-tac-2002-5-sa-721-cc)

- 75 United Nations Human Rights Council resolution, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/38/L.10/Rev.1 (4 July 2018). Available from <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/203/73/PDF/G1820373.pdf?OpenElement>. United Nations General Assembly resolution, *Information and communications technologies for development*, A/RES/68/198 (15 January 2014). Available from [https://www.un.org/en/ga/search/view\\_doc.asp?symbol=A/RES/68/198](https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/198)
- 76 For example, see India: *K. S. Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012 (Sup. Ct. India 24 August 2017). Available from [https://main.sci.gov.in/supremecourt/2012/35071/35071\\_2012\\_Judgement\\_24-Aug-2017.pdf](https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf); see also Jamaica: *Robinson, J. v. the Attorney General of Jamaica*, [2019] JMFC Full 04. Available from <https://supremecourt.gov.jm/content/robinson-julian-v-attorney-general-jamaica>; and Mauritius: *Madhewoo M. v. the State of Mauritius* (2016 Privy Council Appeal). Available from [www.jcpc.uk/cases/docs/jcpc-2016-0006-judgment.pdf](http://www.jcpc.uk/cases/docs/jcpc-2016-0006-judgment.pdf)
- 77 *Nubian Rights Forum v. Attorney-General*, 2019 High Court of Kenya. Available from <http://kenyalaw.org/caselaw/cases/view/172447>
- 78 *Nederlands Juristen Comité voor de Mensenrechten tegen Staat der Nederlanden [Netherlands Jurists Committee of Human Rights v State of the Netherlands]*, Rechtbank Den Haag [Hague District Court], C/09/550982/HA ZA 18-388 (5 February 2020). Available from <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865>
- 79 Office of the High Commissioner for Human Rights, *United Nations Guiding Principles on Business and Human Rights* (2011). Available from [www.ohchr.org/documents/publications/guidingprinciplesbusinesshr\\_en.pdf](http://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf); See also European Commission, *ICT Sector Guide on Implementing the United Nations Guiding Principles on Business and Human Rights* (2014). Available from <https://op.europa.eu/en/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b> and United Nations Committee on Economic, Social and Cultural Rights, CESCR General Comment No. 25 on Science and economic, social and cultural rights, paras 75–76. Available from [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=9&DocTypeID=11;Toronto Declaration on the protecting the right to equality and non-discrimination in machine learning systems](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=9&DocTypeID=11;Toronto%20Declaration%20on%20the%20protecting%20the%20right%20to%20equality%20and%20non-discrimination%20in%20machine%20learning%20systems) (16 May 2018). Available from [www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems](http://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems); see also Report of the Special Rapporteur on the right to health on advancing rights-based agenda on mental health – Puras, Dainius, *Mental Health and Human Rights: Setting a Rights-based Global Agenda*, A/HRC/44/48, para 78 (2020). Available from <https://undocs.org/A/HRC/44/48>
- 80 Principle 13 of the United Nations Guiding Principles on Business and Human Rights. Office of the High Commissioner for Human Rights, *United Nations Guiding Principles on Business and Human Rights* (2011). Available from [www.ohchr.org/documents/publications/guidingprinciplesbusinesshr\\_en.pdf](http://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf)
- 81 European Commission, *ICT Sector Guide on Implementing the United Nations Guiding Principles on Business and Human Rights*, p. 15 (2014). Available from <https://op.europa.eu/en/publication-detail/-/publication/ab151420-d60a-40a7-b264-adce304e138b>
- 82 *African Union Convention on Cyber Security and Personal Data Protection* [hereafter known as “AU Convention”], 27 June 2014. Available from <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>
- 83 *Asia-Pacific Economic Cooperation Privacy Framework* [hereafter known as “APEC Privacy Framework”] (December 2005). Available from [www.apec.org/Publications/2005/12/APEC-Privacy-Framework](http://www.apec.org/Publications/2005/12/APEC-Privacy-Framework)
- 84 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [hereafter known as “EU GDPR”]. Available from <http://data.europa.eu/eli/reg/2016/679/2016-05-04>
- 85 *Standards for Data Protection for the Ibero-American States* [hereafter known as “Ibero-American Standards”] (20 June 2017). Available from <https://iapp.org/resources/Article/standards-for-data-protection-for-the-ibero-american-states>
- 86 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Available from [www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108](http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108)
- 87 United Nations Development System, *Data Privacy, Ethics and Protection: Guidance Note for Big Data for Achievement of the 2030 Agenda* (2017). Available from [https://unsdg.un.org/sites/default/files/UNDG\\_BigData\\_final\\_web.pdf](https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf); see also United Nations Chief Executives Board for Coordination, *Principles on Personal Data Protection and Privacy* (2018). Available from [www.unsceb.org/principles-personal-data-protection-and-privacy](http://www.unsceb.org/principles-personal-data-protection-and-privacy)
- 88 Synthesized from key principles in EU GDPR, Articles 12–23. Available from <https://gdpr.eu/tag/chapter-3>; *African Union Convention*, Articles 16–19; Ibero-American Standards, Chapter III (Holder’s Rights), Articles 24–32; *Council of*

- Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* [hereafter known as “Convention 108+”], Article 9 (18 May 2018). Available from [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf)
- 89 For EU GDPR, see Article 5.1-2; for the AU Convention, see Articles 13 and 22; for Convention 108+, see Article 5, [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf); for Ibero-American Standards, see chapter II; see also APEC Privacy Framework, Part III – APEC Information Privacy Principles.
- 90 For EU GDPR, Article 7; for the *AU Convention*, see Article 13; for *Convention 108+*, Article 5; for Ibero-American Standards, see Article 12; for APEC Privacy Framework, see principle V. Choice.
- 91 For EU GDPR, Article 32; see also Recital 78, Appropriate technical and organizational measures. Available from <https://gdpr.eu/recital-78-appropriate-technical-and-organizational-measures>; for the *AU Convention*, see Articles 13, 20-21; for *Convention 108+*, Article 7; for Ibero-American Standards, see Articles 19, 21, 23; for APEC Privacy Framework, see principle VII. Security safeguards.
- 92 For EU GDPR, Article 32; see also Recital 78, Appropriate technical and organizational measures. Available from <https://gdpr.eu/recital-78-appropriate-technical-and-organizational-measures>; for the *AU Convention*, see Articles 13, 20–21; for *Convention 108+*, Article 7; for Ibero-American Standards, see Articles 19, 21, 23; for APEC Privacy Framework, see principle VII. Security safeguards.
- 93 See *Convention 108+*, Article 6 – The use of biometrics should not be used when the risks of surveillance of marginalized or criminalized population outweighs the harms. See also the *AU Convention*, Article 14; Ibero-American Standards, Article 9.
- 94 Mandate of the United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data, *Draft Recommendation on the Protection and Use of Health-related Data* (2019). Available from [https://ohchr.org/Documents/Issues/Privacy/SR\\_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf](https://ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf)
- 95 Available from [www.ohchr.org/EN/Issues/Racism/SRRacism/Pages/Info-Technologies-And-Racial-Equality.aspx](http://www.ohchr.org/EN/Issues/Racism/SRRacism/Pages/Info-Technologies-And-Racial-Equality.aspx)
- 96 United Nations, Chief Executives Board for Coordination, *First Version of a Draft Text of a Recommendation on the Ethics of Artificial Intelligence* (July 2020).
- 97 See, for instance, the International Guidelines on HIV and Human Rights. Office of the High Commission for Human Rights and UNAIDS, *International Guidelines on HIV/AIDS and Human Rights* (2006). Available from [www.ohchr.org/Documents/Issues/HIV/ConsolidatedGuidelinesHIV.pdf](http://www.ohchr.org/Documents/Issues/HIV/ConsolidatedGuidelinesHIV.pdf)
- 98 For another United Nations resource that assesses the benefits and risks of digital technology, see [www.unglobalpulse.org/policy/risk-assessment/#:~:text=The%20Risks%2C%20Harms%20and%20Benefits,Benefits%20Assessment%20should%20be%20conducted](http://www.unglobalpulse.org/policy/risk-assessment/#:~:text=The%20Risks%2C%20Harms%20and%20Benefits,Benefits%20Assessment%20should%20be%20conducted)
- 99 For examples of legitimate purposes, see discussion on the EU GDPR and *Convention 108+*.
- 100 For more guiding principles on COVID-19 contact tracing apps, see World Health Organization, *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing – Interim guidance* (28 May 2020).
- 101 Adapted from World Health Organization. *Classification of digital health interventions v1.0* (2018). Available from [www.who.int/reproductivehealth/publications/mhealth/classification-digital-health-interventions/en](http://www.who.int/reproductivehealth/publications/mhealth/classification-digital-health-interventions/en)
- 102 “eHealth”. World Health Organization. Available from [www.who.int/ehealth/en](http://www.who.int/ehealth/en). Accessed 3 September 2020.
- 103 “What is MomConnect?”, Department of Health – Republic of South Africa. Available from [www.health.gov.za/index.php/mom-connect](http://www.health.gov.za/index.php/mom-connect). Accessed 3 September 2020; see also “MomConnect South Africa”, Praekelt.org. Available from [www.praekelt.org/momconnect](http://www.praekelt.org/momconnect). Accessed 3 September 2020.
- 104 Andrey Rylkov Foundation. *2018 Annual Report*. Available from <https://rylkov-fond.org/files/2019/04/AIDS-fonds-final-report-RUS-17.04.pdf>
- 105 Humanitarian Project NGO, *2019 Activity Report*. Available from <https://human.org.ru/otchet>
- 106 ICT Works, How Telehealth is Preserving HIV Service Delivery during COVID-19 (15 January 2021). Available from [www.ictworks.org/telehealth-hiv-service-delivery-covid-19/#.YBmatehKg2x](http://www.ictworks.org/telehealth-hiv-service-delivery-covid-19/#.YBmatehKg2x). Accessed 2 February 2021.
- 107 UNICEF Eastern and South Africa, UNICEF’s HIV Programming in the Context of COVID-19: Sustaining the gains and reimagining the future for children, adolescents and women (July 2020). Available from [www.unicef.org/esa/media/6621/file/HIV%20COVID-19%20Compendium%20-July%202020.pdf](http://www.unicef.org/esa/media/6621/file/HIV%20COVID-19%20Compendium%20-July%202020.pdf)
- 108 Hemapriya, D., Viswanath, P., Mithra, V. M., Nagalakshmi, S., Umarani, G., Wearable medical devices — Design challenges and issues. In 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT) pp. 1–6. IEEE. (March 2017).
- 109 Vashist, S.K., Point-of-care diagnostics: Recent advances and trends. *Biosensors* 2017, 7(4). 62 (4) (2017).

- 110 UNICEF, CHAI, ASLM, EGPAF, CDC, WHO, Unitaid, *Key Considerations for Introducing New HIV Point-of-Care Diagnostic Technologies in National Health Systems* (2018). Available from [http://childrenandaids.org/sites/default/files/poc-toolkit/KCD\\_draft\\_English\\_Low-Res.pdf](http://childrenandaids.org/sites/default/files/poc-toolkit/KCD_draft_English_Low-Res.pdf)
- 111 World Health Organization and European Respiratory Society, *Digital Health for the End TB Strategy: An Agenda for Action* (2015). Available from [www.who.int/tb/areas-of-work/digital-health/Digital\\_health\\_EndTBstrategy.pdf?ua=1](http://www.who.int/tb/areas-of-work/digital-health/Digital_health_EndTBstrategy.pdf?ua=1); see also Garcia-Basteiro, A.L., DiNardo, A., Saavedra, B., Silva, D.R., Palmero, D., Gegia, M., Migliori, G.B., et al., *Point of care diagnostics for tuberculosis*, *Pulmonology Journal*, Vol. 24, Issue 2 (March–April 2018), pp.73–85. Available from <https://doi.org/10.1016/j.rppnen.2017.12.002>
- 112 World Health Organization, *Guideline: Recommendations on digital interventions for health system strengthening*. Geneva (2019).
- 113 Saberi, P., Catz, S.L., Leyden, W.A., et al., Antiretroviral therapy adherence and use of an electronic shared medical record among people living with HIV. *AIDS and Behavior*. 2015; 19:177–185.
- 114 Within the context of providing cancer care and treatment, see Snyder, C.F., Wu, A.W., Miller, R.S., Jensen, R.E., Bantug, E.T., Wolff, A.C., The role of informatics in promoting patient-centered care. *Cancer J*. 2011;17(4):211–218. doi: 10.1097/PPO.0b013e318225ff89
- 115 World Health Organization Executive Board resolution, *Health Informatics and Telemedicine: Report by the Director-General*, EB99/30 (6 January 1997). Available from [https://apps.who.int/iris/bitstream/handle/10665/173171/EB99\\_30\\_eng.pdf?sequence=1&isAllowed=y](https://apps.who.int/iris/bitstream/handle/10665/173171/EB99_30_eng.pdf?sequence=1&isAllowed=y)
- 116 See Braitstein, P., Einterz, R.M., Sidle, J.E., Kimaiyo S., Tierney W., “Talkin’ about a revolution”: How electronic health records can facilitate the scale-up of HIV care and treatment and catalyze primary care in resource-constrained settings. *J Acquir Immune Defic Syndr*. 52 Suppl 1 (Nov. 2009); S54–7; see also Herwehe, J., Wilbright, W., Abrams, A., Bergson, S., Foxhood, J., Kaiser, M., Magnus, M., Implementation of an innovative, integrated electronic medical record (EMR) and public health information exchange for HIV/AIDS. *Journal of the American Medical Informatics Association*, 19(3) (2012) 448–452; and Aragonés, C., Campos, J. R., Pérez, D., Martínez, A., Pérez, J., SIDATRA: informatics to improve HIV/AIDS care. *MEDICC review*, 14(4). 5–9 (2021).
- 117 World Health Organization, *Telemedicine: opportunities and developments in Member States: report on the second global survey on eHealth* (Global Observatory for eHealth Series, 2) (2010). Available from [www.who.int/goe/publications/goe\\_telemedicine\\_2010.pdf](http://www.who.int/goe/publications/goe_telemedicine_2010.pdf).
- 118 Zolfo, M., Bateganya, M. H., Adetifa, I. M., Colebunders, R., Lynen, L., A telemedicine service for HIV/AIDS physicians working in developing countries. *Journal of telemedicine and telecare*, 17(2) (2011) 65–70. Available from <https://doi.org/10.1258/jtt.2010.100308>
- 119 Rogers, B.G., Coats, C.S., Adams, E., et al., Development of Telemedicine Infrastructure at an LGBTQ+ Clinic to Support HIV Prevention and Care in Response to COVID-19, Providence, RI. *AIDS Behav.*24(10) (2020). 2743–2747. doi:10.1007/s10461-020-02895-1
- 120 ICT Works, How Telehealth is Preserving HIV Service Delivery During COVID-19 (15 January 2021). Available from [www.ictworks.org/telehealth-hiv-service-delivery-covid-19/#.YBmatehKg2x](http://www.ictworks.org/telehealth-hiv-service-delivery-covid-19/#.YBmatehKg2x). Accessed 2 February 2021.
- 121 Colombia: Gomez Sarmiento, Isabelle, “The Pandemic And Legal Abortion: What Happens When Access Is Limited?” National Public Radio (8 June 2020). Available from [www.npr.org/sections/goatsandsoda/2020/06/08/864970278/lockdown-limits-access-to-legal-abortion-in-colombia-telemedicine-is-now-an-opti](http://www.npr.org/sections/goatsandsoda/2020/06/08/864970278/lockdown-limits-access-to-legal-abortion-in-colombia-telemedicine-is-now-an-opti); United Kingdom: Margolis, Hillary, “England Leads Way in UK after U-Turn on COVID-19 Abortion Access”, Human Rights Watch (31 March 2020). Available from [www.hrw.org/news/2020/03/31/england-leads-way-uk-after-u-turn-covid-19-abortion-access](http://www.hrw.org/news/2020/03/31/england-leads-way-uk-after-u-turn-covid-19-abortion-access)
- 122 Sze-Yunn, Pang, “Telehealth could be a game-changer in the fight against COVID-19. Here’s why”, World Economic Forum (1 May 2020). Available from [www.weforum.org/agenda/2020/05/telehealth-could-be-a-game-changer-in-the-fight-against-covid-19-here-s-why](http://www.weforum.org/agenda/2020/05/telehealth-could-be-a-game-changer-in-the-fight-against-covid-19-here-s-why)
- 123 World Bank Group and Digital Impact Alliance, *The Role of Digital Identification for Healthcare: The Emerging Use Cases* (2018). Available from <http://documents1.worldbank.org/curated/en/595741519657604541/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf>
- 124 Anne, N., Dunbar, M. D., Abuna, F., Simpson, P., Macharia, P., Betz, B., et al., Feasibility and acceptability of an iris biometric system for unique patient identification in routine HIV services in Kenya. *International journal of medical informatics*, 133, 104006 (2020). Available from <https://doi.org/10.1016/j.ijmedinf.2019.104006>
- 125 Davis, S.L.M., Esom, K., Gustav, R., Maleche, A., Podmore, M., A Democracy Deficit in Digital Health?, *Health and Human Rights Journal* (16 January 2020). Available from [www.hhrjournal.org/2020/01/a-democracy-deficit-in-digital-health](http://www.hhrjournal.org/2020/01/a-democracy-deficit-in-digital-health); see also Davis, S.L.M., Contact Tracing Apps: Extra Risks for Women and Marginalized Groups, *Health and Human Rights Journal* (29 April 2020). Available from [www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups](http://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups)

- 126 World Health Organization, *Guideline: Recommendations on digital interventions for health system strengthening*. Geneva (2019).
- 127 World Health Organization, "Human Genomics in Global Health", Available from [www.who.int/genomics/geneticsVSgenomics/en](http://www.who.int/genomics/geneticsVSgenomics/en). Accessed 3 September 2020.
- 128 Telenti, A., Goldstein, D.B., Genomics meets HIV-1. *Nature Reviews Microbiology*, 4(11) (2006). 865–873.
- 129 U.S. Centers for Disease Control, *Detecting and Responding to HIV Transmission Clusters: a Guide for Health Departments* (2018). Available from [www.cdc.gov/hiv/pdf/funding/announcements/ps18-1802/CDC-HIV-PS18-1802-AttachmentE-Detecting-Investigating-and-Responding-to-HIV-Transmission-Clusters.pdf](http://www.cdc.gov/hiv/pdf/funding/announcements/ps18-1802/CDC-HIV-PS18-1802-AttachmentE-Detecting-Investigating-and-Responding-to-HIV-Transmission-Clusters.pdf)
- 130 Coltart, C.E.M., Hoppe, A., Parker, M., et al., Ethical considerations in global HIV phylogenetic research. *Lancet HIV*. 5(11) (2018): e656–e666. doi:10.1016/S2352-3018(18)30134-6. Available from [www.ncbi.nlm.nih.gov/pmc/Articles/PMC7327184/](http://www.ncbi.nlm.nih.gov/pmc/Articles/PMC7327184/)
- 131 Dash, S., Shakyawar, S.K., Sharma, M. et al., Big data in health care: management, analysis and future prospects. *J Big Data* 6, 54 (2019). Available from <https://doi.org/10.1186/s40537-019-0217-0>
- 132 Jannes, M., Friele, M., Jannes, C., Woopen, C., *Algorithms in Digital Healthcare: An Interdisciplinary Analysis*, Cologne Center for Ethics, Rights, Economics and Social Sciences of Health and Bertelsmann Stiftung (2019). Available from [www.bertelsmann-stiftung.de/fileadmin/files/BS/Publikationen/GrauePublikationen/BS\\_Algorithms\\_Healthcare.pdf](http://www.bertelsmann-stiftung.de/fileadmin/files/BS/Publikationen/GrauePublikationen/BS_Algorithms_Healthcare.pdf)
- 133 Young, S.D., A "big data" approach to HIV epidemiology and prevention. *Preventive medicine*, 70 (2015) 17–18.
- 134 Jokonya, O., Towards a Big Data Framework for the Prevention and Control of HIV/AIDS, TB and silicosis in the mining industry. *Procedia Technology*, 16 (2014). 1533–1541.
- 135 Young S.D., Zhang Q., Using search engine big data for predicting new HIV diagnoses. *PLoS ONE* 13(7) (2018) e0199527 <https://doi.org/10.1371/journal.pone.0199527>
- 136 "Overview: Artificial Intelligence", Oxford Reference. Available from [www.oxfordreference.com/view/10.1093/oi/authority.20110803095426960](http://www.oxfordreference.com/view/10.1093/oi/authority.20110803095426960). Accessed 3 September 2020.
- 137 Ramachandran A., Kumar A, Koenig H., et al., Predictive Analytics for Retention in Care in an Urban HIV Clinic. *Sci Rep*. 2020;10(1):6421 (14 Apr 2020). doi:10.1038/s41598-020-62729-x. Available from [www.ncbi.nlm.nih.gov/pmc/Articles/PMC7156693](http://www.ncbi.nlm.nih.gov/pmc/Articles/PMC7156693)
- 138 Wahl, B., Cossy-Gantner, A., Germann, S., Schwalbe, N.R., Artificial intelligence (AI) and global health: How can AI contribute to health in resource-poor settings? *BMJ global health*, 3(4) (2018) e000798.
- 139 Vamathevan, J., Clark, D., Czodrowski P, et al., Applications of machine learning in drug discovery and development. *Nat Rev Drug Discov*. 2019;18(6):463-477. doi:10.1038/s41573-019-0024-5
- 140 For nanotechnology, see das Neves, J., Novel Approaches for the Delivery of Anti-HIV Drugs—What Is new? *Pharmaceutics* 2019, 11(11) (2019) 554. For genomics sequencing, see Telenti, A., Goldstein, D.B., Genomics meets HIV-1. *Nature Reviews Microbiology*. 4(11) (2006) 865–873.
- 141 Whitelaw, S. et al., *Applications of digital technology in COVID-19 pandemic planning and response*, *Lancet Digital Health* (29 June 2020). DOI:[https://doi.org/10.1016/S2589-7500\(20\)30142-4](https://doi.org/10.1016/S2589-7500(20)30142-4).



...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...

...the ...



United Nations Development Programme  
One United Nations Plaza, New York,  
NY 10017, USA

UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at [undp.org](https://undp.org) or follow at [@UNDP](https://twitter.com/UNDP)

[Edgar A. Whitley](#)

## Trusted digital identity provision: GOV.UK Verify's federated approach

### Report

**Original citation:**

Whitley, Edgar A. (2018) *Trusted digital identity provision: GOV.UK Verify's federated approach*. CGD policy paper, 131. Center for Global Development, Washington, USA.

Originally available from the [Center for Global Development](#)

This version available at: <http://eprints.lse.ac.uk/90577/>

Available in LSE Research Online: November 2018

© 2018 [CGD](#)  
CC BY-NC 4.0

LSE has developed LSE Research Online so that users may access research output of the School. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LSE Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain. You may freely distribute the URL (<http://eprints.lse.ac.uk>) of the LSE Research Online website.

# Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach

**Edgar A. Whitley**

## Abstract

The UK's recently launched GOV.UK Verify service relies on a novel federated approach for digital identity verification. Accredited private companies are tasked with verifying the identities of individuals to enable them to access various government services and portals. The private identity providers can draw on a number of public and private databases to validate users' identities to a given level of identity assurance. The paper provides an overview of the GOV.UK Verify approach to identity verification. It describes the government's motivations for developing such a system; the standards, principles, and governance arrangements that underpin it; and how the identity proofing and verification works in practice. It considers the expansion of the Verify model for other government and private sector uses and discusses the exclusion, privacy, and liability risks associated with the use of the system. Finally, the paper highlights important lessons for other countries seeking to develop similar systems for digital access.

Keywords: Digital identity, identity assurance, federated identity, privacy, GOV.UK Verify

Edgar A. Whitley. 2018. "Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach" CGD Policy Paper. Washington, DC: Center for Global Development. <https://www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated-approach>

CGD is grateful for contributions from Bill & Melinda Gates Foundation in support of this work.

Center for Global Development  
2055 L Street NW  
Fifth Floor  
Washington DC 20036  
202-416-4000  
[www.cgdev.org](http://www.cgdev.org)

This work is made available under  
the terms of the Creative Commons  
Attribution-NonCommercial 4.0  
license.

 Center  
for Global  
Development  
[www.cgdev.org](http://www.cgdev.org)

CGD Policy Paper 131  
November 2018

## **Preface**

The United Kingdom’s GOV.UK Verify service offers a unique model for proving one’s identity online. As a country with no national ID or other universally held common identifier, its identity verification process rests on a risk- and standards-based approach that allows identities to be verified to different levels of assurance, as required for accessing a given service or transaction. Unlike most other identification systems where the government acts as the identity provider, verifier, and user, here the identity verification process is carried out by accredited private sector entities who collect “identity evidence” by checking user data against a diverse set of publicly and privately held records. Though Verify’s implementation is still in early stages, its unique, federated approach to digital identity verification, its operational standards, as well as its closely embedded privacy principles can offer many lessons for governments as well as private entities seeking to provide online access to services and transactions.

The UK’s enduring concerns for preserving privacy are evident from all aspects of Verify’s design. Identity-verifying companies do not know which government service the user has requested access to, nor can the government service providers tell which private entity has verified their user’s identity. Another remarkable feature of the UK’s system is its use of levels of identity assurance instead of a single “gold-standard” identity required to access government services online. The identity assurance framework and the standards developed for determining what forms of identity evidence satisfy each level of identity assurance provide valuable guidance for other countries and can be easily adapted to different contexts.

Verify’s risk-based approach to identity verification can be particularly useful where no single, national ID exists, but it also points to the value of supplementing official identification with other “dynamic” evidence of identity. While it may not provide first-stage “foundational” identification—still a priority for many developing countries—it offers insights that will become more valuable with the spread of digital societies and economies.

Alan Gelb  
Senior Fellow  
Center for Global Development

For Janet Hughes, programme director of GOV.UK Verify between 2013 and 2016, who encouraged her team to “be bold.”

## **About the Author**

Dr. Edgar A. Whitley is an Associate Professor (Reader) in Information Systems in the Department of Management at the London School of Economics and Political Science.

Edgar was the research coordinator of the influential LSE Identity Project on the UK's proposals to introduce biometric identity cards; proposals that were scrapped following the 2010 general election. He has been closely involved in the development of GOV.UK Verify and is co-chair of the UK Cabinet Office Privacy and Consumer Advisory Group. Edgar has also advised governments in Brazil, Chile, Ecuador, India, Jamaica, Japan, and Mexico about the political, technological, and social challenges of effective identity policies and has contributed to reports for Omidyar Network and the World Bank on various aspects of digital identity systems.

He has a BSc (Econ) and PhD in Information Systems, both from the LSE. He is the co-editor of *Information Technology and People*, senior editor for the *Journal of Information Technology* and for the *AIS Transactions of Replication Research* and an associate editor for the *Journal of the AIS*.

## **Disclaimer**

Although this report draws on information obtained from Edgar's close working relationship with Verify, all inferences and assessments are his own and should not be taken as inferring or implying anything regarding official UK government policy for Verify and its associated services. This report has benefited from suggestions by the GDS team. These should not be taken as an endorsement of the document or confirmation of its accuracy but were provided in the spirit of supporting transparency in GOV.UK Verify operations.

## **How to Read this Report**

This report consists of six main sections. Section A provides an overview of GOV.UK Verify, including details of how it operates and a summary of the socio-political context that resulted in its distinctive approach. The next three sections provide more detailed descriptions of how Verify works (section B), how it was built and operates (section C), and its governance arrangements (section D). Each of these detailed sections can be read in isolation from the others. Section E outlines the next steps for Verify now that it is a live service, including future applications and critiques of the approach it adopts. Nevertheless, evaluating the broader politics and pragmatics of delivering digital government in the UK is beyond the scope of this report. Section F reflects on the lessons that can be learned from Verify in relation to the World Bank principles on identification for sustainable development as the design choices that underpin the Verify model can provide a useful template against which current and future identity practices can be contrasted. For example, reflecting on the innovations that arise from Verify's use of multiple identity providers may provide trigger innovative improvements in the customer experience even when the government acts as the sole identity provider. Appendices provide a glossary of key terms and abbreviations as well as a more detailed historical background to Verify.

**Table of Contents**

- A. Overview..... 7
  - Introducing GOV.UK Verify ..... 7
  - Typical Verify User Journeys ..... 8
  - Understanding the Socio–political Context of Verify ..... 22
- B. How Verify Works ..... 25
  - Verify’s Approach to Identity Proofing and Verification ..... 25
  - Identity Proofing and Verification in Practice ..... 29
  - Innovation in Identity Authentication ..... 36
  - Using a Verify’d Identity to Access Government Services..... 36
  - Paying for Verify..... 37
- C. Building and Running Verify ..... 40
  - Integration with Online Government Services..... 42
- D. Verify’s Governance Arrangements..... 43
  - Openness and Transparency..... 43
  - Embedding Privacy in Verify..... 45
  - Governance Structures ..... 50
- E. Verify: Life After Live ..... 55
  - Working with Local Authorities..... 57
  - Private Sector use of Verify’d Identities ..... 57
  - EU Integration, eIDAS, and BREXIT’ ..... 58
  - Future Government Services Using Verify ..... 60
  - Limitations and Critiques ..... 63
- F. Learning from Verify..... 65
  - 1. Ensuring Universal Coverage for Individuals from Birth to Death, Free from Discrimination..... 65
  - 2. Removing Barriers to Access and Usage and Disparities in the Availability of Information and Technology..... 66
  - 3. Establishing a Robust—Unique, Secure, and Accurate—Identity..... 66
  - 4. Creating a Platform that Is Interoperable and Responsive to the Needs of Various Users ..... 67
  - 5. Using Open Standards and Ensuring Vendor and Technology Neutrality ..... 69



6. Protecting User Privacy and Control through System Design.....	69
7. Planning for Financial and Operational Sustainability without Compromising Accessibility .....	70
8. Safeguarding Data Privacy, Security, and User Rights through a Comprehensive Legal and Regulatory Framework .....	70
9. Establishing Clear Institutional Mandates and Accountability .....	71
10. Enforcing Legal and Trust Frameworks through Independent Oversight and Adjudication of Grievances.....	71
Functional? Foundational? What Verify Is and Isn't.....	71
G. Appendices.....	73
Appendix 1: Glossary and Abbreviations.....	73
Appendix 2: Historical Background to Verify.....	75
H. References.....	80

## List of Figures

Figure 1. GOV.UK Verify: Start of a user journey .....	9
Figure 2. GOV.UK Verify: New and existing users.....	10
Figure 3. GOV.UK Verify: Introducing the certified companies .....	10
Figure 4. GOV.UK Verify: What identity documents are to hand?.....	11
Figure 5. GOV.UK Verify: What technologies are to hand?.....	12
Figure 6. GOV.UK Verify: Choose a company.....	13
Figure 7. Experian: Account creation.....	14
Figure 8. Experian: Basic details collection .....	15
Figure 9. Experian: Document checks .....	16
Figure 10. Experian: Proving it's you .....	17
Figure 11. Experian: Financial data identity test.....	18
Figure 12. Experian: Account security .....	19
Figure 13. Experian: Verification complete.....	19
Figure 14. GOV.UK Verify: Reusing an existing identity account.....	20
Figure 15. Data flows in Verify.....	21
Figure 16. The traditional checking model when government acts as the identity provider.....	30
Figure 17. Identity checking in Verify .....	31
Figure 18. Matching Service Adapter as a black box interface to Verify.....	43

Figure 19. Number of users (October 2014–July 2018) .....	44
Figure 20. Existing users signing in each week (October 2014–July 2018) .....	45
Figure 21. Verify governance taken from (GOV.UK Verify 2015d).....	51

## List of Tables

Table 1. Identity proofing and verification elements and scores .....	26
Table 2. Examples of various forms of identity evidence.....	28
Table 3. Illustrative examples of activity events.....	29
Table 4. Live and onboarding central government uses of Verify.....	60
Table 5. Future central government uses of Verify.....	62

## A. Overview

### Introducing GOV.UK Verify

GOV.UK Verify is a way to prove who you are online in the United Kingdom, providing a safe, simple and fast access to government services like submitting a tax return or checking driving licence information (GOV.UK Verify 2018a, 2016a).

At the time of finalising this report (July 2018—a real-time list of available services is available at (GOV.UK Verify 2018b)), individuals can use Verify to:

- check your income tax (HM Revenue & Customs)
- check your state pension (Department for Work and Pensions, HM Revenue & Customs)
- claim a tax refund (HM Revenue & Customs)
- claim for redundancy payment (Insolvency Service)
- disclosure and barring service (Home Office)
- get your state pension (Department for Work and Pensions)
- help your friends or family with their tax (HM Revenue & Customs)
- PAYE for employees: Company car (HM Revenue & Customs)
- personal tax account (HM Revenue & Customs)
- renew your short-term medical driving licence (DVLA)
- report a medical condition that affects your driving (DVLA)
- rural payments (DEFRA)
- self-assessment tax return (HM Revenue & Customs)
- sign your mortgage deed (HM Land Registry)
- Universal Credit Digital Service (Department for Work and Pensions)
- vehicle operator licensing (DVSA)
- view or share your driving licence information (DVLA)

A range of further central government services are currently in progress for becoming live services. Discovery work is also being undertaken with local authorities to integrate Verify into local authority service provision (GOV.UK Verify 2016b). Additionally, there are a number of industry (private sector) projects at various stages of development and the intention is that the identity infrastructure behind Verify will enable private sector as well as public sector use.

As a fully operational system Verify has four key features that have resulted in a distinctive identification system. Whilst not all of these features are immediately replicable in other contexts, both individually and collectively they offer key exemplars that can influence the provision of identity related services globally. The key features of Verify (the “Verify model”) are:

- risk- and standards-based approach to identity verification and authentication;
- federated architecture involving multiple identity providers that encourages innovation in both verification and authentication activities;

- privacy-by-design approach that embeds privacy principles in contracts, memoranda of understanding and norms and includes expert oversight of privacy and consumer issues;
- user focussed service delivery approach that includes an emphasis on transparency and engagement with all relevant stakeholders and diverse users.

## **Typical Verify User Journeys**

As Verify offers a relatively novel approach to digital identity practices, the best way to understand it is to follow two typical user journeys that provide a useful illustration of how Verify operates in practice. The first journey involves a user creating a Verify'd identity in order to access an online government service. The second involves the same user re-using their previously created Verify'd identity to access another online government service.

### **User Journey 1: Creating a Verify'd Identity to Access Online Government Services**

In this user journey, a user intends to access an online government service such as submitting their tax return online. In 2016 89 percent of self-assessment returns were completed online (BBC News 2016). Having found the self-assessment page (<https://www.gov.uk/log-in-file-self-assessment-tax-return>) on the GOV.UK website, the user is invited to sign in (see figure 1).<sup>1</sup> There are two ways to sign in, via GOV.UK Verify or via the Government Gateway (which is due to be decommissioned in 2018 (Hall 2016)).

Creating a Verify'd identity can normally be done in 10–15 minutes (GOV.UK Verify 2018a). In contrast, the final stage of setting up and using a Government Gateway account typically involves a secure activation code that needs to be sent to the user in the post. As a result, the process of setting up a Government Gateway account can take up to seven days. This can be problematic for citizens as there are penalties of up to £100 for late submission of tax returns (Whitley 2015).

---

<sup>1</sup> Screenshots are based on a user journey undertaken in late June 2016. The whole journey is reviewed regularly alongside being used for A/B testing, so wording, fonts, branding and steps are subject to change.

Figure 1. GOV.UK Verify: Start of a user journey

# Sign in and file your Self Assessment tax return

[Sign in to your online account](#) to send your tax return to HM Revenue and Customs (HMRC). You can go back to a tax return you've already started.

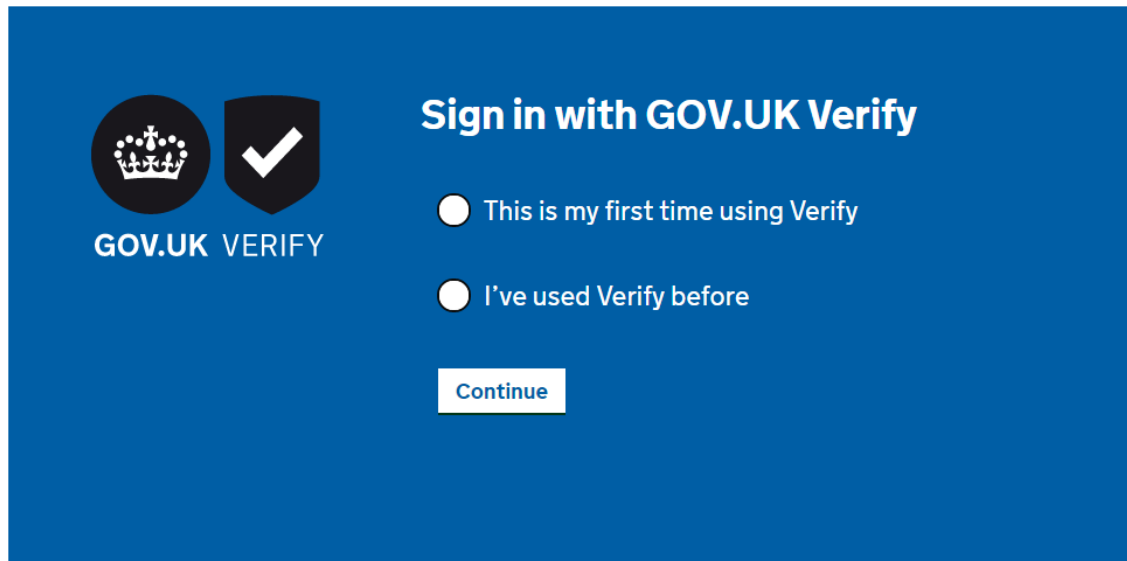
This page is also available [in Welsh \(Cymraeg\)](#).

Use the user ID and password you got when you [registered for Self Assessment](#) or when you set up your HMRC online account.

You can also sign in with a [GOV.UK Verify](#) account.

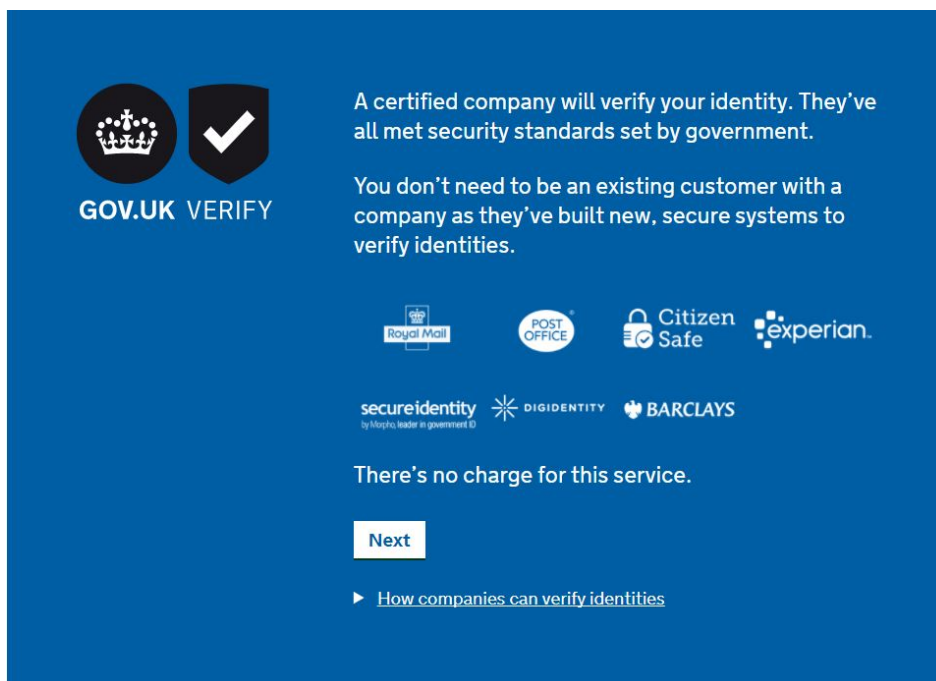
A user who chooses to use Verify then states whether this is their first time using Verify or if they have used the service before, see figure 2 as there is no obvious way to check whether a particular individual has used the service previously. This also means that a user can create a new Verify'd identity with a different identity provider by following the "first time using Verify" option.

Figure 2. GOV.UK Verify: New and existing users



First-time users are then told about the Verify service and the certified companies who will verify their identity. This also informs them that the companies meet government security standards and that there is no charge to use the service, see figure 3.

Figure 3. GOV.UK Verify: Introducing the certified companies



Next, users are (currently) asked a few questions that will help determine which of the certified companies will best be able to undertake the identity verification checks on them. The companies can draw on different data sets for identity verification and offer different technical solutions (e.g., apps) for identity verification and authentication. For example, not all the companies may be able to use identity documents issued by countries other than the UK, whilst some can do the identity checks for UK nationals who only have some “standard” documents, see figure 4. Some allow for verification and authentication using user installed apps, see figure 5.

Figure 4. GOV.UK Verify: What identity documents are to hand?

# Select all the documents you have

Certified companies use information from different identity documents to verify you.

## Do you have these documents with you?

1. UK photocard driving licence (excluding Northern Ireland)  Yes  No

2. UK passport  Yes  No

3. Identity document from another country (passport, ID card or driving licence)  Yes  No

I don't have any of these documents with me

**Continue**

Figure 5. GOV.UK Verify: What technologies are to hand?

## Do you have a mobile phone or tablet?

Certified companies can send security codes to your mobile.

Yes  No

Can you install apps on your device?

Yes

No

I don't know

[Continue](#)

Based on the answers to these and other pre-selection questions, the user is presented with a list of certified companies that are “likely” to be able to verify their identities, see figure 6. In some circumstances, for example, a potential user with no UK address, it will not be possible to obtain a Verify’d identity and the user will be advised to contact the relevant service directly. In other cases, the user answers might result in a warning that they may not be able have their identity verified and would need to contact the relevant service directly but also giving them the option nevertheless to try using Verify.







Figure 6. GOV.UK Verify: Choose a company

### Choose a company

- [Why there's a choice of companies](#)

Based on your answers, 4 companies can verify you now:

 <a href="#">About Post Office</a>	<a href="#">Choose Post Office</a>
 <a href="#">About CitizenSafe</a>	<a href="#">Choose CitizenSafe</a>
 <a href="#">About Digidentity</a>	<a href="#">Choose Digidentity</a>
 <a href="#">About Experian</a>	<a href="#">Choose Experian</a>

We've filtered out 4 companies, as they're unlikely to be able to verify you based on your answers.

- ▶ [Companies that are unlikely to verify you](#)

Choosing one of these companies, for example Experian, takes the user to an account creation page with the certified company, see figure 7.

Figure 7. Experian: Account creation

**FREE, SAFE AND SECURE.**  
Join thousands of others who have chosen Experian as their GOV.UK identity provider.

**Creating your identity account**

**Email**  
Enter your email address  
We will not spam this email address.

**Create Password**  
At least 8 characters, 1 uppercase, 1 lowercase & 1 number.

**Confirm Password**  
Confirm your password

I agree to the Experian [Privacy Policy](#) and [Terms and Conditions](#)

Cancel **Let's get started**

Already have an account? [Sign in](#)

**FREE**  
Your Experian Identity Account is completely free.

**SAFE**  
We pride ourselves in keeping your information safe from prying eyes.

**SECURE**  
Your information is protected using the latest encryption standards.

[Terms & Conditions](#) [Privacy Policy](#) [FAQs](#) [Contact Us](#)


Experian registered in England and Wales under the company registration number 653331.

This creates an account with the certified company and next the user provides basic details that are used to start the verification process, figure 8. As noted above, these screenshots, used with permission, were taken from the process as at late June 2016. The whole journey is reviewed regularly so wording, fonts, branding, and steps are subject to change.

Figure 8. Experian: Basic details collection

## Your Details

We need to gather some information about you so we can perform the identity check.

 Quick Tip. All fields are mandatory unless stated otherwise, if you're concerned as to why we need this information click on the icon

### Why do you need this information?

Experian uses this information to verify your identity using guidelines set out by the Government.


All information collected is done so in accordance with the Data Protection Act 1998.

**Title**

**First Name(s)**

**Middle Name or Initial**

**Surname**

**Previous Surname**  
 

**Date of Birth**

**Gender**  
 Male  
 Female  
 Not Specified

**Mobile Phone Number**

**Home Phone Number**

[Cancel](#)

Experian also ask for address details and then begins the identity verification process based on the data entered by the user as well as data that they have access to. Identity verification normally involves further checks, for example, against government issued documents such as passports and driving licences, see figure 9.

Figure 9. Experian: Document checks

## Identity Check

### Document Check

---

We need to verify your identity.

The easiest way for us to do this is for you to enter details from your driving licence and/or passport.

If you **don't** have a driving licence or passport, please select "I don't own either of these documents" below.

If you have a driving licence or passport, but don't have these documents to hand, you can [save and finish later](#).

Select your document choice:

 UK photocard Driving Licence	 UK Passport	 UK photocard Driving Licence & UK Passport	 I don't own either of these documents
---	--	---	---

[Finish Later](#)

[Continue](#)

#### How safe is my information?

---

We will check the details you enter against the appropriate records held by the Passport Office or the DVLA.

Experian do not have access to these records. We will simply receive a confirmation that the details match.


This will help us prove your identity and make sure it is really you we are dealing with.

---

Figure 10. Experian: Proving it's you






## Proving It's You - We Need More Information

### Additional Information

 Success: Your **Driving Licence** details have been submitted and are currently being checked.

We need to gather further information to check your identity, please select **one** of the following options:

**Verification options:**

 <p>Current Account</p>	<p>Current accounts for Banks and Building Societies only. <b>No payment will be taken.</b></p>	 <p>UK Passport</p>	<p>We will check the details you enter against the appropriate records held by the Passport Office.</p>
 <p>Identity Test</p>	<p>Answer a question based on information Experian has access to. <a href="#">What is an Identity Test?</a></p>	 <p>Credit or Debit Card</p>	<p>Visa, Maestro and MasterCard only. <b>NO payment will be taken</b> and your full card number will not be stored.</p>
 <p>I am unable to supply any of these options</p>	<p>Only select if you don't have any of the verification options. If you don't have them to hand you can always save and finish later.</p>		

Finish LaterContinue

Entering driving licence details allows them to be checked with the Driver and Vehicle Licencing Agency (DVLA) in terms of a “confirmation that the details match.” Whilst those details are being checked, Experian allows the user to provide further information to “prove it's you.” The range of additional information types that can be provided is given in figure 10. Choosing the identity test option will result in “knowledge-based” questions being asked, such as asking who has provided the user with a credit card and what the recent closing balance on that account was, see figure 11. Not all identity providers offer the option of knowledge-based questions and draw on other methods of identity verification instead.

Figure 11. Experian: Financial data identity test

## Identity Check

### Identity Test

---

Please answer all of the following questions:

▶ [More about identity test questions](#)

**Who provides one of your credit cards?**

- SANTANDER CARDS UK (BURTON)
- IKANO BANK AB
- JOHN LEWIS FINANCIAL SERVICES
- METRO BANK PLC
- VIRGIN MONEY PLC

**What was the closing balance of this credit card, as shown on your May statement?**

£



Finish Later

Continue

A final step in the Experian process is setting up account security, see figure 12.

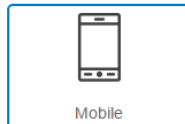
Figure 12. Experian: Account security

## Account Security

### Securing your Information

When you use your Experian Identity Account to access other government services, we need you to set up additional security to quickly and securely confirm that it's you logging on.

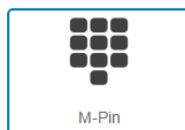
To allow us to do this you will need to choose one of the following Account Security options:



We will send a code by text message each time you log into your account.



We will send a code to your landline phone number each time you log into your account.



You set up a pin which you will need to use each time you log into your account.

[What is M-Pin?](#)

Cancel

Continue

#### Why do I need to set up extra security?


The security of your data is very important to us.

Extra security is used to make sure your account can't be accessed by other people.

Each security option is used in addition to your log-in credentials and is commonly referred to as second-factor authentication.

Once a suitable form of account security has been set up (in this case, setting up a secure PIN using the M-Pin app), Experian confirms that the identity has been verified and the account can now be used to sign in to the requested online service, see figure 13.

Figure 13. Experian: Verification complete



**GOV.UK VERIFY**

## Experian has verified your identity

You can now sign in wherever you see the GOV.UK Verify logo

[Complete your self assessment](#)

At this point, the user is in the (in this case) HMRC system and can complete their tax self-assessment.








### User Journey 2: Using an Existing Verify'd Account to Access Online Government Services

Creating a Verify'd account only needs to be done once. The next time the user wants to work on their tax return, they indicate, at the step illustrated in figure 2, that they have used Verify before. They are then asked which company they have their account with, see figure 14.

Figure 14. GOV.UK Verify: Reusing an existing identity account

## Who do you have an identity account with?

If you don't have an identity account, you can [start now](#).

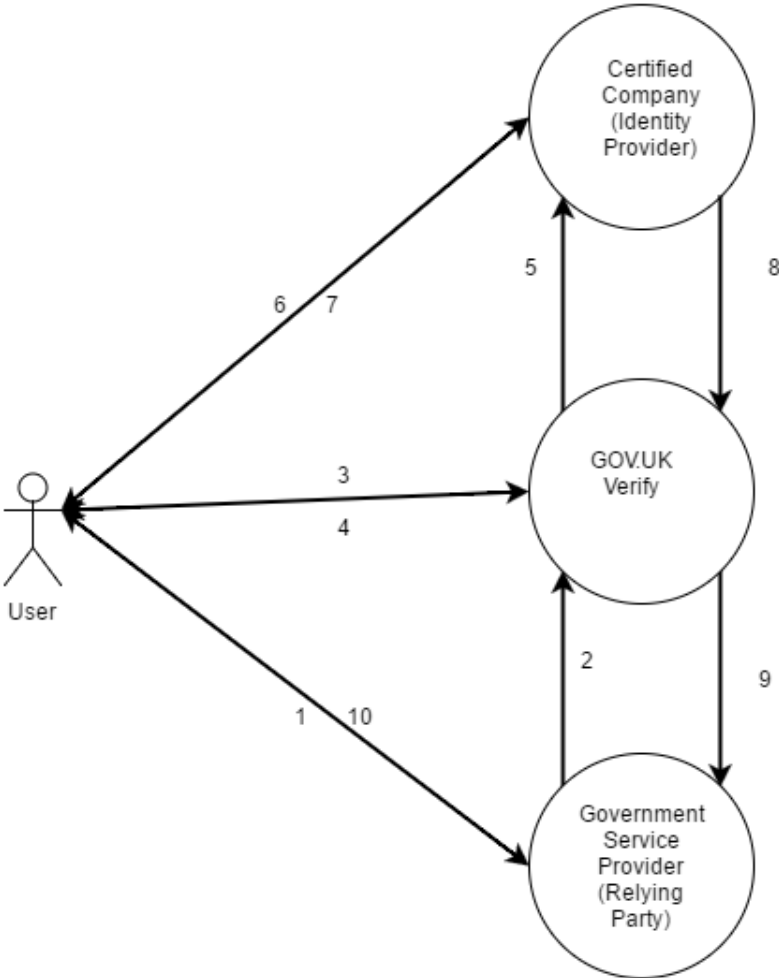
 <a href="#">Select Barclays</a>	 <a href="#">Select Royal Mail</a>	 <a href="#">Select Post Office</a>
 <a href="#">Select CitizenSafe</a>	 <a href="#">Select Experian</a>	 <a href="#">Select Digidentity</a>
 <a href="#">Select Secureidentity</a>		



Choosing Experian, returns the user to the Experian account sign in. Then, following the appropriate account security check (i.e., authentication using M-Pin), the user is immediately redirected to the requested online government service.

Figure 15 presents these data flows diagrammatically, starting with the user connecting to the Government service provider (1), being redirected to Verify (2) where they are asked to either pick a certified company to obtain a Verify'd identity from or to choose a certified company they already have a Verify'd identity account with (3, 4). The user is then redirected to the certified company (5) and there either undertakes the identity proofing and verification checks (6, 7) or authenticates themselves (6, 7). Once this is done, the user is returned to Verify (8) and, from there, on to the Government service provider (9) and thereafter the Government service provider interacts directly with the user (10).

**Figure 15. Data flows in Verify**



## **Understanding the Socio-political Context of Verify**

Although there is an ongoing academic debate about the extent to which human values may shape the technical design of systems and architectures (Winner 1980; Woolgar and Cooper 1999), the socio-political context around the scrapping of the previous identity cards scheme resulted in the development of the Verify model. A fuller description of this historical context is available in Appendix 2: Historical background to Verify.

In particular, Verify emerged as a replacement identity infrastructure following the scrapping of the previous government's controversial scheme for biometric identity cards based around a centralised National Identity Register (Whitley 2014). Politically, the coalition government of 2010 eschewed any notion of a centralised identity database or anything that might be seen as a proxy National Identity Register.

The Verify model brought together a number of existing themes. The first of these was the focus on citizen, rather than government, needs that had been highlighted by the report written by Sir James Crosby (2008).

This user-centric thinking developed alongside work by CESG (now the National Cyber Security Centre (NCSC)), the Information Security Arm of GCHQ (NCSC 2018), who issued a two-part report on the requirements for the secure delivery of online public services (RSDOPS). This guidance, now officially released as Good Practice Guide (GPG) 43 (GOV.UK 2012), takes a transactional viewpoint “as a way of describing and reasoning about information risk. This approach takes account of the overall business function and its distributed service model.” It is concerned with “ensuring security of a transaction end to end and therefore takes account of not just technical security aspects but additionally the need to ensure security of the business processes and sometimes, complex stakeholder relationships that support the provision of an online service.”

The third key factor relates to privacy concerns that were mentioned by Crosby and RSDOPS and were a major factor in the political decision to scrap the identity cards scheme.

Finally, responsibility for the development of the alternative identity policy for the UK was removed from the Identity and Passport Service (a division of the Home Office (interior ministry)) and brought to the Cabinet Office, the central department responsible for coordinating the delivery of government objectives. In particular, responsibility for identity policy was located within the Government Digital Services (GDS), formed in April 2011 to deliver the Government's “digital by default” strategy.

### **The Crosby Report and a Focus on User Needs**

In 2006, Sir James Crosby was appointed by the then Chancellor of the Exchequer, Gordon Brown, to lead a “public private forum on identity” (Brown 2006). His report was issued on 6 March 2008 (Sir James Crosby 2008), alongside the six-monthly report on the likely costs of the identity cards scheme (the so-called section 37 reports).

In his report, Crosby chose to differentiate between *identity management* which “is designed to benefit the holder of the information” and *identity assurance*, which “is focused on bringing benefits to the consumer,” arguing that the distinction between the two is “fundamental” (2008, para. 1.6). “As a result,” he continued, “although the technology employed to achieve [identity] assurance and management may be similar, the end design of the system is likely to be very different. An [identity] assurance scheme built primarily to deliver high levels of assurance for consumers will address issues, such as the amount and type of data stored and the degree to which this information is shared, differently to one inspired mainly by the needs of its owners” (2008, para. 1.7).

Before it was rebranded as GOV.UK Verify, identity policy development within GDS adopted Crosby’s preferred nomenclature and was known as the Identity Assurance programme.

### **RSDOPS and a Risk–Based Transactional Perspective**

CESG’s RSDOPS guidance presents a six stage process that “that allows public Service Providers to better understand what is needed from a security perspective to support delivery of an online service” (GOV.UK 2012, para. 14). The outputs from the process are intended “to open a discussion on the security problem and to develop a shared understanding of its implications” and “will assist Information Risk Owners in reaching an understanding of the information risk implications of their business decisions and satisfy themselves that the security response is proportionate and fairly represents the concerns and expectations of the business and the customers for the service” (2012, paras. 17–18).

As part of the risk–based and transactional perspective, the guidance indicates that there are different (levels of) requirements for personal registration (“the act of establishing the identity of an individual as a condition for issuing credentials that can be used subsequently to reaffirm that identity”) including a base level where “the real identity of the individual is not relevant to the service,” through increasing levels of assurance: “asserted,” “tested,” and “verified.” At this top level, “the user claims a real identity and the claimed identity is subject to rigorous testing to independently verify the individual’s identity and presence. The independent evidence of identity might be cited in support of criminal proceedings” (2012, p. 25).

This graduated approach provides an alternative perspective to the “gold standard of identity” approach found in the previous identity cards scheme and led to the development of Good Practice Guide 45 on identity proofing and verification (GOV.UK 2018a) that explicitly introduces levels of assurance.

A key feature of GPG 45 is its formalisation of levels of assurance. In the first instance, a Verify’d identity is one which has been verified to Level of Assurance 2 (LoA2) although there are plans to extend the service by offering identities that have only been verified to LoA1 as well (GOV.UK Verify 2017a).

## **Identity Assurance Principles and the Privacy and Consumer Advisory Group**

In order to properly address the privacy and consumer concerns around identity assurance identified by Sir James Crosby, in 2011 the Cabinet Office created the Privacy and Consumer Advisory Group (PCAG) (GOV.UK Verify 2017b) which held its first meeting on 2 August 2011. According to its terms of reference (GOV.UK Verify 2015a), “PCAG is a forum that provides an independent view on issues involving privacy and wider consumer concerns” on a “variety of initiatives with implications for individuals regarding the use of their personal data and their privacy.” These range from “the identity assurance programme to the use of patient records in the NHS, to interdepartmental data sharing and anti–fraud initiatives” (GOV.UK Verify 2015a). Membership of the group includes academics, privacy advocates, consumer groups and others with specialist expertise in the area. It meets monthly and the minutes of its meeting are published by GDS (GOV.UK Verify 2017b). Alongside regular engagement with the programme, it developed the “Identity Assurance principles” (GOV.UK Verify 2014a).

A first draft of these Identity Assurance principles was issued for public consultation and feedback in April 2012 and beta released in June 2013. These set out, in detail, how GOV.UK Verify could be configured to meet the privacy and consumer expectations of its users. A second version of the document was released in September 2014 incorporating feedback received during a consultation on the beta version published in June 2013 (GOV.UK Verify 2014a).

## **GDS and the Delivery of Government Digital Services**

Verify is a part of GDS and GDS is itself part of the Cabinet Office and the Efficiency and Reform Group. It is responsible for the delivery of Government as a platform (Brown et al. 2017), an approach that will “deliver cross–government programmes that will improve public services and deliver efficiencies including. . . the development of the GOV.UK Verify programme to enable individuals to prove their identity online and to access government services securely and safely” (GOV.UK 2015a, para. 11.20), see also (GOV.UK 2017a; GDS 2017a; GOV.UK 2017b).

GDS is creating “a set of shared components, service designs, platforms, data and hosting, that every government service can use. This frees up teams to spend their time designing user–centric services rather than starting from scratch, so services become easier to create and cheaper to run” (GOV.UK 2018b).

GDS has created a digital service standard (GDS 2018a) which includes 18 criteria to help government create and run good digital services. Important criteria for Verify include “(1) Understand user needs,” “(2) Do ongoing user research,” “(4) Use agile methods,” and “(5) Iterate and improve frequently.” As such, the development approach runs counter to more traditional “waterfall models” of systems development which are sequential and non–iterative. Waterfall models have, arguably, been the cause of widespread system failures in UK Government IT (Institute for Government 2011; Public Administration Select Committee 2011).

One consequence of the digital service standard is that all GDS projects, including Verify, pass through a series of phases: Discovery, Alpha and Beta before becoming live services that provide a “fully resilient service to all end users” and meet “all security and performance standards” (GDS 2018b).

## **B. How Verify Works**

### **Verify’s Approach to Identity Proofing and Verification**

Verify is not intended to provide a “gold standard of identification” that relies on a definitive register of personal data, rather it operates in a context that includes a number of different levels of assurance (GOV.UK 2018a). The current approach is based on four levels of assurance in the identity proofing and verification process. Each level provides an increasing level of confidence that the applicant’s claimed identity is their real identity (2018a, chap. 2). Currently, Government services that use Verify operate at Level of Assurance 2 although there are plans to extend Verify to services that operate at Level of Assurance 1 (GOV.UK Verify 2017a).

**Level of Assurance (LoA) 1 Identity:** “At Level 1 there is no requirement for the identity of the Applicant to be proven. The Applicant has provided an Identifier that can be used to confirm an individual as the Applicant. The Identifier has been checked to ensure that it is in the possession and/or control of the Applicant.”

**LoA2 Identity:** “A Level 2 Identity is a Claimed Identity with evidence that supports the real-world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of civil proceedings.”

**LoA3 Identity:** “A Level 3 Identity is a Claimed Identity with evidence that supports the real-world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of criminal proceedings.”

**LoA4 Identity:** “A Level 4 Identity is a Level 3 Identity that is required to provide further evidence and is subjected to additional and specific processes, including the use of biometrics, to further protect the identity from impersonation or fabrication. This is intended for those persons who may be in a position of trust or situations where compromise could represent a danger to life.”

The identity proofing process “should enable a legitimate individual to prove their identity in a straightforward manner whilst creating significant barriers to those trying to claim to be somebody they are not.” The individual presents evidence to support their identity claims and the evidence shall be confirmed as being “Valid and/or Genuine and belonging to the individual.” This includes checking whether the identity exists in the real world and, importantly, the “breadth and depth of evidence and checking required shall differ

depending on the level of assurance needed in that the identity is real and belongs to the individual.”

In particular, this means that the identity proofing process does not rely on possession of a single breeder document, such as a birth certificate or passport (Berghel 2006; Collings 2008). Instead, the individual provides access to an “identity evidence package” (2018a, chap. 3) that includes evidence that can be categorised into three broad categories: *Citizen*, *Money* and *Living* (GOV.UK Verify 2014b). Consideration of the identity evidence package will normally include reviewing the activity history of the evidence (i.e., existence in the real world over a period of time) and active counter–fraud checks to ensure it is not a known fraudulent identity.

There are five different headings for evaluating and scoring different kinds of identity evidence (2018a, chap. 5), see table 1.

**Table 1. Identity proofing and verification elements and scores**

Element		Score				
		0	1	2	3	4
A	Strength of identity evidence					
B	Outcome of attempts to validate the identity evidence					
C	Outcome of the identity verification					
D	Outcome of active counter–fraud checks					
E	Strength of activity history evidence					

**Element A** is consideration of the strength of the identity evidence. A score of 1 is given if the issuing source performed no identity checking itself, but the issuing process can be reasonably assumed to have been delivered into the possession of an individual and the evidence contains at least one unique reference number or contains a photograph/image/biometric of the person to whom it relates.

A score of 3 is given if the identity evidence confirmed the applicant’s identity in a manner that complies with the identity checking requirements that satisfy Money Laundering regulations. The highest score (4) is awarded when the issuing source for the identity evidence visually identified the applicant and performed further checks to confirm the existence of that identity.

**Element B** is the outcome of attempts to validate the identity evidence. A score of 0 means that the validation attempt was unsuccessful, a score of 1 means that all personal details from the identity evidence have been confirmed as valid by comparison with information held/published by the issuing/authoritative source. A score of 2 requires both the personal details and identity evidence to be confirmed as valid, or the issued identity evidence has been confirmed as genuine by trained personnel using their skill and appropriate equipment and who confirmed the integrity of the physical security features or the issued identity evidence has been confirmed as genuine by confirmation of the integrity of the

cryptographic security features. A score of 3 is given if the personal details and identity evidence are confirmed by the source and the integrity of credential is confirmed whilst a score of 4 tightens the requirements further.

**Element C** relates to the outcome of the identity verification. A score of 0 means that it was not possible to confirm that the applicant is the owner of the claimed identity, a score of 1 means the applicant has been confirmed as having access to the identity evidence provided to support the claimed identity. A level 2 score can be achieved by static or dynamic “knowledge-based verification” or physical or biometric comparison to the strongest piece of identity evidence provided whilst higher scores place further restrictions on this process.

**Element D** relates to active counter-fraud checks. Here a score of 0 indicates that the applicant is suspected of being, or known to be, fraudulent. A score of 1 indicates an absence of evidence that the identifier is being used for fraudulent activity. Higher scores move from reliable independent sources confirming no fraudulent activity to using sources private to the Government to check that there is no evidence that the applicant is fraudulent.

It is helpful to note that whilst there are strong operational reasons for allowing known fraudulent identities to be created, so that they can be tracked through the system and thus result in criminal prosecutions and intelligence about the weaknesses in government systems, the Verify identity proofing and verification process explicitly only provides verified identities that are not known to be fraudulent, thus closing down this particular avenue of anti-fraud activity.

**Element E** relates to the activity history of the claimed identity. Here a score of 0 means that it was not possible to demonstrate the required activity history, a score of 1 means that it was not necessary to demonstrate the required activity history, a score of 2 relates to activity of at least 180 days (6 months), a score of 3 relates to an activity history of 405 days (just over a year) and a score of 4 for a claimed identity with an activity history of at least 1080 days (3 years).

In order to satisfy the current requirements for a Verify'd identity (i.e., one that meets LoA2), the identity evidence package must contain (2018a, chap. 6):

Identity Evidence that as a minimum meets one of following profiles: 1 piece of identity evidence with a score of 3 and 1 piece of identity evidence with a score of 2 (known as an identity evidence profile of 3:2) or 3 pieces of identity evidence with a score of 2 (known as an identity evidence profile of 2:2:2). Each piece of identity evidence must be validated with a process that is able to achieve a score that matches the identity evidence profile; i.e. where the profile is 3:2 the validation processes must be able to also achieve scores of 3:2 respectively. Additionally, as a minimum the applicant must be verified as being the owner of the claimed identity by a process that is able to achieve a score of 2 for verification. In terms of counter-fraud checks the claimed identity must be subjected to a counter-fraud check by a process that is able to achieve a score of 2 as a minimum. Finally, as a

minimum, the activity event package must be able to achieve a score of 2 for the activity history of the claimed identity (GOV.UK 2018a, chap. 6).

GPG 45 also gives examples of various forms of identity evidence, their associated levels (Element A) and which aspect (Citizen, Money, Living) they correspond to (the full illustrative list is available in 2018a, chap. Annex A):

**Table 2. Examples of various forms of identity evidence**

Identity Evidence	Level	Citizen	Money	Living
Fixed line telephone account	1			X
Police bail sheet	1	X		
Firearm certificate	2	X		X
HMG issued Statelessness person document	2	X		X
Unsecured personal loan account	2		X	X
An education certificate from a well-recognised higher education institution	2			X
Mobile telephone contract account	2		X	X
Passports that comply with ICAO 9303 (Machine Readable Travel Documents)	3	X		
Bank savings account	3		X	
Mortgage account	3		X	X
Non-bank credit account (including credit/store/charge cards)	3		X	
EEA/EU full driving licences that comply with European Directive 2006/126/EC	3	X		X
Biometric passports that comply with ICAO 9303 (e-passports) and implement basic or enhanced access control (e.g., UK/EEA/EU/US/AU/NZ/CN)	4	X		
EEA/EU government-issued identity cards that comply with Council Regulation (EC) No 2252/2004 that contain a biometric	4	X		
UK Biometric Residence Permit (BRP)	4	X		
NHS staff card containing a biometric	4			X



The Guide also provides illustrative examples of activity events (2018a, chap. Annex E).

**Table 3. Illustrative examples of activity events**

Citizen	Money	Living
Electoral roll entry	Repayments on an unsecured personal loan account (excluding pay day loans)	Land registry entry
	Repayments and transactions on a non-bank credit account (credit card)	National pupil database entry
	Debits and credits on a retail bank/credit union/building society current account	Post on internet/social media site
	Repayments on a student loan account	Repayments on a secured loan account
	Repayments and transactions on a bank credit account (credit card)	Repayments on a mortgage account
	Debits and credits on a savings account	Repayments on a gas account
	Repayments on a buy to let mortgage account	Repayments on an electricity account

Identity proofing and verification does not end once an identity has been Verify'd. Instead, there is a requirement for periodic checks after the registration has taken place as well as checks "every time a user signs into a service" (GOV.UK Verify 2014b). These checks include things like repeating the counter-fraud check periodically or ensuring that verification of an address is not older than a set number of days.

### **Identity Proofing and Verification in Practice**

The kind of identity proofing and verification model used in Verify is a natural consequence of the RSDOPS inspired risk-based approach to identity claims and standards. The Verify implementation, however, has the additional distinguishing feature in that the government does not act as an identity provider undertaking the identity proofing and verification activities. Instead, it only acts as a service provider (relying party) that relies on Verify'd identities.

Figure 16. The traditional checking model when government acts as the identity provider

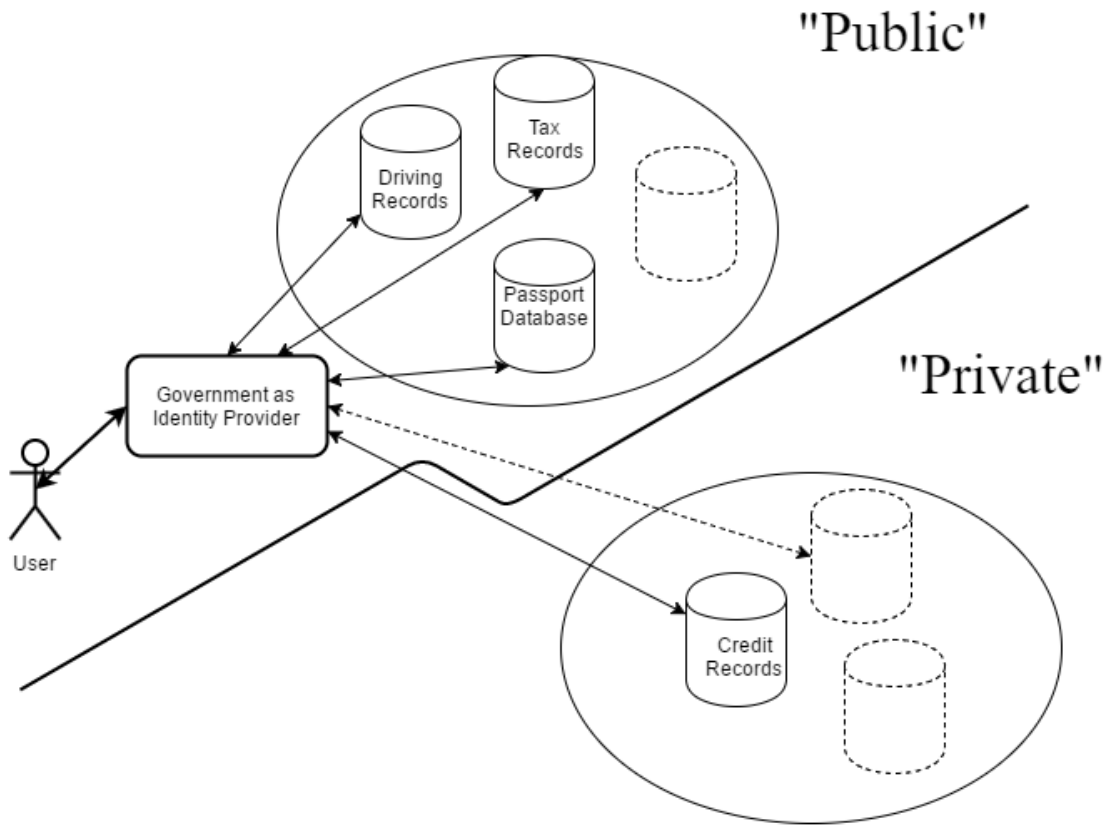


Figure 17. Identity checking in Verify

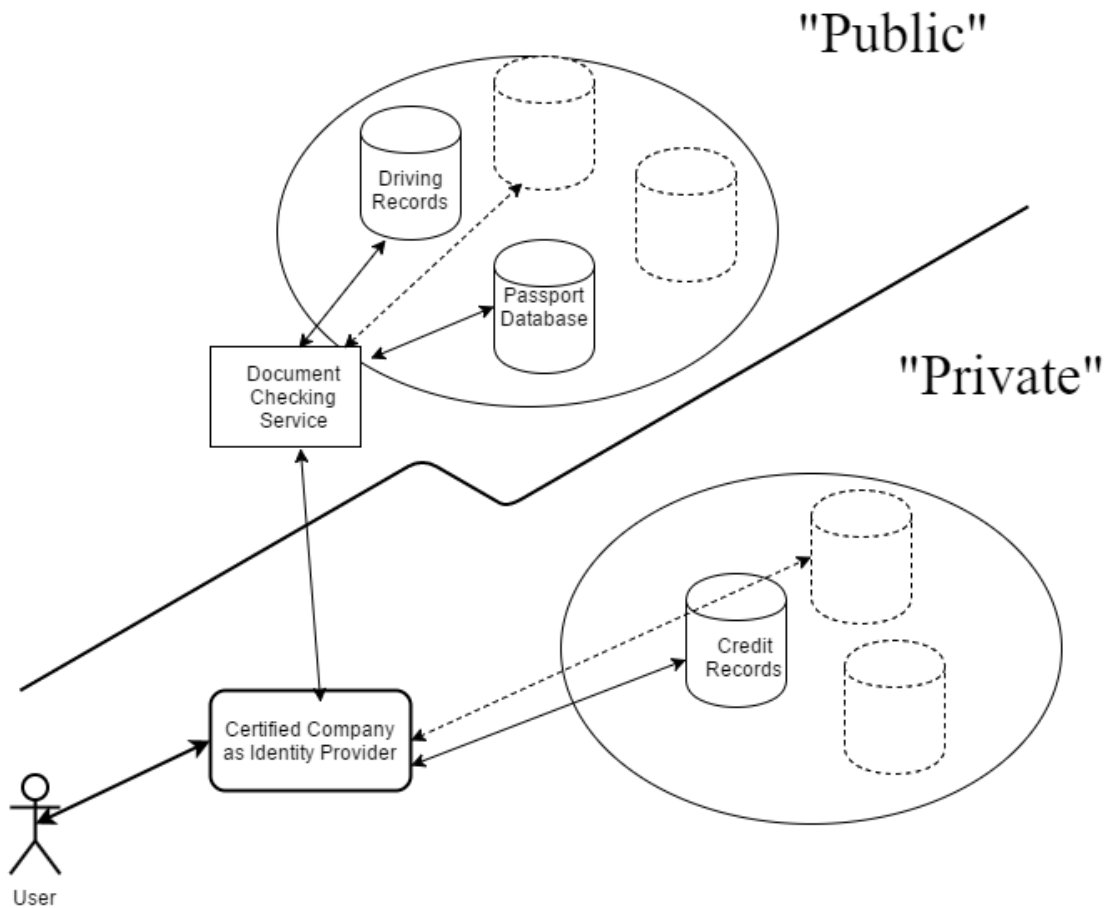


Figure 16 and figure 17 illustrate the conceptual difference between existing models of identity checking and the Verify model. The existing government as identity provider approach increasingly already relies on a mix of public data sets and private sector data sets (Lips et al. 2009; Lips 2013). In the Verify model, the certified companies are able to use the Document Checking Service to confirm the Driving Licence and Passport information provided by the user (GOV.UK Verify 2014). The checking service allows the certified companies to check user data against a subset of the data held about individuals by the government. The certified companies are also able to bring in novel data sources for identity proofing and verification purposes.

### Certified Identity Providers

The role of identity providers is undertaken by a range of commercial (private sector) organisations. At the time of writing, seven companies are certified identity providers providing services for Verify. That is, they both successfully participated in the framework agreement procurement exercise and completed the accreditation and onboarding process to become live identity providers and continued to satisfy the requirements:

- Barclays
- CitizenSafe
- Digidentity
- Experian
- Post Office
- Royal Mail
- SecureIdentity

The governance processes for these private companies offering services to government are discussed below, but as they need to implement identity proofing and verification to the level of assurance required by government service providers (i.e., currently LoA2), the Verify team has issued an “operations manual” that provides guidance on how the identity providers should implement the identity proofing and verification activities (GOV.UK Verify 2014c). This public version of the report is redacted due to operational security requirements.

### **Identity Proofing and Verification (IPV) Operations Manual**

The guidance includes details of how to check whether physical identity evidence (e.g., a passport) is genuine and identifies both the kinds of physical equipment needed to check them (e.g., ultraviolet light to highlight features of key passport pages (HM Passport Office 2011)) as well as the kinds of training required to test the genuineness of these documents to the different standards of evidence described above. It also includes details of the identifier formats for common identifiers, such as driving licence numbers, bank card numbers etc. to provide basic, “checksum” type checks to ensure the identifiers are valid numbers.

Amongst the counter–fraud capabilities discussed in the guide are checking whether the claimed identity has been subject to identity theft regardless of whether it was successful or not, checking whether the claimed identity is deceased and checking whether the address history of the claimed identity is consistent with the declaration by the customer.

Matching the identity evidence package against information held by external data aggregators (including credit reference agencies) includes guidance on how to match against known synonyms, such as Bill and William as well as variations in how addresses are stored.

It is important to recognise that “simply because the identity provider has discovered a contra indicator that is associated with a fraud identifier does not in itself imply that there is an actual fraud only that there is a risk of fraud. In order to determine that there are reasonable grounds to suspect that a fraud may be taking place the fraud identifier shall need to be confirmed by following the mitigating actions associated with the contra indicator. Where the identity provider does not have the capability to perform the mitigating action then they cannot apply the ‘pass’ score and by definition the fraud identifier cannot be ‘confirmed’” (2014c, paras. 108–109).

A key goal for Verify is to maximise its demographic coverage (i.e., the proportion of the UK population who can verify their identity using GOV.UK Verify). Gaps in the coverage

can lead to high profile failures that cause embarrassment for the service and, more importantly, frustration from service users who are unable to access important government services online and are key technical delivery priorities (GOV.UK Verify 2016c). Verify's attempts to understand and improve demographic coverage are discussed in more detail below.

Perhaps the highest profile example of a gap in demographic coverage arose in November 2014 where many farmers were unable to register for the Department of Food and Rural Affairs (DEFRA) Common Agricultural Policy information service (Fiveash 2014). With hindsight, it is understandable that this community, who are infrequent international travellers and who may eschew mortgages and other forms of debt, had many problems verifying their identity using the identity evidence packages available at that time. It has been suggested that one form of possible identity evidence that is held by many farmers is a firearms certificate (listed in GPG 45 as level 2 identity evidence for citizen and living categories). Unfortunately, information about who holds a firearms certificate is not available in a checkable register and so none of the available identity providers would be able to perform identity checks against that particular identity source.

### **Innovation in Identity Verification**

One of the benefits of using private sector identity providers operating in a competitive marketplace is that there is a strong incentive for the identity providers to offer as wide a range of possible identity checking services as possible as they are paid on the basis of successful enrolments (e.g., Merrett 2016a). For example, young people, particularly those aged 16–24, are less likely to have an established identity footprint that could be used as part of the identity evidence package (GOV.UK Verify 2015b) and, importantly, would have limited activity history associated with any evidence they did possess (even their mobile phone contracts would often have been taken out by their parents) (GOV.UK Verify 2016d).

An Open Identity eXchange UK (OIXUK) discovery project with the JustGiving website, however, identifies a number of areas where alternative data sources could be used to support a claimed identity to LoA2 (OIXUK 2016a). According to the OIXUK report, JustGiving is a tech-for-good company that facilitates donations and fundraising for charities. In 2001, JustGiving launched as the first UK online fundraising platform and has grown to include a database of users which covers 89 percent of UK postcodes. This translates to over 6 million active users in the previous 12 months (2015). Importantly, each user that transacts has achieved a certain standard of verification, with a proportion achieving a greater degree of verification. JustGiving transactions can be used in the knowledge-based verification stage by asking the individual which was the last charity they supported or who they have supported via the site in an analogous manner to which an individual might identify which bank account they most recently opened or which cards they have recently used for a particular purchase. Other forms of online history evidence have also been explored (GOV.UK Verify 2016e; Veridu 2016) as well as alternative approaches to gathering identity evidence including data aggregators using micro sources of data (OIXUK 2017a).

Alongside this work, other forms “end–point innovation” include the ability to take photographs of identity documents (such as passports and driving licences) to enable “physical” checks of the document alongside data checks. These photographs are handled using secure in–app image processing techniques, rather than using the device’s camera app which would store the document image less securely on the device. Additionally, some identity providers are able to undertake back–end checks against financial evidence by undertaking a £0.00 transaction with an individual’s account (this goes one step beyond the kind of nominal transaction (£0.10) introduced by services such as PayPal to confirm account ownership).

Enhancing the user experience is a key driver for some of these innovations and searches for alternative means of identity proofing and verification as there is growing evidence (particularly in the form of analysis of incomplete initial registration journeys (cf OIXUK 2017b)) that users do not like knowledge-based verification type questions such as “What was the amount of your last month credit card bill?” or “What was the period of your most recent mortgage application”?

It is also important to recognise that although Verify is a digital only service, the Government’s Digital by Default strategy includes assisted digital, whereby those service users who are unable, for whatever reason, to use digital services can use alternative means (including face-to-face and telephone-based services) (GOV.UK Verify 2016f) and using support workers to assist people through the Verify user journey (GOV.UK Verify 2017c).

When stating that the identity proofing process “should enable a legitimate individual to prove their identity in a straightforward manner” GPG 45 explicitly does not make any assumptions about non–UK nationals obtaining Verify’d identities. Instead, the question simply becomes one of whether they have sufficient identity evidence (that can be checked) to support a LoA2 identity. Whilst it is reasonable to expect that checking any (UK) state issued documents held by UK nationals will be included in the default offering of the certified companies, the companies are increasingly able to check evidence from outside the UK as well, including passports and other official documents issued by foreign countries (GOV.UK Verify 2016d).

A related concern surrounds the demographic profile of individuals who might find it more difficult to provide sufficient identity evidence, such as younger (or older) people, those who are unemployed etc. Careful modelling, however, suggests that the problem is primarily one of combinations of evidence, perhaps unsurprising given the different kinds of evidence that Verify uses.

Simply relying on coverage of data available in individual data sets is insufficient. For example, with 78 percent of adults aged 18 and over having a driving licence and 80 percent of England and Wales residents having a passport this does not necessarily mean that 95.6 percent of people have either a driving licence or a passport as the correlations between owning one document and the other are unknown (GOV.UK Verify 2016g).

An online tool that allows one to visualise the combination process and explore the underlying data is available at Dale (2016) and this data can be supplemented by survey data provided by the Office of National Statistics (ONS). This enhanced data set now suggests that at least 79 percent of the adult population (rising to 88 percent if they are in employment), have enough evidence to successfully verify their identity (GOV.UK Verify 2016h). This enhanced data set can be explored at Dale (2017).

More generally, this proactive approach seeks to identify those characteristics that might lead, either directly or indirectly, to systemic gaps in identity evidence that might preclude certain parts of society from being able to obtain a Verify'd identity. This information can then be used by the certified companies to integrate alternative data sources as part of the service they offer.

### **Automated Identity Checks?**

As Verify offers a digital-only identity service, ideally, many of the basic identity proofing and verification checks should be able to be made electronically by the identity provider (using real-time access to data sources such as the Document Checking Service via Application Programming Interfaces (APIs)). In practice, despite the UK's strong position in the open data field, many of the possible data sources are not (yet) available for such automated checking via APIs and, instead, manual back office checks need to be undertaken. Additionally, the "physical" checks of identity documents (based on photographs) are done manually, although again, identity providers are moving to offer such checks on a 24/7 rather than "office hours" basis.

Other problems with automated identity checks have arisen in the context of married (female) users who have some identity evidence using their married name and others, including professional-based information, in their maiden name. In some cases, the split between these two different forms of identity evidence mean that it is not possible to achieve a sufficient score for a LoA2 Verify'd identity using either name.

An ongoing challenge for all the data sources used in identity proofing and verification is the quality of the underlying data. Thus, for example, if there are data entry errors in the database that the identity evidence is being checked against (at one time the DVLA driving licence database reported errors in up to 30 percent of all records (BBC News 2005; Blackhurst 1993; Whitley 1994)), or if the data is not up-to-date (for example, not notifying the organisation of a change of address) the identity proofing and verification will fail.

One natural consequence being considered is that once an identity has been Verify'd, this Verify'd identity could then be used to provide the authorisation to update the checking databases with the new identity data, for example with a new, confirmed address.

### **Data Minimisation in Identity Proofing and Verification**

A key design choice in the Verify model is that a minimal amount of data is stored as part of the identity proofing and verification process. This is considered best practice in both data protection and digital identity practice (Nyst et al. 2016). Thus, although a user may provide

passport details as part of the initial registration process and this data are used to confirm that the passport is genuine, has not been recalled etc., the verification process returns a simple Yes/No response. This response, plus the date upon which it was received is stored by the identity provider. Additionally, the identity provider is obliged to retain the original information provided by the user (e.g., passport number) for audit purposes only. This audit requirement is driven by regulatory requirements and the information is needed in case the legitimacy of the account activation is questioned in the future. This non-operational, audit-only data can be stored securely in a separate system.

### **Innovation in Identity Authentication**

Identity providers are also innovating in terms of the kinds of authentication services they can offer. Alongside the use of one-time-passcodes sent via SMS identity providers are introducing apps that can be installed on the user's smart phone or tablet and thus provide an alternative, out of band, authentication method whereby the user authenticates themselves via the app (Ashford 2015). Such alternative approaches, provided that they satisfy the requirements specified in GPG 44, may address growing concerns about the use, for example, of SMS for authentication (Chirgwin 2016; Pauli 2016).

Innovation around identity authentication can also include privacy-friendly fraud monitoring, for example, searching for browser hijacks and man-in-the-middle attacks (GOV.UK Verify 2016i).

### **Using a Verify'd Identity to Access Government Services**

As indicated in the user journey presented earlier, once an individual has a Verify'd identity this can be used to access online government services. As the user journey illustrates, this begins with the user seeking to access an online government service, for example, completing a self-assessment tax return. Using Verify, users are first redirected to the "Hub" and then choose (one of) the identity providers that they have a Verify'd identity with and authenticate themselves with that identity provider, see Figure 15.

The Hub is a key privacy enhancing feature of the Verify model. It acts as an intermediary between the identity provider and the service provider and helps ensure that the identity provider cannot know which service provider the user is using and hence exploit this information for commercial gain (cf Gal 2016; Zuboff 2015). All that the identity provider can see is that a user, who has successfully authenticated with the identity provider, is accessing a government service.

Government service providers, in the same way, only receive identity data from the Hub and, whilst they can be assured that the identity has been Verify'd to the specified level of assurance, they cannot know (or specify) which identity provider has been used.

The Hub model is not without its own privacy concerns (Brandão et al. 2015) but the Verify team is working with one of that report's authors to address them. In addition, one of the



authors of that report has become a member of the Privacy and Consumer Advisory Group (GOV.UK Verify 2015c).

The identity data that passes through the Hub is a small “matching data set” (previously known as the minimal data set). It is sent, in encrypted form, from the identity provider to the Hub. The Hub then forwards the matching data set (again encrypted) to a matching service operated for the government service provider (the relying party). The matching service, as its name suggests, matches the matching data set against the records held by the service provider, identifying the unique service records associated with the user. Thereafter the user interacts directly with the service provider’s systems and their own records. If initiating a new service, the matching data can, with the user’s consent, be used to populate key fields with the new service (GOV.UK Verify 2017d, sec. 3.3.3.1).

Thus, if I use Verify to complete a self–assessment tax return with HM Revenue and Customs, the matching service uses my associated matching data set to find my tax record (and its associated tax reference number). The tax reference number is then used as the database key for interactions with the tax system. If I use Verify to check my state pension (with the Department of Work and Pensions) the matching service uses my matching data set to find my state pension record (and its associated national insurance number). The national insurance number is then used as the database key for interactions with the pension system. If I use Verify to claim a redundancy payment, I can choose to use the data from the matching data set to set up my new account with the insolvency service.

The matching data set consists of full name, address, date of birth, history of attributes and the associated assertion of level of assurance. The matching data set also allows for an optional gender field, but identity providers are under no obligation to collect this data and the user is under no compulsion to provide it. Rather than offer different matching sets for different government services (which would involve the Hub knowing which service was being used, a potentially privacy sensitive choice), the same, standard matching data set is sent to any government service that is connected to Verify.

This means that much of the heavy work is undertaken, in fact, by the matching service and this is where the history of attributes becomes important. For example, a user may have a Verify’d identity based on their new address but be accessing a government service that has their old address on file. A simple version of the matching service would therefore report that the Verify’d identity could not be matched against the service provider’s records, whereas a check against the history of attributes (including earlier addresses) would allow the match to take place the user to access the service, perhaps also flagging that an out of date address is held by the service provider.

## **Paying for Verify**

The financial arrangements around Verify are an important feature of the programme. This section covers the three areas of funding, the costing of Verify’d identities and liability issues.

## Funding

In November 2015, the Government announced the Spending Review and Autumn Statement. This was a four-year plan to fix the public's finances. Part of the spending review included resourcing to cover the cost to government of the Verify service (GOV.UK 2015b).

This high-profile support for Verify built on the recognition that government needs a secure online identity service in order to create digital services around user needs that would allow users to securely transfer personal data in real time, reducing or avoiding manual processing costs. It was also based on a business case that emphasised that Verify would only require users prove their identity once to government, giving a consistent experience for users which will reduce failure and waste, provides a consistent level of security across government services and a consistent experience for users, rather than creating loopholes and fraud opportunities between different departmental approaches to identity assurance.

It also takes advantage of rapidly developing technology and capabilities in the private sector and is more capable of responding effectively to rapidly evolving threats, costs less per transaction compared with a single government identity provider or separate solutions for each department. Government pays once to verify a user's identity and then the user can use their account to interact with any online government service, so that as more services adopt GOV.UK Verify, the cost per transaction decreases (GOV.UK Verify 2015d). Recent press reports suggest that the business case predicted £71m of annual cost savings by 2020, with running costs of £37m (Glick 2017a).

The business case also highlighted how Verify was stimulating a new market of competing commercial suppliers, reducing price and constantly improving quality through ongoing competition, is intended to be scalable beyond central government at low marginal cost as well as being usable in the private sector where it can contribute to preventing fraud and stimulating innovation and efficiencies in the wider economy. It also noted that Verify is supported by privacy campaign groups and consumer experts which increases public trust and potential digital uptake. Finally, it noted that Verify enables departments to comply with the new European Regulation on electronic identification by 2018, at no additional cost to them as, by 2018, government services will have to accept strong identities assured by other EU member states (European Commission 2016; GOV.UK Verify 2015d).

It is important to recognise that “GOV.UK Verify is a piece of enabling infrastructure—it will enable departments to transform their services. Departments have already counted the value of their transformation plans, albeit that they depend partly on being able to adopt GOV.UK Verify. The Verify business case does not attempt to attribute a portion of those savings specifically to GOV.UK Verify—departments are responsible for delivering their transformation plans and realising the benefits from them” (GOV.UK Verify 2015d).

An alternative approach that the government could have adopted was to allow the development of department-by-department solutions, whereby individual departments “could develop solutions tailored to each of their services. Identity verification is a common component but there could be competing ways to solve this. In this option departments

would invest in building their own solutions which might be uniquely tailored to their requirements but across government as a whole will involve duplicating time, effort and money.” This is likely to include additional costs due to duplicated software build and maintenance costs, reduced government buying power when transacting with commercial suppliers and duplicated process costs of identity verification (e.g., if an average user uses two services from different departments their identity would have to be verified twice). Moreover, the user experience would be sub-optimal as users would have to maintain credentials for every department or service that they used. Press reports suggest that the GDS business case claimed a saving of £263m by avoiding departments spending money on developing their own identity systems and using Verify instead (Glick 2017a).

The final alternative would be to replace commercial identity providers with a central government identity verification service. As noted above, this option has significant political costs associated with it. Additionally this approach carries the risk that a single national identity provider would become a “honey pot”—single point of failure at a greater security risk from attacks and less resilient in the event of failure or attack (Leyden 2016a, 2016b, 2016c; Thomson 2015).

According to a 2017 report on digital transformation in government by the National Audit Office (NAO 2017) GDS received funding of £455 million in the 2015 Spending Review, covering expenditure for the four years from 2016–17. Of the £54 million increase in funding between 2015–16 and 2016–17, £43 million (80 percent) is ring-fenced for Verify, Government as a Platform and Common Technology Services with Verify taking the largest share of this increase. Additionally, the NAO reports that Verify is expected to become self-funding in 2018-19. This means that two-thirds of the £53 million decrease in GDS’s funding between 2017–18 and 2018–19 (£36 million) relates to removal of revenue programme funding for Verify (NAO 2017, fig. 3).

### **Costs**

Identity providers are paid each time a user successfully creates a Verify’d identity with them. The initial framework contracts covered the first 600,000 registrations (GOV.UK Verify 2014d). The overall cost of payments to certified companies is entirely driven by demand—they are paid each time they successfully verify an identity at LoA2. They were paid 5 percent of their LoA2 during a trial of “basic accounts” in 2015 (GOV.UK Verify 2015e). In order to incentivise identity providers to provide a good user experience and demographic coverage improvements, there is no payment for failed attempts to verify at LoA2.

Under the first framework, identity providers were paid the same price as an LoA2 verification for certain types of fraud detection. Under the new framework providers are required to absorb the cost of detecting fraud in their price per successful verification (GOV.UK Verify 2014e).

If an LoA2 account remains active after a year, the provider receives a second payment for ongoing maintenance of the account at the same level of assurance (this involves ongoing

evidence checks and fraud checks, for example). The payment is a percentage of their price for initial verification.

Importantly, there is no payment for login or per transaction. Government pays for each verification (or renewal) and then the account can be used an unlimited number of logins to an unlimited range of services. This means that adding more services reduces the cost per transaction—there is no marginal cost for each service that adopts GOV.UK Verify and there is no charge per transaction (Glick 2017a; GOV.UK Verify 2017d).

The GOV.UK Verify Code of Interoperability (2017d) explains how government service providers contribute to the running costs for Verify calculated on the basis of the number of users directed through GOV.UK Verify to the services. Departments must pay a maximum of £1.20 per User, per year to use GOV.UK Verify. The price paid will reduce if the cost of the programme is less than the income from departments however this is not expected to occur before 2020.

For example, if 100,000 unique Verify'd identities sign in with GOV.UK Verify to access DWP services in a year across 1 million transactions the DWP will pay £120,000. Similarly, a user who signs in with GOV.UK Verify for self-assessment 5 times, claims a tax refund twice and company car tax once in financial year 2016–17 will cost £1.20 for HMRC, not £9.60 (£1.20 x 8) (GOV.UK Verify 2017d, sec. 4).

### **Liability**

With government services acting as the relying party in identity transactions, questions of liability are significant. What is the liability/responsibility if an illegitimate identity transaction takes place? Such questions were never satisfactorily resolved with the previous UK Identity Cards Scheme as it was never clear what liability a government service provider would face if it relied on an official identity card (Whitley and Hosein 2010a). Would service provider liability be lower if they performed a biometric verification of the identity card compared to the liability associated with a visual inspection of the card?

Questions of liability are particularly important in the case of Verify where commercial organisations are acting as identity providers for government service providers. Here, the active governance measures described below enable a model whereby a properly functioning identity provider should not be held liable for issuing a Verify'd identity to LoA2 that, it turns out, should not have been issued unless the issuing process did not comply with the identity proofing and verification checks specified in GPG 45. If, however, identity proofing and verification checks as outlined in GPG 45 are coupled with secure credentials that satisfy GPG 44 to interact across the Hub that has the active risk management and use of cryptographic measures described above, then neither the identity provider nor the service provider can reasonably be held liable for issues that arise.

## **C. Building and Running Verify**

Alongside the GDS delivery approach that focuses on service design phases, Verify is also an active user of agile development methods (GOV.UK Verify 2016j). As Verify has grown, it

has been necessary to scale the agile methods to cope with the more complex governance arrangements for Verify.

The process of managing a programme of the complexity of Verify within the timescales and cycles of Parliament, spending reviews, new technological capabilities etc. is very complex (GOV.UK Verify 2016k) and requires careful management.

There are two main groups that manage the programme: the Senior Management Team and the Portfolio Group. The Senior Management Team meets on a weekly basis and is responsible for setting the vision for GOV.UK Verify, executive stakeholder management, managing programme budgets and team recruitment. The Senior Management Team includes all the people who lead teams in the programme and the weekly meeting includes each team reporting what's going on for them that week. This helps ensure everyone across the programme is aware of what's going on that week.

The Portfolio Group also meets weekly and is responsible for managing the project portfolio within the programme. This is commonly where individual projects report on their overall status, ask for additional resource and solve delivery issues. The Portfolio Group, along with the Risk Management Group, is responsible for managing programme assets, such as the risk/issues register, programme plan and programme roles and responsibilities.

In the spirit of agile, although teams are required to track their work and report status, Verify operates a “management by exception” principle so that projects can autonomously deliver as long as they stay within any confines (time, scope, budget) set by the Portfolio Group. This means that teams are free to choose the tools and the methods that best suit the task at hand (GOV.UK Verify 2016j).

Amongst the techniques that Verify uses are careful studies of user needs (GDS 2017b; GOV.UK Verify 2016l), including extensive A/B testing of various parts of the user experience (GOV.UK Verify 2016m), in fact it was recently reported that the 100<sup>th</sup> round of user experience research had been completed (GOV.UK Verify 2016n).

Verify has experimented with “mob programming” (GOV.UK Verify 2016o) whereby groups of between 3 and 7 people tackle one task at a time. During this process one person will “drive” the mouse and keyboard while the rest of the mob act as “navigators” by suggesting what source code needs to be produced (GDS 2016a). Mob programming was adopted in the expectation that it would help establish a shared and consistent understanding of how the new frontend to Verify would be built. Mob programming would also significantly reduce the chance of disruption to delivery when team members aren't available. Alongside mob programming, the Verify technical team has also undertaken various group learning activities (GOV.UK Verify 2016p).

The project has also started making part of Verify open source (GOV.UK Verify 2014f, 2016q) as well as making the user front end available in Welsh (GOV.UK Verify 2016r). At the same time, efforts have been made to tidy up the code base (GOV.UK Verify 2016m). More recently, it has begun providing sandbox environments for private sector users to

experiment with integrating their own services with Verify (GOV.UK Verify 2017e; OIXUK 2016b).

## **Integration with Online Government Services**

Unlike many digital identity systems in other countries, Verify has been designed from the ground up to provide access to online government services. As noted above, from a technological perspective, the key technological component that needs to be developed is based around the matching service that takes the Verify'd matching data set and links this to the relevant record in the online government service. However, the process of "onboarding" government services to work with Verify is much more than this.

To support this process, Verify has developed an "onboarding guide" for "government service providers wanting to learn about and integrate with GOV.UK Verify" (GOV.UK Verify 2016s). This involves a six-stage process that covers developing a proposal, needs analysis, planning, build and integration testing, production onboarding and beta stage.

The proposal stage involves determining whether the government service needs to use Verify and, if so, the level of assurance required. Attempts to use Verify for services that don't really need it tend to result in very poor completion rates for users who don't have an existing Verify account. It is important, therefore, that the proposal stage has a clear understanding of what integration with Verify would seek to achieve and the Verify team works closely with government services beginning to think about integration with Verify (GOV.UK Verify 2015f).

The needs assessment stage includes completing a full risk assessment of the digital service and agreeing the level of assurance required with the Service's Senior Information Risk Officer (SIRO). The service is also expected to review the quality of its own data assets, particularly in reference to the matching process. The detailed analysis also includes identification of any known peaks in usage of the service (such as particular deadlines for completion of particular transactions) and any distinct demographic features of the user population (highlighting any that might currently find it difficult to obtain a Verify'd identity) (GOV.UK Verify 2014g).

The planning stage includes consideration of any approvals needed to proceed with using Verify, the operational support model for the new service and the communications plan associated with integrating Verify with the service. Planning also includes delivery milestones (for alpha, beta and live) and the service's approach to (system) testing.

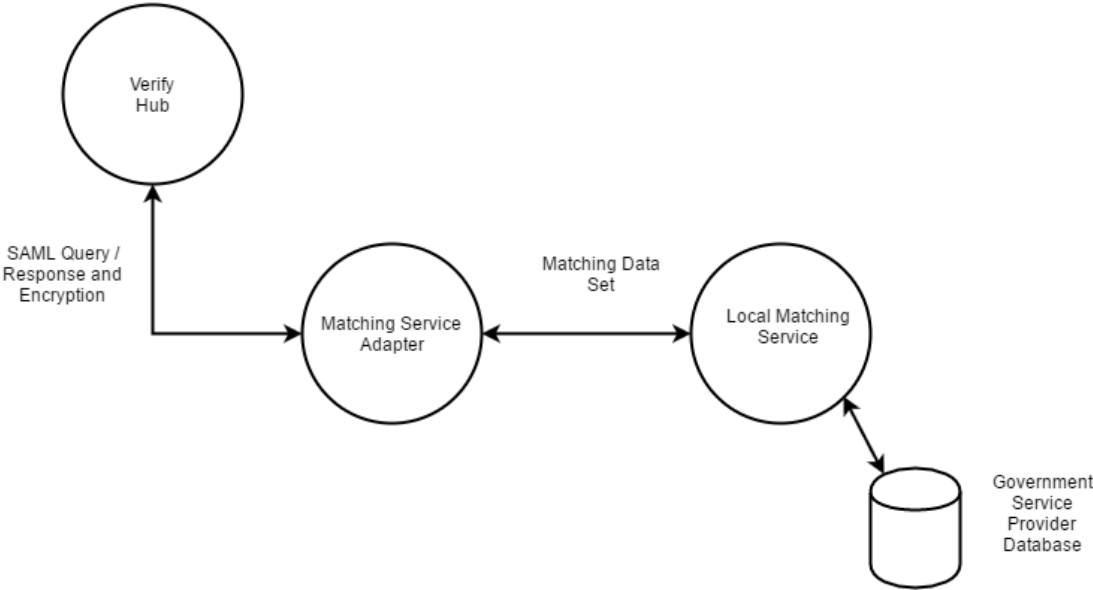
The build and integration testing approach involves building a service that sends SAML (Security Assertion Markup Language) authentication requests to, and receives SAML authentication responses from, the GOV.UK Verify Hub, building a local matching service that matches users' verified identities to the service's data sources, installing the matching service adapter provided by the GOV.UK Verify team and integrating it to the GOV.UK Verify Hub, running SAML compliance tests using the compliance tool, requesting public key infrastructure (PKI) test certificates for the GOV.UK Verify integration environment,

requesting access to the integration environment and running end-to-end testing of all the user journeys in the integration environment.

Following this work, the final stages involve switching on the service to become a beta and then live service. It is also important to recall that Verify only provides a Verify'd identity to specified levels of assurance. It does not determine eligibility or entitlement to any particular service. These decisions (and the internal processes associated with them) are the responsibility of the service provider (GOV.UK Verify 2017d).

Recognising that not all government services that want to use Verify will necessarily have the technical sophistication to build a matching service and integrate it with the Hub, Verify has broken the matching service into two components, the first is a matching service adapter that provide a SAML endpoint that links with the Hub as well as dealing with the message logic and cryptographic functionality. The adapter then interacts with a local matching service which uses data from the government service provider's internal databases. Hiding key aspects of the matching service in this way allows for easier integration of new government services into Verify, see figure 18.

**Figure 18. Matching service adapter as a black box interface to Verify**



## D. Verify's Governance Arrangements

### Openness and Transparency

A key feature of the GDS organisational culture is its attitude to learning, particularly learning about user needs. This means that, despite hiring top quality staff, it doesn't assume that it knows best. One consequence of this for the Verify team is that there is a

presumption of openness whereby key activities and processes are made available publicly enabling feedback and comment (GOV.UK Verify 2016t).

A simple example of this is the GDS performance dashboard for Verify (GOV.UK Verify 2018b). This provides real-time access to the overall performance of Verify, including listing the various live services that Verify is integrated with, the total account use (i.e., authentications to date), see figure 19 (live data is available at (GOV.UK Verify 2018c)) and account use by existing users per week, see figure 20 (live data available at (GOV.UK Verify 2018d)).

In contrast, under the previous identity cards scheme, the only way to know about the number of identity cards that had been issued was when a MP was given a Parliamentary written answer (for example, on 16 June 2010 (shortly after the Coalition government came into power), a written answer (Parliament 2010) revealed that “Approximately 14,000 identity cards had been issued to British citizens by 31 May 2010”). Nevertheless, publishing performance data in this way allows critics to point to issues with Verify (e.g., Moss 2016a).

Figure 19. Number of users (October 2014–July 2018)

## Number of users accessing services using GOV.UK Verify

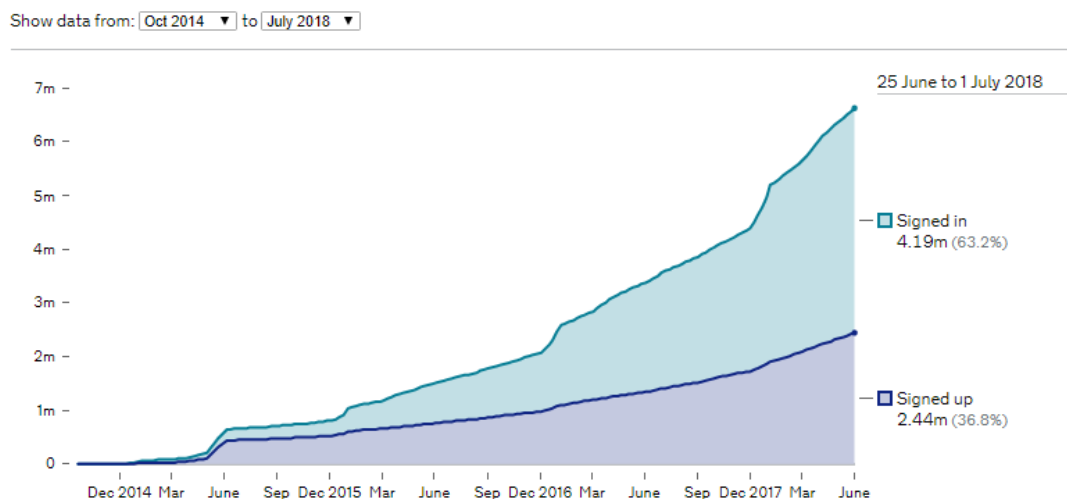




Figure 20. Existing users signing in each week (October 2014–July 2018)

## Existing users signing in each week



### Embedding Privacy in Verify

As noted above, the Privacy and Consumer Advisory Group (PCAG) was explicitly set up to ensure that the identity assurance programme “engages effectively with its stakeholders to incorporate issues related to privacy, trust and confidence during each of the design phases.” This was needed because “privacy and security are fundamental principles underpinning the new citizen–centric ID Assurance approach and unless the solution is trusted by users, they will not use it to safely log onto digital public services. The individual user must be able to control their own personal data and the ID Assurance Programme solution design is intended to this” (McCluggage 2011).

After being brought up to speed on the overall vision for what would become Verify as well as a detailed understanding of the proposed architecture, one of the first tasks for the group was the development of a set of principles to underpin the operation and roll out of the identity assurance scheme.

The principles are intended to “cover all aspects of the operation of a user–centric, identity assurance service which places the individual service–user in control of when and how they assert their identity” (GOV.UK Verify 2013a, sec. 2). The principles were developed using the expertise of the group and include considerations that are specific to the architecture of the system as well as current (and likely future) data protection laws including the General Data Protection Regulation (GDPR) and the principles behind them (OECD 1980; OPSI 1998). They draw on specialist guidance around identity, including Kim Cameron’s Laws of Identity (Cameron 2005) and best practice in consumer support, see also Nyst et al. (2016, chap. 9).

The draft principles were published for consultation in June 2013 and, following careful analysis of the responses to the consultation, a revised version (3.1) of the principles was published in September 2014. The high-level principles are explicitly presented using the first–person and active voice to reinforce the role of the citizen at the centre of the process. Now that Verify is a live service and there are plans to make it available beyond central

Government PCAG intends to review and possibly revise the principles, including providing further guidance on how to operationalise them.

Recent research reports that there was a high level of awareness of the identity assurance principles amongst key members of the UK identity industry, with 78 percent of respondents feeling that having a set of privacy principles was very important to a cross industry identity approach and a similar proportion feeling that the privacy principles were very relevant to their sector or organisations (OIXUK 2016c).

## **The Identity Assurance Principles**

### *User Control*

*I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them.*

This first principle perhaps best exemplifies the citizen–centric approach first advocated by Sir James Crosby (2008). It emphasises that the citizen, through giving consent to use the service, can trigger various identity assurance activities (typically logging on to a government service). If this consent is not forthcoming or is withdrawn it then follows that no activity can take place. This emphasis on consent also anticipated the strengthened consent requirements in the EU’s General Data Protection Regulation and post BREXIT UK Data Protection Act (GOV.UK 2017c, 2017d; OPSI 2018)

One instance where consent issues were discussed in detail relate to the Hub identity picker service. The picker service is intended to guide users to the most appropriate identity providers for them, based on their answers to very simple questions such as whether they have a driving licence, passport or a smartphone that can install apps. A version of the hints service shares this data with identity providers to improve the registration process, but the data collected is not retained and is primarily intended to produce a list of identity providers that are likely to be able to provide a Verify’d identity given the data the user has available.

Further discussions with PCAG revolved around whether the answers to these questions constituted “personally identifiable data” and whether it would be appropriate to obtain user consent to the collection of this data. The wording of the privacy notice was altered accordingly.

### *Transparency*

*Identity assurance can only take place in ways I understand and when I am fully informed.*

As described above, being open and transparent about what is happening during the identity assurance process is a key feature of the whole Verify programme. This principle reiterates this emphasis on transparency and is implemented in terms of detailed guidance about what happens to a user’s data on the website of the various identity providers and in their privacy

policies. This is discussed further in relation to Verify's Data Protection Impact Assessment below.

There is ongoing academic discussion about what it means to be “fully informed,” particularly about something as technologically sophisticated as the Verify architecture, but the intention is to ensure that the interested user can find as much information about the process as they desire without overburdening the average users who are less interested in this detail.

### *Multiplicity*

*I can use and choose as many different identifiers or identity providers as I want to.*

This principle is specific to Verify as the architecture is designed around a federated model with a number of certified identity providers. This principle allows users to create Verify'd identities with as many, or as few, identity providers as they wish. The author, for example, has a Verify'd identity with each of the existing identity providers. When coupled with the central role of the Hub, this means that government service providers cannot require users to obtain a Verify'd identity from a particular identity provider and as the hub only shares a matching data set that has been provided to agreed standards, shouldn't need to.

The federated approach with multiple identity providers allows users the option to segment their online interactions further (even though logically the Hub architecture means this shouldn't be necessary), for example by choosing to use one identity provider to interact with the Department of Work and Pensions and another to interact with HM Revenue and Customs etc.

This principle also allows for the situation where new identity providers who already have strong identity evidence for existing customers would be able to offer a Verify'd identity as part of their regular customer service proposition by becoming certified companies in future procurement rounds, even if those individuals already have Verify'd identities with other identity providers. For example, banks (who already have undertaken strong Know-Your-Customer (KYC) checks) might allow customers to access online government services using their online banking account (Reuters 2016).

### *Data Minimisation*

*My interactions only use the minimum data necessary to meet my needs.*

Data minimisation is a data protection principle that was first explicitly articulated in the OECD principles as the “collection limitation principle” (OECD 1980). Data minimisation avoids the collection of extra data “just in case” it might be useful. As a described above, data minimisation applies during the identity proofing and verification stages whereby any data obtained as part of the verification process (e.g., passport number and date of issue) is not retained for purposes other than audit once the verification result has been obtained. Similarly, when a Verify'd identity is used to access a government service only a minimal matching data set is sent to the service via the Hub.

### *Data Quality*

*I choose when to update my records.*

This principle is an explicit reaction to the identity management mentality that Sir James Crosby warned about in his report (2008). For example, in the UK, failure to notify the DVLA of a change of address is punishable with a fine of up to £1000 (GOV.UK 2018c). Verify does not impose any such obligation on users and hence doesn't have the associated regulatory enforcement costs. Instead, if a user fails to update their records with the identity provider, this will either be picked up as part of the ongoing revalidation of their Verify'd identity or may cause the transaction with the government service provider to fail.

### *Service User Access and Portability*

*I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want.*

This principle picks up on two themes. The first is the issue of explicit data portability introduced as part of the GDPR. Verify is a new service and so doesn't emerge from existing legacy systems. As such, it is possible for the certified companies to build comprehensive and automatic data extraction capabilities into their systems. More generally, as the user is authenticated by the identity provider to a level that would allow them to interact with government, the user should also be able to complete an automatic, self-service "subject access request" to access this data rather than needing to submit a paper-based request.

As this capability is not a formal requirement of the identity providers, the onboarding process currently only encourages them to accept such online subject access requests alongside paper-based applications whilst allowing them to use offline channels for further checks and payment.

The principle also allows a user to revoke their consent for an identity provider to hold their Verify'd identity (Curren and Kaye 2010). This also ties in with the "right to erasure" in the GDPR and the associated Data Protection Act in the UK (GOV.UK 2017c; OPSI 2018).

### *Certification*

*I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements.*

Although Verify implements a federated identity approach it places restrictions on which identity providers can participate. Because the transactions with the Hub are encrypted, only those identity providers that are certified by Verify (including for their compliance with the identity assurance principles) are issued with keys that will allow them to interact successfully with the Hub and associated services. This use of cryptographic keys also means, for example, that if a particular identity provider suddenly fails to satisfy the governance requirements (perhaps because of a security incident, financial problems or restructuring of its identity proofing and verification services) it is possible to revoke their keys whilst retaining

the keys of the remaining identity providers. This would exclude, effectively instantly, the no-longer accredited identity provider from the federation. Additionally, if they were removed from the page where users select their chosen identity provider, they would be unable to initiate encrypted transactions via the Hub.

Of course, this moves the issue to the question of what it means to be “certified against common governance requirements” (GOV.UK Verify 2014h) including how strictly the requirements are enforced and how they are interpreted (cf Moss 2016b). For example, does a rebadged identity service that is already provided by a certified provider need to be certified in its own right or can Verify rely on the accreditation of the underlying service?

Similarly, user service requirements might allow ongoing use of a certified company while back office issues are being resolved, for example, responding to the regulatory consequences of the “safe harbour” ruling (Orlowski 2015).

#### *Dispute Resolution*

*If I have a dispute, I can go to an independent Third Party for a resolution.*

Verify works on the assumption that, as a large-scale service, users will inevitably have some problems with the service. These could range from temporary service outages, misunderstandings about the scope and capability of the service to problems with identity proofing and verification. The dispute resolution principle provides for an independent third party that can help resolve any problems the user has, particularly in cases where initial attempts to resolve the issue with the identity provider have not proved satisfactory.

The identity assurance principles are written for the time when the service is “mature and well established,” acknowledging that “in the early stages of its development there may well be a phasing-in period” and that, in some cases, “a principle might need a degree of initial flexibility” (GOV.UK Verify 2014a, para. 2.4).

In the case of the dispute resolution principle, although Verify has undertaken discovery work around the dispute resolution/ombudsman role, disputes and queries are currently being addressed by the Verify customer support team (GOV.UK Verify 2016u). The team provides regular updates on the level and kinds of issues to the Privacy and Consumer Advisory Group as well as the Verify Senior Management Team.

#### *Exceptional Circumstances*

*I know that any exception has to be approved by Parliament and is subject to independent scrutiny.*

It is recognised that there will be exceptional circumstances where the identity assurance principles need to be ignored. This principle seeks to ensure that any potential exceptions are explicitly discussed in Parliament rather than being implemented by statutory instruments (Parliament 2016) that are rarely properly debated. It also seeks to guard against the (mis)use of existing legislation, such as the use, in the UK, of Section 94 of the Telecommunications

Act 1984, that permits the Home Secretary to give “directions of a general character” which appear to be in the interests of national security to require a mobile phone company to hand over all call data (Strasburger 2016), or the use, in the USA, of the 1789 All Writs Act to compel Apple to decrypt smartphone data (Thomson 2014).

### **Data Protection Impact Assessment**

As a government technology project, GOV.UK Verify was subject to a Privacy Impact Assessment (PIA) and Data Protection compliance check before the programme started in 2013. As the programme has since evolved significantly, a fresh Privacy Impact Assessment (known as a Data Protection Impact Assessment in the GDPR) has been produced and provides “an analysis of core aspects of GOV.UK Verify from the perspective of a user” and is intended to help “understand their privacy-related needs” (GOV.UK Verify 2016v). The full impact assessment document has been published online (GOV.UK Verify 2016w). In addition, the Pan Government Accreditation Service has undertaken a government wide impact assessment.

Perhaps unsurprisingly given that Verify is an exemplar of how live systems can be built with privacy principles incorporated from the start, the detailed data protection compliance check only makes a small number of recommendations, for example that GDS should “should establish procedures to create and maintain a comprehensive record of use of personal data across the GOV.UK Verify ecosystem. The record should include details of processing carried out on GDS’ behalf. This record should be checked regularly” (2016w, p. 29), that GDS “should establish protocols to ensure the regular review of retention periods for personal data” (2016w, p. 34) and “should establish user support procedures for reviewing and responding to service user’s notice or a court order for rectification, blocking, erasure or destruction of personal data” (2016w, p. 38).

In terms of compliance with the identity assurance principles, the impact assessment recommends that GDS “should mandate that certified companies are not permitted to solicit, infer or otherwise obtain information about the service user’s interactions with Government Services (including knowing the identity of those Government Services)” (2016w, p. 51), that they “should ensure that certified companies and Government Services do not charge service users for access to their personal data (Subject Access)” (2016w, p. 54) and that GDS “regularly reviews the requirement for the identity assurance supervisor function [dispute resolution], which is currently served by the user support team and should expand the function should that be necessary” (2016w, p. 59) etc.

### **Governance Structures**

The identity assurance programme has very specific governance needs stemming from its dual role as a central provider of a cross government service and as the sole contractual authority with the market for identity services on behalf of central government. It has a number of governance needs, including:

- department ownership of their plans to connect services to GOV.UK Verify;

- active and visible monitoring of progress by officials and Ministers;
- change control, particularly relating to competing departmental priorities for Verify;
- clear decision processes and escalation channels;
- collective strategic decisions (policy, commercial, use of Verify beyond central government etc.). Alignment with wider government plans and goals for data, technology and digital services (GOV.UK Verify 2015d).

Thus, governance activities take place at several different levels, see figure 21.

**Figure 21. Verify governance taken from (GOV.UK Verify 2015d)**



### **The Verify Team**

The Verify programme director is currently Jess McEvoy, who took over in August 2016 from Janet Hughes, who had led the team since June 2013 (GOV.UK Verify 2016x). The Verify programme team is responsible for all aspects of the delivery of the Verify service as well as liaison with other government departments and external bodies. Verify is part of GDS, which is itself part of the Cabinet Office. The Minister for the Cabinet Office is David Lidington MP, a role previously held by Damian Green MP, Ben Gummer MP, Matt Hancock, MP and Francis Maude, MP (GDS 2016b, 2017c). The Director General of GDS since August 2016 is Kevin Cunnington (GDS 2016c). This new role replaces the role of Executive Director of GDS previously held by Stephen Foreshow–Cain and Mike Bracken.

### **Contracts and the Framework Agreement**

Key functionality for Verify is provided by private sector identity providers (the certified companies) and their responsibilities are determined by their contractual relationship with the UK Government and the Verify team. Structurally, the contracts are based on Framework agreements. Framework agreements are a type of “umbrella” agreement

normally negotiated with suppliers by Crown Commercial Services on behalf of the public sector (GOV.UK 2015c), although the Verify Framework Agreement was negotiated by GDS. Framework agreements with providers set out terms and conditions under which agreements for specific purchases (known as call-off contracts) can be made throughout the term of the agreement (Crown Commercial Services 2016).

To date there have been two framework agreements for Verify. Each begins with the issuing of a prior information notice (PIN) in the Official Journal of the European Union (OJEU). This notifies companies that they intend to start a formal procurement process (GOV.UK Verify 2014e). There are also specialist supplier events that describe, in more detail, what the government intends to procure.

The first framework agreement resulted in contracts being signed with five potential identity providers (Digidentity, Experian, Mydex, The Post Office and Verizon) although Mydex never offered a live service and didn't participate in the second framework agreement (GOV.UK Verify 2015g). The second framework brought the number of potential certified companies to nine (Barclays, Digidentity, Experian, GB Group, Morpho, PayPal, Post Office, Royal Mail and Verizon) although PayPal ended up withdrawing from the second framework (Merrett 2016b).

Under the current frameworks, certified companies have to be certified by tScheme, an industry-led, self-regulatory scheme set up to create strict assessment criteria, against which it will approve various Trust Services (tScheme 2017).

Alongside the privacy, security and associated business requirements that the certified companies must provide, the framework process also tries to ensure healthy competition in the marketplace of identity providers, to encourage innovation. To this end, the second framework agreement sought to restrict the number of organisations that “material sub-contractors” (who assess and analyse evidence and data to meet one or more of the five elements of the identity proofing and verification process) could work for, so that Verify didn't end up with a situation whereby all the certified companies were relying on a small number of “material sub-contractors” to do all the work involved in verifying a person's identity (GOV.UK Verify 2014i).

In July 2016 Verizon was “temporarily removed” as a certified company for Verify (Merrett 2016c). This meant they were not listed as an option for new users from July 2016 and permanently withdrew thereafter (GOV.UK Verify 2017f).

The identity assurance principles were not a formal part of the first framework procurement, although they were incorporated in the second framework, Part 17.1 Privacy of the Procurement 2 Framework Agreement. This required that identity providers were obliged to offer “a privacy policy (the “Provider Privacy Policy”) which is clear and easily comprehensible and which outlines (i) the steps the Provider, its Affiliates and Provider Personnel have taken to comply with the provisions in the Identity Assurance Principles which are applicable to such parties; and (ii) any measures they plan to implement in future” (GOV.UK Verify 2016w, sec. 7.2).



The identity assurance principles are not, however, one of the mandatory compliance requirements defined in Part 8.3 Provision of Services. They have, however, been reviewed as part of the privacy assessment (GOV.UK Verify 2016w, sec. 7).

### **Code of Interoperability**

The GOV.UK Verify Code of Interoperability (CoIn) (GOV.UK Verify 2017d) plays an equivalent contractual role in relation to the government service providers that will consume Verify'd identities from the Hub. It describes the controls that organisations must implement and the responsibilities they must undertake to access GOV.UK Verify, and the responsibilities of Government Digital Service (GDS) in relation the GOV.UK Verify service.

The signed CoIn takes effect as a Memorandum of Understanding between GDS and department that will use Verify services. It describes the controls that Relying Party organisations must implement and the responsibilities they must undertake in order to access GOV.UK Verify. In particular, this means that they are required to:

- complete the Onboarding Process and provide all the evidence required as part of the Onboarding Process to the standard required within this process; and
- comply with the requirements for security controls.

The CoIn also details the payments associated with using GOV.UK Verify.

### **Technological Controls**

Alongside the Good Practice Guides on RSDOPS and identity proofing and verification written by GDS in collaboration with CESG, CESG has published GPG (44) (GOV.UK 2014) that relates to the use of identity credentials to support user authentication for online government services (GOV.UK Verify 2016y). This provides guidance about different types of credentials and the quality of authentication they can achieve (e.g., what kinds of protections they provide against misuse in the event of credential theft). The guidance also identifies different levels of quality for credentials (such as whether they contain protective measures that prevent prediction or duplication, whether any tokens resist tampering and whether they are tamper-evident).

The guidance discusses the quality of different forms of credential management (including revocation) and active monitoring of credential use (e.g., the same credential being used in two very different physical locations at the same time). It also discusses the role that biometrics can play in authentication.

SAML (Security Assertion Markup Language) is used for all data flowing between the identity providers, the Hub and the service providers (GOV.UK Verify 2013b), see also (GOV.UK Verify 2015h, 2015i). With all data flows encrypted as they pass between the identity providers, the Hub and the service providers, another form of governance emerges, namely technological (cryptographic) enforcement of required standards and processes. An identity provider or service provider that fails to deliver a service that satisfies the norms,

service standards or contractual requirements of the Verify service can effectively be locked out of the system by revoking the encryption keys of the errant service and by removing it from the Verify interface. This form of governance allows for very rapid action, for example, as a result of a data breach and should help ensure that trust in Verify is maintained.

This occurred recently, while Verizon completed its external certification process following a material change in the company's contracting structure (Merrett 2016c).

### **Risk Management Processes**

The technological controls put in place around Verify are best understood in relation to the Pan-Government Accreditation (PGA) service which seeks to manage risks related to the use, processing, storage and transmission of data.

As with other parts of government, managing information assurance and security risks is a key part of the overall business of building and running public services (NAO 2016).

GOV.UK Verify has specialist team members who follow a risk assessment methodology to define risk in a quantifiable and repeatable manner. They communicate those risks back into the programme Senior Management Team with recommendations on appropriate mitigations to those risks, allowing the right people to make informed decisions. The wider GOV.UK Verify team, including its security experts, provide support to ensure that what they are doing is appropriate and sensible (GOV.UK Verify 2016i).

There are two groups within the GOV.UK Verify team that are responsible for looking at risk more broadly: the risk management group and portfolio group. These groups work to ensure Verify has the resources available to mitigate identified risks in a timely manner. The risk assessment process evaluates the impact of something going wrong, understands who poses a threat and how they will attempt to gain access and analyses the motivation and capability of identified threats. As such, they follow industry standard good practice and apply it to the Verify service. Based on this risk assessment they then establish baseline controls and work with the technical development team to work out the best technological controls to protect Verify. Additional mechanisms available include procedural and operational implementation controls, staff management and supervision and physical controls to ensure the protection of equipment and people. Additionally, monitoring and audit checks whether all the controls are working.

Because Verify a cross-government service, the senior information risk owner for GOV.UK Verify reports to the Government Senior Information Risk Owner (GSIRO). The GSIRO has cross-government remit and responsibilities including responsibility for making sure that GOV.UK Verify is managing its risk appropriately.

The GSIRO needs to know that what the programme are telling them about potential risks and mitigation is accurate. To facilitate that an independent person, known as an Accreditor, is normally appointed to act as an arbiter of risk. In the case of GOV.UK Verify it has two Accreditors. One is from GDS (but outside the GOV.UK Verify team): they make sure the team consider all risks and apply the appropriate controls in line with Cabinet Office policy.

The other is a Pan Government Accreditor (PGA) from CESG: they ensure that risks to wider government are considered and reported back to the GSIRO.

The regular meetings that take place between the independent Accreditors and members of the GOV.UK Verify team mean that there is a constant open communication channel between all those concerned about security risk (GOV.UK Verify 2016i). This process includes active monitoring of potential threats as well as checking for attempts to introduce false/fake documents as part of the registration process.

Another key part of this process is ensuring effective plans are in place for the eventuality that Verify might be offline (GOV.UK Verify 2016z).

### **PCAG Guidance**

As noted above, PCAG's identity assurance principles formed part of the second procurement framework and whilst they are not currently a mandatory compliance requirement, the most recent data protection assessment made only limited recommendations for ensuring that the principles continue to be complied with. PCAG therefore plays a non-standard role in the governance of Verify. It is a body that is independent of the Verify team and the Cabinet Office more generally, although GDS notes that it is guided by PCAG (amongst others) (GDS 2018c). PCAG is a signatory to the World Bank principles on identification (World Bank 2017) and is described there as the "Privacy and Consumer Advisory Group to the Government Digital Service and GOV.UK." Its scope has primarily been around identity assurance although it has advised ministers and civil servants about privacy and consumer issues around government data handling more broadly. As can be seen by the incorporation of its identity assurance principles in the framework procurement process, there is a strong, symbiotic working relationship with the Verify team, whereby the advice of PCAG is sought on all key decisions.

## **E. Verify: Life After Live**

In the months since May 2016 when Verify became a live service, there have been a number of significant changes in the leadership of GDS and the Verify team. The Cabinet Reshuffle following Teresa May's appointment as Prime Minister in July 2016 resulted in a new Minister for the Cabinet Office, Ben Gummer MP (GDS 2016b). A few weeks later saw the arrival of Kevin Cunnington as Director General of GDS. This new role gives GDS a similar status to other significant parts of the civil service. Cunnington was previously Director General for Business Transformation in the Department for Work and Pensions (DWP). Shortly after his arrival, Janet Hughes decided to leave GDS and she has been replaced by Jess McEvoy as interim Programme Director.

Given this level of staff turnover, it is understandable that there has been press speculation about the fate of GDS and the Verify team (Evenstad 2016a, 2016b; Virgo 2016). Cunnington has brought in some of his own advisers from DWP (Glick 2016a) to assess all aspects of GDS's operations and develop a new strategy for GDS by the end of 2016 (Bicknell 2016a).

In early February 2017, GDS released its Government Transformation Strategy (GDS 2017a, 2017d) for the period 2017–2020. This included a commitment to making better use of GOV.UK Verify by working towards 25 million users by 2020 and exploring options for delivery of identity services for businesses and intermediaries. This strategy fed into the UK Digital Strategy (GOV.UK 2017b) and its proposals for maintaining the UK government as a world leader in serving its citizens online (GOV.UK 2017a).

In April 2017, the Prime Minister called a surprise general election. Ben Gummer was a lead author of the Conservative Party manifesto (Conservative Party 2017) which included a whole section on digital government and public services. This committed a future Conservative government to using “common platforms across government and the wider public sector.” This would include Verify as a “single, common and safe way of verifying themselves to all parts of government” stating that this “is why we shall roll out Verify, so that people can identify themselves on all government online services by 2020, using their own secure data that is not held by government.” The manifesto continued noting that the government “will also make this platform more widely available, so that people can safely verify their identify to access non-government services such as banking” (2017, p. 81).

Although the government lost its majority in Parliament following the election, and Gummer lost his seat, the manifesto commitments remain the policy of the (minority) government.

This explicit commitment to Verify was particularly timely in light of external pressures on Verify. In February 2017, a blog by HMRC digital seemed to imply that transformations in the Government Gateway (due to close in its current incarnation in 2018) meant that HMRC was going to provide an alternative identity service to Verify (Cellan-Jones 2017). When journalists picked up on this issue and highlighted the potential public confusion and higher bill for the public purse, HMRC rapidly backed down and clarified that it didn’t intend to provide an alternative to Verify and reiterated its support for Verify beyond the revamp of the Government Gateway (Bicknell 2017; Burton 2017a, 2017b; Fiveash 2017; Glick 2017b; Merrett 2017a).

In March 2017, the NAO report on digital transformation included a specific section reviewing GOV.UK Verify warning that take-up of Verify has been undermined by its performance and GDS had lost focus on the longer term strategic case for the programme (NAO 2017, para. 18) echoing some of the concerns raised in an earlier report by the Institute for Government (2016). Moreover, PCAG co-chair Jerry Fishenden, who had been part of the NAO team, resigned from his GOV.UK Verify role and called for a fundamental review of Verify (Fishenden 2017; Glick 2017c).

In terms of Verify, although the time for it to be a live service has affected Britain’s progress on digital government (Bicknell 2016b), Cunnington is reportedly “very bullish” about Verify (Glick 2016b) and now that it is a live service is keen for its adoption to be expanded, including working closely with local authorities and the private sector. Verify is seen by Kevin Cunnington as a key enabler for the kinds of digital transformations needed to give government the right tools to get the job done (GDS 2016d).

New services with existing Departments are proceeding through the various onboarding stages (GOV.UK Verify 2016aa). Other application areas, including integration with the National Health Service are also being considered (Merrett 2016d).

This emphasis on increasing the use of Verify and increasing its take up is supported by the certified companies, some of whom are reporting earnings issues because of the lower than anticipated use of Verify (Schonberg 2016).

## **Working with Local Authorities**

A major development, already in process before Cunnington arrived at GDS but given increased prominence under him, is the exploration of how Verify can be used by local authorities (GOV.UK Verify 2016ab). Following the GDS approach, this work has begun with a discovery phase. This has resulted in interactions with 80 local authorities who provided details about the transaction costs and volume data needed in support of pilot projects from more than 60 local authorities (GOV.UK Verify 2016ac).

Some local authority applications (e.g., parking permit, concessionary travel and taxi licensing services) need to combine identity data with driving related attributes based on data held by the Driver and Vehicle Licensing Agency (DVLA) and so two discovery days were held with DVLA and involving participants from 41 councils (GOV.UK Verify 2016ad). Verify has already worked collaboratively with the DVLA on the design of a number of their services (GOV.UK Verify 2016ae).

Following this discovery work, two pilots are underway (GOV.UK Verify 2016b). These relate to older people's concessionary travel and residents' parking permit services. These are services that most local authorities are looking to transform. In order to participate in the pilot studies, local authorities must agree to the requirements of the pilot project agreement which includes buy-in and participation from key stakeholders, a commitment in principle to implement GOV.UK Verify in accordance with various standards including the identity assurance principles (Merrett 2016e).

Nineteen local authorities have signed up for the #VerifyLocal pilots, six of whom will pilot both services (GOV.UK Verify 2016af). A lot of local authorities, including many of the pilot participants, work directly with suppliers to provide aspects of their services and so local authority integration in such cases will also involve integration with the systems provided by these suppliers. A distinct strand of discovery work is being undertaken to better understand these requirements (GOV.UK Verify 2016ag).

## **Private Sector Use of Verify'd Identities**

From the earliest days of Verify, the programme team has engaged with the private sector, not simply to support the verification process or to become an identity provider or in their role as the providers of services for local authorities. Rather the engagement has been based on the premise that the logic of performing a one-time verification and then being able to

use a Verify'd identity that was "good enough for government" for commercial transactions would offer additional benefits to citizens (UKAuthority.com 2016).

In order to explore these possibilities, in 2012 the Verify team became a founder member of OIXUK—the UK chapter of the Open Identity eXchange. OIXUK a nonprofit, technology agnostic, collaborative cross sector membership organisation with the purpose of accelerating the adoption of digital identity services based on open standards.

Verify uses OIXUK "to communicate with the marketplace for identity assurance supply and to support experimental alpha and discovery projects that explore the real-world business, design and technical challenges that will shape the adoption of digital identity services based on open standards." A number of OIXUK discovery projects have been undertaken. Resulting white papers are available on the OIXUK website (OIXUK 2018).

For example, a recent OIX report (OIXUK 2016c), highlighted industry's needs for identity related attributes that go beyond the matching data set of core identity attributes (name, address, date of birth and optionally gender).

Other reports explore the possible use of Verify'd identities for the peer-to-peer economy, for creating a pensions dashboard (Merrett 2017b), to transform attitudes and behaviours towards savings, to open a bank account and undertake financial transactions in another country, as well as opening an account in the UK before arriving (GOV.UK Verify 2016ah) and digital "blue badges" which enable special parking allowances for individuals with mobility issues.

There have also been OIXUK technical reports around attribute exchange, shared signals (for spotting and sharing threats) and the role of mobile operators in the digital identity space.

## **EU Integration, eIDAS, and BREXIT**

On 23 June 2016 a referendum in the UK voted (52 percent/48 percent) in favour of the UK leaving the European Union, the so-called BREXIT. The new Prime Minister, Theresa May, has confirmed that BREXIT will be taking place and she invoked "article 50," and thus initiated the process whereby the UK leaves the EU two years later, at the end of March 2017. At the time of writing, the implications for Verify in terms of EU interactions are unclear. Nevertheless, it is possible draw a number of inferences based on previously issued statements.

The first implication is that for most aspects of its service, BREXIT will have no direct effect on the function and operation of Verify. Verify enables secure online transactions with the UK government and BREXIT will have no effect on this. Similarly, identity evidence from other EU countries will continue to be assessed in the same ways as before (although one consequence of BREXIT might be a lower demand for verification of EU documents as a result of reduced numbers of EU citizens living and working in the UK).

As part of arrangements to support labour mobility within Europe, European Member States want people to be able to identify themselves online for digital services in other countries. To achieve this, Member States have agreed to set up a system that will allow people to use a digital identity verified in one country to access public services in other countries. This is covered in the eIDAS regulations, which also cover the interoperability of electronic digital signatures (European Commission 2016).

Under this process, the eIDAS regulations set up arrangements whereby a user will be able to choose to verify their identity with one country's system, in order to use a digital service from another country (Tsakalakis et al. 2017). For example, it would be possible to use a GOV.UK Verify account to prove identity to the Danish tax authorities, making it easier to file a tax return for individuals who live or work there. Formally, eIDAS is concerned with the mutual acceptance of eID across borders through authentication of a verified identity, that is the user chooses to authenticate with their home member state's eID rather than verifying their identity in the other country.

When a user wants to access a service in a different country to the one that has verified their identity, those two countries' identity assurance services will need to be able to trust and talk to each other securely. The eIDAS Regulation sets out the rules of how this will work and recently the standards and supporting details have been agreed.

The plan is for citizens to use their trusted national digital identity scheme to sign-in to any relevant EU Member State service. eIDAS also covers "legal persons" (i.e., businesses) and businesses operating in the UK are likely to use eIDAS to file things such as VAT returns, export licenses and intellectual property rights.

As long as the digital identity scheme used by a Member State meets the assurance levels set down in the Regulation (GOV.UK Verify 2015j), the scheme can be used to transfer identities across the system to a service. This means the UK can continue using GOV.UK Verify, while other countries can use their national identity card schemes. These different approaches can work together to make it possible for users to access digital services across borders. Verify's role in shaping the legislation means that it will be relatively straightforward to map the Verify levels of assurance to the levels of assurance specified in eIDAS. The EU federated approach also does not require a central EU database or a single, persistent, unique national identity number and as such, unsurprisingly, is compatible with the approach taken by Verify.

In November 2015, the Verify team were reporting that, now that the relevant standards and legislation had been agreed, they were looking at how to implement them in the UK (a process that would involve "notifying" the EU that Verify was ready to be part of this interoperable system) (GOV.UK Verify 2015k).

With BREXIT, consideration of whether to include Verify within the EU system is likely to be something to be negotiated alongside other aspects of the UK's withdrawal from the EU. Nevertheless, from 2018, the UK will be legally required to accept identities from other member state's notified schemes.

One indirect consequence of the eIDAS regulations has been their incorporation in the latest anti-money-laundering (AML) regulations. In particular, a new AML directive adopted in 2016 includes full consistency with provisions on electronic identification as governed by the eIDAS regulation (GOV.UK Verify 2016a). Given that Verify is already aligned with eIDAS, the next steps are to transpose the EU regulation into UK national bank regulations (and hope that they remain in place post BREXIT). As the Verify team note, “this explicit cross reference to government identity verification standards in the new AML Directive sets the regulatory framework that will facilitate bank acceptance of a user’s digital identity” (GOV.UK Verify 2016a). The implications of this for the customer account opening process may well be significant.

### Future Government Services Using Verify

A blog post in May 2016 (GOV.UK Verify 2016a) reviewed the scale of current services connected to Verify as well as other government services that were in the process of onboarding with Verify.

**Table 4. Live and onboarding central government uses of Verify**

Department	Service	Status	Total users/year	Anticipated new users sent to GOV.UK Verify by April 2017
DfT/DVLA	View or share your driving licence information	Connected September 2015; in public beta	15m	100–400k
DfT/DVLA	Tell DVLA about your medical condition	Connected May 2016; in private beta	300k	50–90k
DWP	Sign in to the Universal Credit digital account	Connected March 2015; in public beta (restricted by postcode)	10m	>5k
DWP/HMRC	Check your state pension	Connected April 2015; in public beta	3m	100–300k
HMRC	Sign in and file your self-assessment tax return	Connected December 2014; in public beta	3m	>100k
HMRC	Sign in to your personal tax account	Connected July 2015; in public beta.	–	100–200k



HMRC	Check your income tax estimate	Connected February 2015; in public beta. Also accessible via personal tax account.	2m	Volumes include users accessing these services directly via start pages and through the personal tax account
HMRC	Check or update your company car tax	Connected February 2014; Live service. Also accessible via personal tax account.	70k	
HMRC	Claim a tax refund	Connected March 2015; in public beta. Now only accessible via personal tax account.	95k	
HMRC	Help your friends or family with their tax	Connected March 2015; in public beta. Also accessible via personal tax account.	–	
BIS/Insolvency Service	Claim for redundancy and monies owed	Connected February 2015; in public beta	100k	30k
Defra	Claim rural payments	Connected July 2014; in public beta	90k	5–10k
HMRC	Tax credits service	Connected February 2015 as part of a limited trial; trial ended in July 2015.  Service is about to reconnect June 2016	3m	150k

The following services are planning to use Verify (GOV.UK Verify 2016aj):

**Table 5. Future central government uses of Verify**

Department	Service	Status	Anticipated GOV.UK Verify users in the next year
NHS England	View your personal health record (NHS Liverpool Clinical Commissioning Group pilot)	Planning to connect June 2016	5k
DfT/DVLA	Apply for an operator licensing certificate	Planning to connect July 2016	<5k
BIS/Insolvency Service	Declare bankruptcy online	Planning to connect July 2016	10k
BIS/Land Registry	Sign your mortgage deed	Planning to connect September 2016	TBC, Summer 2016
DWP	Activate your state pension	Planning to connect October 2016	<5k
DWP	Apply for the Personal Independence Payment	Planning to connect October 2016	TBC, Summer 2016
HMRC	Apply for childcare support	Planning to connect November 2016	10–20k
HO/Disclosure and Barring Service	Apply for a basic check	Planning to connect December 2016	50k
DWP	Access to work	Planning to connect October to December 2016	15k
DWP	Child maintenance	Planning to connect 2017	TBC, Winter 2016
DWP	Bereavement support	Planning to connect 2017	TBC, Winter 2016
DfE/Ofsted	Childminder or childcare provider	Planning to connect 2017	5k
NI	Register a child's birth in Northern Ireland	TBC	TBC
MOJ	File for uncontested divorce	TBC	TBC
HMRC	Inheritance tax online	TBC	TBC
HMRC	View your medical benefit	TBC	TBC
BIS/Companies House	Voluntary dissolution of a company	TBC	TBC, Winter 2016
DfT/DVLA	Amend your driver record	TBC	TBC

## Limitations and Critiques

There are a number of limitations with Verify. Some of these, such as problems that certain groups in society face when trying to get a Verify'd identity, are a consequence of the decision to use a standards-based approach to identity proofing and verification and the implications of the requirements of these standards. Coverage problems are (hopefully) resolvable and can be addressed by including additional identity evidence data following better analysis of the demographics of who has which evidence that is needed for a Verify'd identity. Other options include consideration of supported verification (for those who have appropriate documentation but need assistance in completing the verification process) as well as the introduction of LoA1 and services that can use LoA1 Verify'd identities.

Moreover, as the identity providers are only paid for successful registrations, they have a strong incentive to identify and use new data sources that will enable them to provide Verify'd identities for as many customers as possible.

Alongside the decision to base Verify on agreed standards is the decision to use private sector companies to implement the various identity related activities the standards require, a decision that not all stakeholders are necessarily comfortable with.

Other limitations, as noted by a recent OIXUK report, relate to the deliberately limited matching data set that is sent by the identity provider via the Hub to the service provider (OIXUK 2016c). There are a number of scenarios where the matching data set needs to be enhanced with (or, occasionally replaced by) attribute exchange. For example, a possible electronic voting service would need an "entitlement to vote" attribute to be exchanged alongside identity data. In other scenarios, an "over 18" attribute might be all that is needed to access age restricted goods and services.

There are a number of ways in which Verify *might* integrate with such attribute exchange capabilities. Alternatively, attribute exchanges might choose to draw on the lessons learned from the Verify approach when implementing a non-Verify service.

Another area where Verify is not operating concerns organisation related identities. Although GPG 46 (GOV.UK 2013) relates to establishing the identities of organisations or individuals acting on behalf of those organisations, the currently preferred approach is for the organisations to assert who their authorised individuals are and then, if necessary, to use Verify to ensure that only Verify'd identities are used by these authorised individuals when acting on behalf of their organisation. A version of this approach has been implemented in terms of rural payments although it has not been widely adopted by government services that make extensive use of people acting as agents for others (e.g., those with powers of attorney or accountants completing tax returns on behalf of their clients).

A final limitation of Verify relates to the number of individuals who fail to complete the Verify registration process to obtain a Verify'd identity. As noted above, some of these incomplete service journeys may be the result of demographic difficulties in obtaining a Verify'd identity or issues with the implementation of the standards. Others, however, might arise when a government service inappropriately requires Verify and a LoA2 Verify'd identity

to access the service. Internal Verify data suggests that completion rates are far higher in those situations where users have an immediate benefit than those where the benefits are less apparent. Thus, services like completing a self-assessment on time and not being fined for late submission or claiming a tax refund are most likely to result in the successful creation of a Verify'd identity. They are also, of course, the services most likely to be targeted by fraudsters and hence carry an associated requirement for proper identity proofing and verification and active security monitoring.

Alongside the acknowledged limitations and design choices associated with Verify, a number of critiques exist. These have been raised at various levels of operation. For example, the paper by Brandão et al. (2015) highlights concerns about the technical design choices in Verify and their vulnerability to various risks and attacks.

Other concerns have been raised about the inclusion of gender in the matching data set. Whilst there is scope for gender to act as a useful further disambiguation mechanism for the matching process, it also raises the prospect, particularly for transgendered individuals, that the matching process will fail and require users to disclose, unnecessarily, their transgender identity even to government service providers whose internal processes do not use gender (Currah and Mulqueen 2011; Martin and Whitley 2013). It is for these reasons that the gender field is optional in the matching data set and does not need to be provided in the initial registration process.

A concern related to both of these points involves the recognition that the matching data set is used in all Verify transactions and so is being shared (in encrypted form) quite widely. Further concerns arise when, for operational reasons, a (semi)persistent identifier is used to speed up the matching process. That is, once a Verify'd identity from a particular identity provider is matched against a service provider's database, a unique identifier (for that pairing of identity, identity provider and service provider) is created, meaning that the matching process can be bypassed if that pairing reoccurs. These internal identifiers are simply intended to speed up the matching process and can be revoked (requiring a repeat of the matching process) as required.

There are probably a number of factors behind the decisions by two certified companies, who were part of their relevant framework agreements, to not offer identity provider services and for Verizon to withdraw from offering identity provider services. Whether these relate to internal reorganisations, concerns about being able to use niche identity evidence checking services for specialist communities or other issues, the high profile of Verify means that any such issues might either undermine confidence in the service or enhance confidence through being clear that only certified companies who can deliver to the quality level the government requires participate in Verify.

Finally, it has taken Verify over five years to become a live service. Critics suggest that this is an unreasonably long time for the service to become live and successful. Although this matches the experiences of other exemplar digital identity systems such as the Estonian model, it does introduce concerns about the long-term viability of Verify.

One potential explanation for the slower than desired roll out of Verify is that, as an exemplar, Verify had to do a lot of the background work that had only been hinted at in proof-of-concept federated identity systems for citizens. Certainly, a lot has been learned in the process and much of the information is available in the public domain and in open standards, whether it relates to identity proofing and verification, the requirements for strong authentication credentials, open sourced software or the SAML profiles associated with delivering the services. Another partial explanation relates to the amount of business process transformation that is required when Verify'd identities are used in legacy processes.

## **F. Learning from Verify**

Although Verify emerged as a response to a very specific socio-political context in the UK, the Verify model contains many features which can inform identity policies in other countries and contexts. At one level it is possible to explicitly use (parts of) the Verify model directly in alternative contexts, as is the case with the EU eIDAS regulations (European Commission 2016) and the work of the Australian Digital Transformation Office (Easton 2016; Head 2016). In fact, GDS has a special “international team” that is responsible for such international collaborations, ranging from participation in international standards bodies through to hosting visiting international guests (GDS 2016e).

Alternatively, the design choices that underpin the Verify model can provide a useful template against which current and future identity practices can be contrasted. The intention in this case is provide an alternative approach against which to review the reasons for the proposed practices against the reasons why Verify might do things differently. For example, reflecting on the innovations that arise from Verify's use of multiple identity providers may provide trigger innovative improvements in the customer experience even when the government acts as the sole identity provider.

The World Bank's principles on identification in a digital age (World Bank 2017). present ten principles are “fundamental to maximizing the benefits of identification systems for sustainable development while mitigating many of the risks” (World Bank 2017, p. 3). They provide a convenient structure for reflecting on how the Verify model can inform identity systems globally.

### **1. Ensuring Universal Coverage for Individuals from Birth to Death, Free from Discrimination**

In some contexts, this principle might involve explicit attempts to ensure that under-represented groups such as women or the rural poor are able to enrol in the identity system (e.g., Abraham et al. 2017; Nyst et al. 2016). In the context of GOV.UK Verify, it can be understood specifically in relation to the work involved in improving the demographic coverage that is supported by Verify including supporting individuals in creating their Verify'd identity (GOV.UK Verify 2016u, 2016ak, 2017c; OIXUK 2017a). It also involves ensuring that assisted digital paths are available for all government services.

## **2. Removing Barriers to Access and Usage and Disparities in the Availability of Information and Technology**

Alongside traditional considerations about literacy, access to technology and appropriate support, GOV.UK Verify also highlights the importance of careful service (re)design. For many services, a Verify'd identity may not be necessary or may not be needed to LoA2. A failure to carefully design appropriate user journeys may result in poor user experiences and reduced trust in both the identity system and the government service.

For example, when reviewing the completion rate on the Verify dashboard (GOV.UK Verify 2018b) (i.e., the proportion of visits started on GOV.UK Verify that result in successfully accessing a service, following the creation or re-use of a verified account with a certified company) there is a marked difference between the highest performing service (around 74 percent completion) and the average of all services (around 35 percent completion). Much of this variation can be attributed to the appropriateness of the service (re)design for each of the services.

## **3. Establishing a Robust—Unique, Secure, and Accurate—Identity**

Perhaps the most easily adapted aspect of Verify is its use of a risk and standards-based approach to identity verification and authentication. As discussed in Section B the risk-based approach recognises that the quality of identity credentials can vary from context to context. For accessing Government services online, particularly those that involve the government making welfare payments the UK has decided that an identity that satisfies Level of Assurance 2 (LoA2) is required. Other parts of government, in contrast, might need different levels of assurance (Glick 2016b).

Adopting a risk-based perspective ensures that such issues are explicitly considered by the appropriate risk owner and can result in processes that are fit for purpose rather than the all too often default position that accepts the use of very high levels of identity assurance for all applications.

Having determined the required level(s) of assurance needed for various government services, Verify sets standards for determining what forms of identity evidence satisfy the level of assurance that is required. Verify's approach to specifying what is required to satisfy a particular level of assurance explicitly includes consideration of both errors and targeted attempts to create fraudulent identities. It does not rely on biometric deduplication to ensure uniqueness (to a required level of assurance).

A LoA2 Verify'd identity therefore requires an identity evidence package that includes data about different aspects of an individual's life (citizen, money and living). Thus, although the UK has a well-functioning civil registration system, a birth certificate is only considered as level 2 identity evidence associated with citizenship and, unlike many contexts, is an insufficient basis for an identity that reaches LoA2. If a birth certificate is combined with two other pieces of data at level 2 (e.g., a national 60+ bus pass or a residential property rental or purchase agreement), or with one piece of data at level 3 (e.g., ICAO compliant

passport, mortgage account or student loan account) it can form the basis of a LoA2 Verify'd identity (GOV.UK 2018a, chap. A).

The identity standards that Verify uses also include consideration of the authentication methods associated with the use of a Verify'd identity. Without clear guidance on authentication requirements, any effort to provide high levels of assurance in the identity evidence can be undermined by low quality authentication, such as is the case where a high quality identity credential might be used with a “flash-and-go” visual inspection of the credential (cf Abraham et al. 2017).

Adopting this approach to other contexts will involve both a calibration of the levels of assurance needed for particular government and private sector services and a recognition of quality and availability of existing identity evidence. For example, it may be that a state issued voter card is considered sufficient to allow someone to vote but is deemed unsuitable for determining eligibility for benefits (Gelb and Diofasi 2016, sec. 5). A standards-based approach can help with the transformation of this issue by forcing an explicit consideration of the strengths and weaknesses of various identity credentials including the integrity of their issuance as well as associated concerns about population coverage.

It is important to recognise that the level of assurance associated with a claimed identity is not static. In Verify, ongoing checking could reveal potential issues with the identity evidence package, for example the passport that was used might later be reported lost or stolen. Alternatively, it is possible to create an account with a limited level of assurance, associate this with strong authentication methods and then, over time, build up the identity evidence package to support high levels of assurance (cf Gelb and Manby 2016). Even if further documentation is not added to the identity evidence package, it will be possible to strengthen the activity history associated with the existing identity evidence.

As a result, although Verify might come across as only being suitable for those contexts where diverse and good quality sources of identity evidence already exist, such an identity evidence building approach could succeed in situations where existing sources of identity evidence are relatively poor (Nyst et al. 2016). In addition, context-sensitive alternative sources of identity evidence, such as those enabled by social media usage or mobile phone contracts, can be incorporated into the identity evidence building process. Verify's experiences about the range of data sources that can be used and their relative coverage can provide useful inputs into this process.

#### **4. Creating a Platform that Is Interoperable and Responsive to the Needs of Various Users**

As Verify has been built from scratch, it has been explicitly designed to ensure interoperability across services. As discussed in Section C, Verify endeavours to provide detailed documentation to assist with the interfacing to existing service provider systems (GOV.UK Verify 2017g). Indeed, recognising that not all government departments will have the technological capacity to integrate with the Verify hub in a secure manner, it offers a

matching service adaptor that provides much of the functionality that service providers need to be able to link to it. In a similar manner, with plans to integrate private sector reuse of Verify'd identities it is also possible to experiment with a Verify sandbox (OIXUK 2016b).

A recent report by the BCS Identity Assurance Working Group (2016) proposes a series of criteria that might be used to distinguish a good online identity system from a poor one. Members of the Working Group are in PCAG and so their analysis was likely to have been shaped by their knowledge of Verify. As a consequence, the working group criteria can be a way to reflect on being responsive to the needs of users of identity services.

In terms of the approach adopted by the BCS working group, rather than focusing on features of the technology (is it a smart card?, which agency issues it?, etc.) features that make up what Orlikowski (2000) calls the *technological artefact* the report focuses on the *technology-in-practice*. Thus it starts with some basic questions: What is the purpose of the Scheme? How strong (in terms of levels of assurance) is it? and Who is it for?

A key feature of Verify, that stems from its origins within the Government Digital Service, is the emphasis placed on user needs. As the GDS Service Design Manual notes, "Building a digital service is a complex task, with many risks. ... As the service progresses through development you'll find out more about users' needs, development requirements and the conditions your service will be operating in. ... This approach allows the team making and operating the service to start small, learn fast, and provide value to users as soon as possible"(GDS 2018b).

The BCS criteria also include other considerations that are explicitly addressed by Verify but which are often implicit or under discussed in national identity systems. Failure to address these issues explicitly typically results in them reappearing later in the process where their effects can be much more significant. Thus, the BCS asks Who pays? Who carries the can (liability)? and How well does the identity system work?

Although the use of multiple identity providers is partly a function of the political decision that the UK government would not act as an identity provider, this approach encourages innovation in both verification and authentication activities.

In most contexts, identity credentials are issued by a state monopoly service and, as such, can fail to be responsive changing user needs (Ciborra 2005). Because of the way in which the procurement framework for Verify has been configured identity providers have strong incentives to improve the user experience, reduce unnecessary costs and broaden the coverage of potential users who can verify their identity with them.

Equally, the requirements for authentication are specified in terms of high level requirements and this again provides flexibility for identity providers to innovate through the use of, for example, apps and mobile phone fingerprint readers for local biometric checks.



The federated architecture is also a privacy-enhancing feature and this may be important for contexts where national identity systems are uncommon or where levels of distrust in government are high.

Federated architectures also minimise the risks associated with holding all identity data in a single entity, where the consequences of a data breach can be significant (e.g., Leyden 2016a, 2016b, 2016c; Thomson 2015).

## **5. Using Open Standards and Ensuring Vendor and Technology Neutrality**

A recent Parliamentary report has described the UK government's overall record in developing and implementing new systems as "appalling" (Public Administration Select Committee 2011) with the problems arising from two main factors: a lack of technology skills in government and an over-reliance on "contracting out" technology to a limited number of suppliers (Institute for Government 2011).

In many cases, Government outsourcing activities resulted in bespoke systems that effectively lock-in government to a small number of suppliers. This is particularly perplexing given that many of the services offered by government whilst large (population) scale are actually fairly standard commodity items that could be procured from the open market.

Verify therefore focuses specifically on open standards and does everything it can to minimise the risks of vendor and technology lock-in. Thus, the certified companies are expected to offer identity proofing and authentication services to the standard of GPG45 rather than specific technological fixes. Similarly, there are specific provisions around the role and scope of the material sub-contractors that seek to ensure that despite an apparent marketplace in certified companies they are not all reliant on a small number of companies to provide key aspects of the identity proofing process (GOV.UK Verify 2014i).

Another example of how Verify is moving towards vendor neutrality can be seen from the case where Verizon was dropped as a certified company (Merrett 2016c). As the government had a marketplace of identity providers, it demonstrated that it was not reliant on particular vendors. Additionally, the form of the contracts that the identity providers sign as part of the framework agreement (GOV.UK Verify 2014e) mean that prices are stable over the period of the agreement.

## **6. Protecting User Privacy and Control through System Design**

The new EU GDPR requires that companies design privacy compliant policies, procedures and systems from the outset. However, there is also widespread recognition that it is costly to bolt privacy protections onto an existing system. It therefore makes sense, particularly when moving towards new digital identity systems, to include privacy considerations throughout the development process. This involves consideration of technological decisions

about what data to collect and share as well as the legal environment within which the identity system operates (Nyst et al. 2016).

As Verify is a brand-new system that has been designed and built from scratch, it is based on a privacy enhancing architecture. In other contexts, building on existing legacy systems, possible changes to the architecture may be more constrained unless the move to a digital identity also involves a more fundamental business process transformation as well.

Privacy-by-design goes beyond the technical architecture and Verify provides an exemplar for how privacy principles can be used to shape the norms associated with a digital identity system, including how privacy principles can be embedded into contractual considerations with providers of identity services.

Finally, the role of PCAG in the overall governance of the Verify scheme is worth noting. As well as developing the privacy principles PCAG illustrates how a government service can engage effectively with independent privacy experts and consumer advocates.

## **7. Planning for Financial and Operational Sustainability without Compromising Accessibility**

In many cases, the funding and charging for identity systems is unclear. Is the identity system a basic part of the nation's infrastructure that should be paid for by centrally, or is it providing a service that should be funded, at least in part, by the service's "users" (and if so, are the "users" the individuals who are accessing government services or the government services who are consuming the identities?).

In the case of Verify, as the business case (GOV.UK Verify 2015d) indicates, Verify is partly paid for centrally and partly by the government services consuming the identities. Verify is seen as a key part of the government's infrastructure and, as such, is supported centrally. Moreover, it seeks to avoid unnecessary duplication in terms of government procurement by having GDS as the sole contracting authority for identity related services. This also helps the user experience as they only have to provide their identity evidence package once before using Verify on a range of services.

Verify charges government services providers who will use Verify'd identities a fixed fee for the number of identities they interact with per year (GOV.UK Verify 2017d, sec. 4) rather than on a per-transaction basis. This will help ensure that proper authentication (and back-end ongoing identity proofing) takes place on all transactions as there is no additional cost to using Verify throughout the year.

## **8. Safeguarding Data Privacy, Security, and User Rights through a Comprehensive Legal and Regulatory Framework**

As is discussed above, a key feature of Verify was its explicit consideration of privacy and consumer rights in terms of the system's technical architecture and governance approach,

e.g., the PCAG identity assurance principles. Verify operates in the context of the UK's Data Protection Act and the EU GDPR. It also operates in a legal environment where contractual arrangements (e.g., between government and the certified companies) are strongly enforced and user data protection rights are overseen by the Information Commissioner's office.

## **9. Establishing Clear Institutional Mandates and Accountability**

The institutional mandates for Verify can be found across a range of government policy documents, ranging from the election manifesto of the current government (Conservative Party 2017) to the UK digital strategy (GOV.UK 2017b). These documents provide clear support for Verify as the identity solution for accessing UK government services online as well as presenting Verify for use by private sector organisations as well.

The discussion of Verify's governance arrangements in Section D provides information about the oversight and accountability for Verify, for example, demonstrating how security considerations for Verify feed into pan government security accreditation.

## **10. Enforcing Legal and Trust Frameworks through Independent Oversight and Adjudication of Grievances**

Given the central role of the user experience in Verify, a key feature of the PCAG principles relates to dispute resolution. If users face problems, for example in obtaining a Verify'd identity or in accessing an online government service, it is important that they know where they can go to get support. In the first instance this is likely to be with the certified company they are using to provide their Verify'd identity. However, in some cases they may want to contact the Verify team directly or even the government department whose service they are trying to access.

## **Functional? Foundational? What Verify Is and Isn't**

Gelb and Clark (2013) distinguish between foundational and functional identity systems. Foundational identity systems are typically those based on core identity systems such as civil registration systems and national identity card systems. Functional identity systems, in contrast, are typically created for specific (functional) purposes such as voting, health insurance etc. In some cases, foundational systems can be used for functional purposes but all too often they sit alongside (and replicate) functional systems resulting in unnecessary duplication of effort and a poor user experience. On this basis, Verify is closer to a foundational identity system than a functional one. In particular, the Verify once, use often approach allows the same (now foundational?) Verify'd identity to be used for a growing range of functions.

The work that Verify is undertaking with, for example, local authorities helps highlight the relationship between a Verify'd identity and the attributes needed for many functional systems. For example, concessionary travel for elderly people needs only to be based on attributes of an individual (are they old enough to be entitled to the concessionary travel?)

rather than their identity per se. Other attributes that enable important functional systems might include citizenship, eligibility to vote, low income status or “settled status” for EU citizens post BREXIT (GOV.UK 2017e).

There are clear savings to be made, however, by linking these attributes to a Verify’d identity (or equivalent foundational identity) rather than seeking to build functional systems around their own identity evidence.

Foundational systems are often derived from civil registry data and, in many economies, the birth registration record is the basis of the identity credential. In the case of Verify, civil registration data can form the basis of a Verify’d identity, but the identity proofing and verification standards used allow for alternative identity evidence to be used instead. As noted above, this is partly because of the proactive anti-fraud processes associated with identity verification, given the relatively high levels of assurance required by Verify. Additionally, because Verify is about enabling access to online government services, there is an explicit need to allow residents to be able to access these services alongside citizens. That is, an identity system should be built for everyone in a nation rather than being a system for nationals. Data about residents, as opposed to citizens, is unlikely to be found in national civil registration systems and so, on this basis Verify appears to be less of a foundational system.

Another way of considering what Verify is and isn’t relates to the notion of legal identity, a key feature of UN Sustainable Development Goal 16.9 (“provide legal identity for all, including birth registration”). This ambiguous goal (Whitley and Manby 2015) highlights the importance of birth registration (one kind of identity evidence for Verify) in relation to the nebulous notion of “legal identity.” In the context of access to online government services, however, a Verify’d identity satisfies a functional interpretation of legal identity, namely an identity that is recognised as being of sufficient quality to access online government services, i.e., a legally operational identity (LOID) (cf BCS Identity Assurance Working Group 2016). Moreover, a LoA2 Verify’d identity not just acceptable for operational purposes it is also based on identity evidence that satisfies the standards required for civil legal proceedings.

This suggests, in a manner analogous to the BCS evaluation of good identity systems, shifting the debate from what an identity is to the conditions that determine when and how an identity can be used for real world transactions.

## **G. Appendices**

### **Appendix 1. Glossary and Abbreviations**

**A/B Testing:** A process whereby users are randomly shown alternative (A or B) interfaces or user experiences and the levels of user satisfaction are measured. This helps refine the best interface/user experience

**API:** Application Programming Interfaces are standards that allow software components to interact and exchange data without needing full access to the underlying data sources

**Authentication:** This is the process of asserting an identity previously established during identification

**Certified companies:** These are the companies that have a contractual agreement with GOV.UK Verify to provide identity assurance services. They must be members of an accredited Scheme (t-Scheme) and have successfully completed a rigorous onboarding process. Currently these are Barclays, CitizenSafe, Digidentity, Experian, Post Office, Royal Mail and SecureIdentity

**DEFRA:** Department for Environment, Food and Rural Affairs. Handles Common Agricultural Policy information service and other rural payments

**DVLA:** Driver and Vehicle Licensing Agency. Handles all driving licence information

**DVSA** Driver and Vehicle Standards Agency. Administers driving tests, approves driving instructors and MOT testers.

**DWP:** Department of Work and Pensions. Responsible for pensions and other social welfare payments

**Government Service Provider:** The government departments that act as relying parties for Verify. Currently they are DEFRA, DVLA, DVSA, DWP, HM Land Registry, HM Revenue and Customs, Home Office and the Insolvency Service

**GPG:** Good Practice Guide

**GDPR:** General Data Protection Regulation

**GDS:** Government Digital Service

**HMRC:** HM Revenue and Customs. Responsible for tax, payments and customs activities

**Hub:** Privacy enhancing feature of the Verify architecture that sits between identity providers and service providers

**Identity evidence package:** A set of identity evidence presented in support of a claimed identity

**Identity evidence profile:** Scoring of the identity evidence package against the Identity Proofing and Verification standards

**Identity proofing and verification:** The process of assuring the identity claims made by an individual

**Identity providers:** A more general term for the certified companies

**KYC:** “Know your customer.” The identity proofing and verification checks required, typically, when opening a bank or financial product account

**Level of Assurance:** The assurance associated with a particular Verify’d identity. Most services currently using Verify currently use an LoA2 Verify’d identity.

**LoA:** Level of Assurance

**Matching data service:** The service that matches the matching data set sent from the Hub with the records held by the service provider

**Matching data set:** A minimal set of personal data used by the matching data service. The data set consists of full name, address, date of birth, optionally gender, history of attributes and the associated assertion of level of assurance (currently only LoA2)

**Relying party:** A more general term for Service Providers

**SAML:** Security Assertion Markup Language. An open standard data format for exchanging authentication and authorization data between parties. It is based on XML the extensible markup language

**SIRO:** Senior Information Risk Owner

**User:** The data subject about whom identity claims relate

**Verify model:** The four distinctive features of Verify: A risk- and standards-based approach to identity verification and authentication; A federated architecture involving multiple identity providers that encourages innovation in both verification and authentication activities; A privacy-by-design approach that embeds privacy principles in contracts and norms and includes expert oversight of privacy and consumer issues; and A user focussed service delivery approach that includes an emphasis on transparency and engagement with all relevant stakeholders

**Verify’d identity:** An identity that has satisfied the identity proofing and verification standards, for example, to LoA2

## Appendix 2. Historical Background to Verify

This section draws on (Whitley et al. 2014; Whitley and Hosein 2010a).

According to Agar (2005), the first ever attempt at a national identity card and population register in the UK was a failure. The programme was introduced during the First World War as a means of determining the extent of the male population in the country. Existing government records were considered incomplete and ineffective for the purposes of developing a policy for conscription. Once the count was completed and the government knew how many men were available to serve, political interest in national registration and identification cards waned and the system was soon abandoned.

However, as Agar notes, the promise of a national identification system was not forgotten by the civil service, who during the Second World War re-introduced the idea of identity cards, primarily as a way of identifying aliens and managing the allocation of food rations.

Crucial to the operation of the second National Register was its intimate connection to the organisation of food rationing. In order to renew a ration book, an identity card would have to be produced for inspection at a local office at regular intervals. Those without an identity card, would within a short period of time no longer be able, legally, to claim rationed food. This intimate connection between two immense administrative systems was vital to the success of the second card—they were not forgotten by members of the public—and provides one of the main historical lessons (Agar 2005).

As identity cards became a facet of everyday life, they started being used for additional purposes (i.e., they were subject to ‘function creep’), including identity checks by police officers. This use continued even after the war was over. Liberal-minded citizens eventually began to question these practices and, in 1950, one such citizen, Clarence Willcock, disputed the police’s routine check of identity cards. Willcock’s legal challenges were not successful, but in the case’s written judgment Lord Goddard (the Lord Chief Justice) criticised the police for abusing identity cards. By 1952 Parliament had repealed the legislative basis for the national identity card and it disappeared from use.

As many observers have noted since that time the civil service and politicians have been regularly captivated by the idea of re-introducing national identity cards in the UK, with the aim of solving a diversity of policy problems, ranging from streamlining tax administration to ‘fixing’ the immigration ‘problem’, among others. By the early 2000s they had tried again.

In 2002, the Labour government, under Prime Minister Tony Blair and with David Blunkett serving as Home Secretary, proposed a new national ‘entitlement card’ scheme. This proposal was then re-branded as a national ‘identity card’ scheme in 2004. Following the 2005 general election in the UK (in which the Labour party was again re-elected to government) the updated proposals were introduced to Parliament in the form of a National Identity Scheme.

In June 2005, a research group based at the London School of Economics (which the author of this report was an integral part of) issued a detailed report that critically analysed the government's proposals (LSE Identity Project 2005). The LSE researchers suggested that the likely cost of the Scheme was far higher than government estimates, evaluated the likely technology solutions and the likely challenges in deploying these technologies and identified focal points around the policy that would likely give rise to privacy and surveillance concerns. This led to widespread, mostly negative, media coverage of the proposed scheme (Pieri 2009) around these lines of criticism and most notably the costs of the scheme; while the Parliamentary debate was fuelled by data and analyses from the LSE report (Whitley 2014).

Despite these concerns, Parliament passed the Identity Cards Act 2006 on 30 March, thus enabling the first national identity card programme in the UK since World War II.

This new Scheme was different from previous ones in several important ways. The proposals called for a system of unprecedented size for that time and complexity, comprising a centralised National Identity Register (the electronic database on which the population's identity data would be held) and the collection and recording of over 50 pieces of personal information from individuals, including most notably the collection and use of the biometric information of UK citizens and residents both for enrolment (to ensure that no individual was entered onto the Register more than once) and verification, the proposed use of a single identification number across government and the private sector (Otjacques et al. 2007) and an 'audit trail' that was expected to record details of every instance that an identity was verified against information stored on the Register.<sup>2</sup>

Even once Parliament had formally approved the Scheme and created the new Identity and Passport Service from the previous Passport Agency, the government's plans did not run smoothly. In July 2006, leaked e-mails from senior civil servants warning about ongoing risks to the Scheme were published on the front page of a major newspaper (The Sunday Times 2006a, 2006b). Shortly thereafter, the new Home Secretary (the third in as many years and the third overseeing this policy) ordered a wholesale review of the plans for the Scheme given worries that many parts of his department were "not fit for purpose." This review resulted in the Strategic Action Plan issued in December 2006 (UKIPS 2006) that sought to reduce the risks, and costs, of the Scheme.

Another significant event that affected the government's plans was the announcement by the then Chancellor Alistair Darling, on 20 November 2007, that a data breach involving "personal data relating to child benefit" had arisen in HM Revenue and Customs (HMRC) [Hansard 20 November 2007: Column 1101-]. On 18 October 2007, in response to a request from the National Audit Office (NAO) for data in relation to payment of child benefit, a civil servant at HMRC sent a full copy of the data on two password-protected compact discs, using an obsolete version of compression software with weak encryption.

---

<sup>2</sup> This requirement for a personal audit trail would prove to be particularly controversial amongst activists, who viewed it as a dangerous surveillance device.



The discs were sent using the HMRC's internal mail service, operated by TNT. The package was not recorded or registered and failed to arrive at the NAO. When the requested discs did not arrive, a second set of discs was sent, this time by recorded delivery. These did arrive.

The discs, containing details of all child benefit recipients—records for 25 million individuals and 7.25 million families—have still not been recovered. The records included the names of recipients as well as their children, address details and dates of birth, child benefit numbers, national insurance numbers and, where relevant, bank or building society account details.

Unsurprisingly, public trust in the government's ability to keep personal data secure was negatively affected by this news and the implications for the National Identity Scheme were widely reported. Surveys by campaign groups opposed to identity cards, as well as those organised by the Home Office, demonstrated falling levels of trust in the government's plans to implement identity cards.

In the run-up to the 2010 general election, opposition parties in the UK began to articulate the basis of their concerns with the government's identity policy, as embodied in the National Identity Scheme and to build on the falling support for the government's plans. For the Conservative Party, the identity card scheme became part of a broader narrative that presented the government's policy as creating a surveillance state, a policy that needed to be reversed (Conservatives 2009). This reversal began with the belief that personal information belongs to the citizen—not the state—and where government collects private details, they are held on trust. As a result, the Conservative Party's logic was that the government must be held accountable to its citizens, not the other way around (Conservatives 2009).

In their 2010 election manifesto, this goal of introducing measures “to protect personal privacy and hold government to account” became an espoused part of the Conservative Party policy agenda, under the heading “Protect our freedoms”:

Labour's approach to our personal privacy is the worst of all worlds—  
intrusive, ineffective and enormously expensive. We will scrap ID cards, the  
National Identity Register and the Contactpoint database (Conservative  
Party 2010).

The third major political party, the Liberal Democrats, also reiterated its longstanding opposition to identity cards. Their manifesto noted that:

increasing use of sophisticated technology, whilst bringing undoubted  
benefits to society, also poses new threats to individual liberty, particularly  
in relation to Identity Cards. The Liberal Party opposes the introduction of  
any form of national Identity Card, whether voluntary or compulsory  
(Liberal Democrats 2010).

By the time of the general election, every political party other than the Labour party had

included proposals to scrap identity cards as part of their election manifestos (Whitley and Hosein 2010b).

In the 2010 election, no single party won an overall majority and, after a period of negotiation and speculation about whether one party might try to operate a minority government, a coalition between the Conservative and Liberal Democrat parties was announced. Perhaps unsurprisingly, a key feature of the joint ‘Coalition Agreement’, announced on 11 May 2010, was plans:

to implement a full programme of measures to reverse the substantial erosion of civil liberties under the Labour Government and roll back state intrusion.

This will include:

\* A Freedom or Great Repeal Bill

\* The scrapping of ID card scheme, the National Identity register, the next generation of biometric passports and the Contact Point Database (Conservative Liberal Democrat coalition negotiations 2010).

The first piece of legislation introduced by the new Coalition Government (“Bill 1 of 2010–11”) was the “Identity Documents Bill,” which was “A Bill to make provision for and in connection with the repeal of the Identity Cards Act 2006.” Passage of the Bill took longer than the government had anticipated partly because of counter proposals made by the Labour Party to compensate those citizens who had paid for identity cards that were about to be revoked. The Bill received Royal Assent on 21 December 2010, at which point the identity cards ceased to have legal status. On 10 February 2011, Home Office minister Damian Green marked the end of the identity card scheme by feeding its drives into an industrial shredder in Essex (Mathieson 2013).

While scrapping the unloved National Identity Scheme and even physically grinding to dust key hardware components of the system, provides an important symbolic moment in the short history of this identity policy, it did not resolve questions of how individuals can feasibly identify themselves in order to gain access to services. The challenge of an effective identity policy did not go away with a new government. In particular, government services still needed to have confidence in the people they are interacting with and citizens need to have trust in the identity system they must to use to interact with government.

For many years, identity verification in the UK has been based on a rather haphazard mix of official documents with passports and driving licences being used to confirm someone’s name and utility bills or existence on the electoral roll being used to confirm address details. Although some checking services exist, for example, a commercial passport verification service or using the utility meter reference number on the utility bill to compare the address of the meter with the claimed address on the bill, these were rarely used. Indeed, even a

former Attorney General was caught out (and fined) over incomplete identity checks and record keeping (Bingham and Prince 2009).

This approach was particularly susceptible risks of compromised breeder documents feeding the whole process (Collings 2008). Moreover, it was hardly conducive to Government's intention to move many services online and operate them securely and it is from this context that the Verify model emerged.

## H. References

All URLs checked 4 July 2018.

- Abraham, R., Bennett, E. S., Sen, N., and Shah, N. B. (2017). State of Aadhaar Report 2016-17, *IDInsight* (available at <http://stateofaadhaar.in/wp-content/uploads/State-of-Aadhaar-Full-Report-2016-17-IDinsight.pdf>).
- Agar, J. (2005). Identity cards in Britain: past experience and policy implications, *History and Policy* (available at <http://www.historyandpolicy.org/papers/policy-paper-33.html>).
- Ashford, W. (2015). Experian chooses UK authentication startup for GOV.UK Verify, *Computer Weekly* (available at <http://www.computerweekly.com/news/4500260479/Experian-chooses-UK-authentication-startup-for-GovUK-Verify>).
- BBC News (2005). “Third” of DVLA car records wrong, (available at <http://news.bbc.co.uk/1/hi/uk/4214281.stm>).
- BBC News (2016). Taxpayers turn to online returns, says HMRC, (available at <http://www.bbc.co.uk/news/business-35458297>).
- BCS Identity Assurance Working Group (2016). Aspects of Identity Yearbook 2015-16: How to recognise a good online identity scheme, (available at [https://policy.bcs.org/sites/policy.bcs.org/files/Aspects%20of%20Identity\\_2015-16\\_A4%204pp\\_WEB.pdf](https://policy.bcs.org/sites/policy.bcs.org/files/Aspects%20of%20Identity_2015-16_A4%204pp_WEB.pdf)).
- Berghel, H. (2006). Fungible credentials and next-generation fraud, *Communications of the Acm* 49(12), 15–19.
- Bicknell, D. (2016a). Cunnington: GDS strategy expected to be out by Christmas, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/cunnington-gds-strategy-expected-to-be-out-by-christmas-5038513>).
- Bicknell, D. (2016b). Verify delays stall Britain’s progress on digital government, Euro report finds, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/verify-delays-stall-britains-progress-on-digital-government-euro-report-finds-5022064>).
- Bicknell, D. (2017). HMRC opens up on Government Gateway and identity plans, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/hmrc-opens-up-on-government-gateway-and-identity-plans-5739073>).
- Bingham, J., and Prince, R. (2009). Attorney General Baroness Scotland fined £5,000 over illegal immigrant housekeeper, *Daily Telegraph* (available at <http://www.telegraph.co.uk/news/politics/6217586/Attorney-General-Baroness-Scotland-fined-5000-over-illegal-immigrant-housekeeper.html>).
- Blackhurst, C. (1993). A third of driving licences incorrect: Wrong DVLA data “wasting police time,” *The Independent* (available at <http://www.independent.co.uk/news/uk/a-third-of-driving-licences-incorrect-wrong-dvla-data-wasting-police-time-1469036.html>).
- Brandão, L. T. A. N., Christin, N., Danezis, G., and Anonymous (2015). Toward Mending Two Nation-Scale Brokered Identification Systems, in *Proceedings on Privacy Enhancing Technologies 2015* (Vol. 2), 1–22.

- Brown, A., Fishenden, J., Thompson, M., and Venters, W. (2017). Appraising the impact and role of platform models and Government as a Platform (GaaP) in UK Government public service reform: Towards a Platform Assessment Framework (PAF), *Government Information Quarterly* 34(2), 167–182.
- Brown, G. (2006). Chancellor appoints Sir James Crosby to lead Public Private Forum on Identity, (available at [http://webarchive.nationalarchives.gov.uk/20130129110402/http://www.hm-treasury.gov.uk/press\\_51\\_06.htm](http://webarchive.nationalarchives.gov.uk/20130129110402/http://www.hm-treasury.gov.uk/press_51_06.htm)).
- Burton, G. (2017a). HMRC denies reports it plans to develop its own authentication system and dump GOV.UK Verify, *Computing.co.uk* (available at <http://www.computing.co.uk/ctg/news/3004690/hmrc-denies-reports-it-plans-to-develop-its-own-authentication-system-to-avoid-govuk-verify>).
- Burton, G. (2017b). HMRC confirms plans to develop its own authentication service rather than use GOV.UK Verify, (available at <http://www.computing.co.uk/ctg/news/3004616/hmrc-confirms-plans-to-develop-its-own-authentication-service-rather-than-use-govuk-verify>).
- Cameron, K. (2005). The laws of identity, (available at <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>).
- Cellan-Jones, R. (2017). Whitehall's identity crisis: HMRC and Verify, (available at <http://www.bbc.com/news/technology-38979144>).
- Chirgwin, R. (2016). US standards lab says SMS is no good for authentication, *The Register* (available at [http://www.theregister.co.uk/2016/07/24/nist\\_says\\_sms\\_no\\_good\\_for\\_authentication/](http://www.theregister.co.uk/2016/07/24/nist_says_sms_no_good_for_authentication/)).
- Ciborra, C. U. (2005). Interpreting e-government and development: Efficiency, transparency or governance at a distance?, *Information Technology and People* 18(3), 260–279.
- Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID), *Information security technical report* 13(2), 61–70.
- Conservative Liberal Democrat coalition negotiations (2010). Agreements reached, (available at <http://www.conservatives.com/~media/Files/Downloadable%20Files/agreement.aspx?dl=true>).
- Conservative Party (2010). Manifesto: Invitation to join the government of Britain, (available at <https://www.conservatives.com/~media/Files/Manifesto2010>).
- Conservative Party (2017). The Conservative Party Manifesto 2017, (available at <https://www.conservatives.com/manifesto>).
- Conservatives (2009). Reversing the rise of the surveillance state: 11 Measures to Protect Personal Privacy and Hold Government to Account, (available at [http://www.conservatives.com/News/News\\_stories/2009/09/Reversing\\_the\\_rise\\_of\\_the\\_surveillance\\_state.aspx](http://www.conservatives.com/News/News_stories/2009/09/Reversing_the_rise_of_the_surveillance_state.aspx)).
- Crown Commercial Services (2016). Guidance on Framework Agreements, (available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/430313/public-contracts-regulations-guidance.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/430313/public-contracts-regulations-guidance.pdf)).
- Currah, P., and Mulqueen, T. (2011). Securitizing gender: Identity, biometrics and transgender bodies at the airport, *Social research* 78(2), 557–582.

- Curren, L., and Kaye, J. (2010). Revoking consent: A “blind spot” in data protection law?, *Computer Law & Security Review* 26(3), 273–283.
- Dale, K. (2016). GOV.UK Verify - estimating demographic coverage v1.1, (available at <http://kyrandale.com/static/clients/gds/app/index.html>).
- Dale, K. (2017). GOV.UK Verify - estimating demographic coverage v2.1, (available at <http://kyrandale.com/static/clients/gds/app/verify-survey.html>).
- Easton, S. (2016). National digital identity framework prototype only weeks away, *The Mandarin* (available at <http://www.themandarin.com.au/68619-national-digital-identity-framework-prototype-only-weeks-away/>).
- European Commission (2016). Trust Services and eID - eIDAS, (available at <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>).
- Evenstad, L. (2016a). GDS loses another senior exec with departure of Gov.uk Verify’s Janet Hughes, *Computer Weekly* (available at <http://www.computerweekly.com/news/450302605/GDS-loses-another-senior-exec-with-departure-of-Govuk-Verifys-Janet-Hughes>).
- Evenstad, L. (2016b). Will Whitehall power struggle cripple Government Digital Service?, *Computer Weekly* (available at <http://www.computerweekly.com/news/450301805/Will-Whitehall-power-struggle-cripple-Government-Digital-Service>).
- Fishenden, J. (2017). GOV.UK Verify and identity assurance - it’s time for a rethink, *Computer Weekly* (available at <http://www.computerweekly.com/opinion/Govuk-Verify-and-identity-assurance-its-time-for-a-rethink>).
- Fiveash, K. (2014). Pitchforks at dawn! UK gov’s Verify ID service FAILS to verify ID, (available at [http://www.theregister.co.uk/2014/11/02/gov\\_uk\\_verify\\_id\\_assurance\\_experian\\_defra\\_test\\_failure/](http://www.theregister.co.uk/2014/11/02/gov_uk_verify_id_assurance_experian_defra_test_failure/)).
- Fiveash, K. (2017). HMRC gingerly rows back on GDS Verify identity system snub, *Arx Technica* (available at <https://arstechnica.com/tech-policy/2017/02/hmrc-gds-verify-government-gateway-identity/>).
- Gal, U. (2016). Data surveillance is all around us, and it’s going to change our behaviour, *The Conversation* (available at <http://theconversation.com/data-surveillance-is-all-around-us-and-its-going-to-change-our-behaviour-65323>).
- GDS (2016a). Using mob programming to solve a problem, (available at <https://gds.blog.gov.uk/2016/09/01/using-mob-programming-to-solve-a-problem/>).
- GDS (2016b). Welcoming our new minister, (available at <https://gds.blog.gov.uk/2016/09/16/welcoming-our-new-minister/>).
- GDS (2016c). Kevin says hello, (available at <https://gds.blog.gov.uk/2016/08/04/kevin-says-hello/>).
- GDS (2016d). The GDS mission: support, enable and assure, (available at <https://gds.blog.gov.uk/2016/10/26/the-gds-mission-support-enable-and-assure/>).
- GDS (2016e). Introducing the GDS International team, (available at <https://gds.blog.gov.uk/2016/08/23/introducing-the-gds-international-team/>).
- GDS (2017a). Government Transformation Strategy, *GDS* (available at <https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy>).

- GDS (2017b). What you can learn from making data user-centred?, (available at <https://gds.blog.gov.uk/2017/01/31/what-you-can-learn-from-making-data-user-centred/>).
- GDS (2017c). New minister pays a visit to GDS's new HQ, (available at <https://gds.blog.gov.uk/2017/06/28/new-minister-pays-a-visit-to-gdss-new-hq/>).
- GDS (2017d). The Government Transformation Strategy 2017 to 2020, *GDS* (available at <https://gds.blog.gov.uk/2017/02/09/the-government-transformation-strategy-2017-to-2020/>).
- GDS (2018a). Digital Service Standard - Digital Service Manual, (available at <https://www.gov.uk/service-manual/service-standard>).
- GDS (2018b). Service design phases — Government Service Design Manual, (available at <https://www.gov.uk/service-manual/phases>).
- GDS (2018c). Our governance - Government Digital Service, (available at <https://www.gov.uk/government/organisations/government-digital-service/about/our-governance>).
- Gelb, A., and Clark, J. (2013). Identification for Development: The Biometrics Revolution - Working Paper 315, *Centre for Global Development* (available at <http://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315>).
- Gelb, A., and Diofasi, A. (2016). Biometric Elections in Poor Countries: Wasteful or a Worthwhile Investment? - Working Paper 435, *Centre for Global Development* (available at <http://www.cgdev.org/publication/biometric-elections-poor-countries-wasteful-or-worthwhile-investment>).
- Gelb, A., and Manby, B. (2016). Has Development Converged with Human Rights? Implications for the Legal Identity SDG, *Centre for Global Development* (available at <http://www.cgdev.org/blog/has-development-converged-human-rights-implications-legal-identity-sdg>).
- Glick, B. (2016a). DWP digital experts brought in to help assess plans for Government Digital Service, *Computer Weekly* (available at <http://www.computerweekly.com/news/450302866/DWP-digital-experts-brought-in-to-help-assess-plans-for-Government-Digital-Service>).
- Glick, B. (2016b). Interview: Kevin Cunnington, director general, Government Digital Service, *Computer Weekly* (available at <http://www.computerweekly.com/news/450401508/Interview-Kevin-Cunnington-director-general-Government-Digital-Service>).
- Glick, B. (2017a). GOV.UK Verify fails to meet key business case targets, *Computer Weekly* (available at <http://www.computerweekly.com/news/450424217/Govuk-Verify-fails-to-meet-key-business-case-targets>).
- Glick, B. (2017b). GDS, HMRC and Verify: so much for cross-government digital collaboration, *Computer Weekly* (available at <http://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/GDS-HMRC-and-Verify-so-much-for-cross-government-digital-collaboration>).
- Glick, B. (2017c). Ex-government privacy advisor calls for “fundamental review” of GOV.UK Verify identity scheme, *Computer Weekly* (available at

- <http://www.computerweekly.com/news/450418300/Ex-government-privacy-advisor-calls-for-fundamental-review-of-Govuk-Verify-identity-scheme>).
- GOV.UK (2012). Requirements for secure delivery of online public services, (available at <https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services>).
- GOV.UK (2013). Identity assurance: organisation identity, (available at <https://www.gov.uk/government/publications/identity-assurance-organisation-identity>).
- GOV.UK (2014). Authentication credentials for online government services, (available at <https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services>).
- GOV.UK (2015a). Spending review and autumn statement 2015 - GOV.UK, (available at <https://www.gov.uk/government/publications/spending-review-and-autumn-statement-2015-documents/spending-review-and-autumn-statement-2015>).
- GOV.UK (2015b). Cabinet Office settlement at the Spending Review 2015 - Press releases, (available at <https://www.gov.uk/government/news/cabinet-office-settlement-at-the-spending-review-2015>).
- GOV.UK (2015c). Buying goods and services: options for public sector buyers - Detailed guidance, (available at <https://www.gov.uk/guidance/buying-goods-and-services-options-for-public-sector-buyers>).
- GOV.UK (2017a). Part 6. Digital government - maintaining the UK government as a world leader in serving its citizens online, *UK Digital Strategy* (available at <https://www.gov.uk/government/publications/uk-digital-strategy/6-digital-government-maintaining-the-uk-government-as-a-world-leader-in-serving-its-citizens-online>).
- GOV.UK (2017b). UK Digital Strategy, (available at <https://www.gov.uk/government/publications/uk-digital-strategy>).
- GOV.UK (2017c). New Data Protection Bill: Our planned reforms, (available at <https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views>).
- GOV.UK (2017d). The exchange and protection of personal data - a future partnership paper, (available at <https://www.gov.uk/government/publications/the-exchange-and-protection-of-personal-data-a-future-partnership-paper>).
- GOV.UK (2017e). Safeguarding the position of EU citizens in the UK and UK nationals in the EU, (available at <https://www.gov.uk/government/publications/safeguarding-the-position-of-eu-citizens-in-the-uk-and-uk-nationals-in-the-eu>).
- GOV.UK (2018a). Identity proofing and verification of an individual, (available at <https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual>).
- GOV.UK (2018b). Government as a Platform, (available at <https://www.gov.uk/government/policies/government-as-a-platform>).
- GOV.UK (2018c). Change the address on your driving licence, (available at <https://www.gov.uk/change-address-driving-licence>).
- GOV.UK Verify (2013a). Privacy and Consumer Advisory Group: Draft Identity Assurance Principles, (available at <https://www.gov.uk/government/consultations/draft-identity->



- assurance-principles/privacy-and-consumer-advisory-group-draft-identity-assurance-principles).
- GOV.UK Verify (2013b). Identity Assurance Hub Service SAML 2.0 Profile, (available at <https://www.gov.uk/government/publications/identity-assurance-hub-service-saml-20-profile>).
- GOV.UK Verify (2014a). Identity Assurance Principles, No. Version 3.1, (available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/361496/PCAG\\_IDA\\_Principles\\_3.1\\_\\_4\\_.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf)).
- GOV.UK Verify (2014b). GOV.UK Verify: checks identity providers must perform - Detailed guidance, (available at <https://www.gov.uk/guidance/govuk-verify-checks-identity-providers-must-perform>).
- GOV.UK Verify (2014c). GOV.UK Verify: IPV Operations Manual (redacted), No. 2.3.1, (available at <https://www.gov.uk/government/publications/govuk-verify-ipv-operations-manual-redacted>).
- GOV.UK Verify (2014d). Identity assurance, procurement 2, (available at <https://identityassurance.blog.gov.uk/2014/04/04/identity-assurance-procurement-2/>).
- GOV.UK Verify (2014e). EU Tender document, *Services - 428146-2014 - TED Tenders Electronic Daily* (available at <http://ted.europa.eu/udl?uri=TED:NOTICE:428146-2014:TEXT:EN:HTML&tabId=1>).
- GOV.UK Verify (2014f). How we use open source code on the identity assurance programme, (available at <https://identityassurance.blog.gov.uk/2014/10/09/how-we-use-open-source-code-on-the-identity-assurance-programme/>).
- GOV.UK Verify (2014g). What we're doing to help teams across government use GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2014/11/19/what-were-doing-to-help-teams-across-government-use-gov-uk-verify/>).
- GOV.UK Verify (2014h). What it means to be a “certified company,” (available at <https://identityassurance.blog.gov.uk/2014/12/11/what-it-means-to-be-a-certified-company/>).
- GOV.UK Verify (2014i). Making sure we have a range of certified companies, (available at <https://identityassurance.blog.gov.uk/2014/12/10/making-sure-we-have-a-range-of-certified-companies/>).
- GOV.UK Verify (2015a). Privacy and Consumer Advisory Group, Terms of Reference, (available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/448101/IDA\\_Privacy\\_and\\_Consumer\\_Advisory\\_Group\\_-\\_ToR\\_PDF.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/448101/IDA_Privacy_and_Consumer_Advisory_Group_-_ToR_PDF.pdf)).
- GOV.UK Verify (2015b). Making GOV.UK Verify available to more people, (available at <https://identityassurance.blog.gov.uk/2015/10/20/making-gov-uk-verify-available-to-more-people/>).
- GOV.UK Verify (2015c). GOV.UK Verify Hub - privacy aspects, (available at <https://identityassurance.blog.gov.uk/2015/06/22/gov-uk-verify-hub-privacy-aspects/>).
- GOV.UK Verify (2015d). GOV.UK Verify Programme Business Case (Redacted),.
- GOV.UK Verify (2015e). Basic identity accounts trial | GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2015/06/11/basic-identity-accounts-trial/>).

- GOV.UK Verify (2015f). Guest post by Lee Croucher: 3 things departments should know about joining GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2015/12/04/guest-post-3-things-departments-should-know-about-joining-gov-uk-verify/>).
- GOV.UK Verify (2015g). GOV.UK Verify and Mydex CIC, (available at <https://identityassurance.blog.gov.uk/2015/03/25/gov-uk-verify-and-mydex/>).
- GOV.UK Verify (2015h). Identity Assurance Hub Service Profile: Authentication Contexts, (available at <https://www.gov.uk/government/publications/identity-assurance-hub-service-profile-authentication-contexts>).
- GOV.UK Verify (2015i). Identity Assurance Hub Service Profile: SAML Attributes, (available at <https://www.gov.uk/government/publications/identity-assurance-hub-service-profile-saml-attributes>).
- GOV.UK Verify (2015j). The basis of trust for EU identity assurance, (available at <https://identityassurance.blog.gov.uk/2015/12/14/the-basis-of-trust-for-eu-identity-assurance/>).
- GOV.UK Verify (2015k). The EU approach to identity assurance: an update, (available at <https://identityassurance.blog.gov.uk/2015/11/20/the-eu-approach-to-identity-assurance-an-update/>).
- GOV.UK Verify (2016a). How we introduce GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/08/17/how-we-introduce-gov-uk-verify/>).
- GOV.UK Verify (2016b). Introducing our first #VerifyLocal pilot plans for local councils, (available at <https://identityassurance.blog.gov.uk/2016/09/08/introducing-our-first-verifylocal-pilot-plans-for-local-councils/>).
- GOV.UK Verify (2016c). GOV.UK Verify: Technical delivery update, 12 July 2016, (available at <https://identityassurance.blog.gov.uk/2016/07/12/gov-uk-verify-technical-delivery-update-12-july-2016/>).
- GOV.UK Verify (2016d). GOV.UK Verify: understanding who can be verified, (available at <https://gds.blog.gov.uk/2016/01/25/gov-uk-verify-understanding-who-can-be-verified/>).
- GOV.UK Verify (2016e). Can online activity history help GOV.UK Verify work for more people?, (available at <https://identityassurance.blog.gov.uk/2016/07/25/can-online-activity-history-help-gov-uk-verify-work-for-more-people/>).
- GOV.UK Verify (2016f). Making GOV.UK Verify the default way to access digital services, (available at <https://identityassurance.blog.gov.uk/2016/03/14/making-gov-uk-verify-the-default-way-to-access-digital-services/>).
- GOV.UK Verify (2016g). Estimating what proportion of the public will be able to use GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/01/25/estimating-what-proportion-of-the-public-will-be-able-to-use-gov-uk-verify/>).
- GOV.UK Verify (2016h). Improving GOV.UK Verify's demographic coverage - an update, (available at <https://identityassurance.blog.gov.uk/2016/08/19/improving-gov-uk-verify-demographic-coverage-an-update/>).
- GOV.UK Verify (2016i). Accreditation and risk management in GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/04/04/accreditation-and-risk-management-in-gov-uk-verify/>).

- GOV.UK Verify (2016j). Building GOV.UK Verify to Agile principles, (available at <https://identityassurance.blog.gov.uk/2016/06/03/building-gov-uk-verify-to-agile-principles/>).
- GOV.UK Verify (2016k). Goals, cycles and people: running an agile, complex programme in government, (available at <https://identityassurance.blog.gov.uk/2016/03/11/goals-cycles-and-people-running-an-agile-complex-programme-in-government/>).
- GOV.UK Verify (2016l). Meeting user needs, (available at <https://identityassurance.blog.gov.uk/2016/02/29/meeting-user-needs/>).
- GOV.UK Verify (2016m). GOV.UK Verify: Technical delivery update, 13 September 2016, (available at <https://identityassurance.blog.gov.uk/2016/09/13/gov-uk-verify-technical-delivery-update-13-september-2016/>).
- GOV.UK Verify (2016n). 100 rounds of user research on GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/08/02/100-rounds-of-user-research-on-gov-uk-verify/>).
- GOV.UK Verify (2016o). Experimenting with mob programming to rebuild the GOV.UK Verify frontend, (available at <https://identityassurance.blog.gov.uk/2016/02/26/experimenting-with-mob-programming-to-rebuild-the-gov-uk-verify-frontend/>).
- GOV.UK Verify (2016p). The technical team working together through group learning, (available at <https://identityassurance.blog.gov.uk/2016/09/16/the-technical-team-working-together-through-group-learning/>).
- GOV.UK Verify (2016q). Releasing safe and useful code for GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/04/07/releasing-safe-and-useful-code-for-gov-uk-verify/>).
- GOV.UK Verify (2016r). Supporting Welsh language users of GOV.UK Verify / Cefnogi defnyddwyr GOV.UK Verify drwy gyfrwng y Gymraeg, (available at <https://identityassurance.blog.gov.uk/2016/04/08/supporting-welsh-language-users-of-gov-uk-verify-cefnogi-defnyddwyr-gov-uk-verify-drwy-gyfrwng-y-gymraeg/>).
- GOV.UK Verify (2016s). GOV.UK Verify Onboarding Guide, (available at <http://alphagov.github.io/identity-assurance-documentation/>).
- GOV.UK Verify (2016t). A lesson from GOV.UK Verify: blog your way towards live, (available at <https://identityassurance.blog.gov.uk/2016/07/14/a-lesson-from-gov-uk-verify-blog-your-way-towards-live/>).
- GOV.UK Verify (2016u). GOV.UK Verify support: assisting users in their journey, (available at <https://identityassurance.blog.gov.uk/2016/09/01/gov-uk-verify-support-assisting-users-in-their-journey/>).
- GOV.UK Verify (2016v). Privacy assessment in public beta, (available at <https://identityassurance.blog.gov.uk/2016/05/19/privacy-assessment-in-public-beta/>).
- GOV.UK Verify (2016w). GOV.UK Verify Data Protection Impact Assessment, (available at <https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf>).
- GOV.UK Verify (2016x). A new phase for GOV.UK Verify, (available at <https://identityassurance.blog.gov.uk/2016/08/16/a-new-phase-for-gov-uk-verify/>).

- GOV.UK Verify (2016y). How we manage fraud and information security risk, (available at <https://identityassurance.blog.gov.uk/2016/01/18/how-we-manage-fraud-and-information-security-risk/>).
- GOV.UK Verify (2016z). Planning for the event of GOV.UK Verify being taken temporarily offline, (available at <https://identityassurance.blog.gov.uk/2016/04/01/planning-for-the-event-of-gov-uk-verify-being-taken-temporarily-offline/>).
- GOV.UK Verify (2016aa). GOV.UK Verify: Update on progress August 2016, (available at <https://identityassurance.blog.gov.uk/2016/08/22/gov-uk-verify-update-on-progress-august-2016/>).
- GOV.UK Verify (2016ab). GOV.UK Verify for local government: working out loud, (available at <https://identityassurance.blog.gov.uk/2016/07/11/gov-uk-verify-for-local-government-working-out-loud/>).
- GOV.UK Verify (2016ac). GOV.UK Verify for local government: outputs of our first discovery events, (available at <https://identityassurance.blog.gov.uk/2016/08/12/local-government-outputs-of-our-first-discovery-events/>).
- GOV.UK Verify (2016ad). GOV.UK Verify / DVLA / local authority discovery day, (available at <https://identityassurance.blog.gov.uk/2016/07/15/gov-uk-verify-dvla-local-authority-discovery-day/>).
- GOV.UK Verify (2016ae). A joined-up approach to improving service design with DVLA, (available at <https://identityassurance.blog.gov.uk/2016/09/05/a-joined-up-approach-to-improving-service-design-with-dvla/>).
- GOV.UK Verify (2016af). #VerifyLocal pilots are open for business, (available at <https://identityassurance.blog.gov.uk/2016/10/03/verifylocal-pilots-are-open-for-business/>).
- GOV.UK Verify (2016ag). Listening to the market: engaging with local authority suppliers, (available at <https://identityassurance.blog.gov.uk/2016/10/17/listening-to-the-market-engaging-with-local-authority-suppliers/>).
- GOV.UK Verify (2016ah). Guest post: GOV.UK Verify, OIX and the future of banking, (available at <https://identityassurance.blog.gov.uk/2016/02/17/guest-post-gov-uk-verify-oix-and-the-future-of-banking/>).
- GOV.UK Verify (2016ai). The value of digital identity to the financial sector, (available at <https://identityassurance.blog.gov.uk/2016/09/22/the-value-of-digital-identity-to-the-financial-sector/>).
- GOV.UK Verify (2016aj). Government services using GOV.UK Verify - May 2016 update, (available at <https://identityassurance.blog.gov.uk/2016/05/25/government-services-using-gov-uk-verify-may-2016-update/>).
- GOV.UK Verify (2016ak). Improving GOV.UK Verify's demographic coverage - an update on Northern Ireland, (available at <https://identityassurance.blog.gov.uk/2016/11/09/improving-gov-uk-verify-demographic-coverage-an-update-on-northern-ireland/>).
- GOV.UK Verify (2017a). Growing Verify: services that need less proof of identity, (available at <https://identityassurance.blog.gov.uk/2017/02/01/growing-verify-services-that-need-less-proof-of-identity/>).

- GOV.UK Verify (2017b). Privacy and Consumer Advisory Group, (available at <https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group>).
- GOV.UK Verify (2017c). How our certified companies support users to verify, (available at <https://identityassurance.blog.gov.uk/2017/03/30/how-our-certified-companies-support-users-to-verify/>).
- GOV.UK Verify (2017d). GOV.UK Verify Code of Interoperability, (available at <https://www.gov.uk/government/publications/govuk-verify-code-of-interoperability>).
- GOV.UK Verify (2017e). Creating test environments with the private sector, (available at <https://identityassurance.blog.gov.uk/2017/02/03/creating-test-environments-with-the-private-sector/>).
- GOV.UK Verify (2017f). The latest improvements across GOV.UK Verify's certified companies, (available at <https://identityassurance.blog.gov.uk/2017/01/06/the-latest-improvements-across-gov-uk-verify-s-certified-companies/>).
- GOV.UK Verify (2017g). About this guide — GOV.UK Verify Technical Guide documentation, (available at <http://alphagov.github.io/rp-onboarding-tech-docs/>).
- GOV.UK Verify (2018a). Introducing GOV.UK Verify, (available at <https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify>).
- GOV.UK Verify (2018b). Service dashboard, (available at <https://www.gov.uk/performance/govuk-verify>).
- GOV.UK Verify (2018c). Account Use, (available at <https://www.gov.uk/performance/govuk-verify/users-accessing-services>).
- GOV.UK Verify (2018d). Account use by week (existing users), (available at <https://www.gov.uk/performance/govuk-verify/sign-in-by-week>).
- Hall, K. (2016). Gov to pull plug on online ID verification portal Gateway in 2018, (available at [http://www.theregister.co.uk/2016/05/13/plug\\_to\\_be\\_pulled\\_on\\_gateway\\_in\\_2018/](http://www.theregister.co.uk/2016/05/13/plug_to_be_pulled_on_gateway_in_2018/)).
- Head, B. (2016). Identity prominent in Australian security debate, *Computer Weekly* (available at <http://www.computerweekly.com/news/450303746/Identity-prominent-in-Australian-security-debate>).
- HM Passport Office (2011). Basic passport checks, (available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/118783/basic-passport-checks.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118783/basic-passport-checks.pdf)).
- Institute for Government (2011). System error: Fixing the flaws in government IT, (available at <http://www.instituteforgovernment.org.uk/sites/default/files/publications/System%20Error.pdf>).
- Institute for Government (2016). Making a success of digital government, *Institute for Government* (available at <http://www.instituteforgovernment.org.uk/publications/making-success-digital-government>).
- Leyden, J. (2016a). Did hacktivists really just expose half of Turkey's entire population to ID theft?, *The Register* (available at [http://www.theregister.co.uk/2016/04/04/turkey\\_megaleak/](http://www.theregister.co.uk/2016/04/04/turkey_megaleak/)).

- Leyden, J. (2016b). Megabreach: 55 MILLION voters' details leaked in Philippines, *The Register* (available at [http://www.theregister.co.uk/2016/04/07/philippine\\_voter\\_data\\_breach/](http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/)).
- Leyden, J. (2016c). "No password" database error exposes info on 93 million Mexican voters, *The Register* (available at [http://www.theregister.co.uk/2016/04/25/mexico\\_voter\\_data\\_breach/](http://www.theregister.co.uk/2016/04/25/mexico_voter_data_breach/)).
- Liberal Democrats (2010). Manifesto 2010, (available at <http://www.general-election-2010.co.uk/2010-general-election-manifestos/Liberal-Democrat-Party-Manifesto-2010.pdf>).
- Lips, A. M. B., Taylor, J. A., and Organ, J. (2009). Identity management, administrative sorting and citizenship in new modes of government, *Information, communication & society* 12(5), 715–734.
- Lips, M. B. (2013). Reconstructing, attributing and fixating citizen identities in digital-era government, *Media, Culture & Society* 35(1), 61–70.
- LSE Identity Project (2005). Main Report, (available at <http://identityproject.lse.ac.uk/identityreport.pdf>).
- Martin, A. K., and Whitley, E. A. (2013). Fixing identity? Biometrics and the tensions of material practices, *Media, Culture and Society* 35(1), 52–60.
- Mathieson, S. A. (2013). *Card declined: how Britain said no to ID cards, three times over*, CreateSpace London.
- McCluggage, W. (2011). ID Assurance Programme - Stakeholder and Communications Group (Privacy and Consumer (PC)), Email invitation to join PCAG sent to the author .
- Merrett, N. (2016a). Experian vows to expand GOV.UK Verify data sources, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/experian-vows-to-expand-govuk-verify-data-sources-4786830>).
- Merrett, N. (2016b). PayPal withdraws from GOV.UK Verify, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/paypal-withdraws-from-govuk-verify-4836965>).
- Merrett, N. (2016c). Verizon "temporarily removed" as GOV.UK Verify ID provider, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/verizon-temporarily-removed-as-govuk-verify-id-provider-4955500>).
- Merrett, N. (2016d). New GOV.UK Verify lead mulls devolution and NHS potential, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/new-govuk-verify-lead-mulls-devolution-and-nhs-potential-4985603>).
- Merrett, N. (2016e). GDS lays down law on council Verify adoption criteria, (available at <http://central-government.governmentcomputing.com/news/govuk-verify-to-underpin-council-permit-transformation-pilots-5001712>).
- Merrett, N. (2017a). HMRC reiterates Verify support beyond Gateway revamp, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/hmrc-reiterates-verify-support-beyond-gateway-revamp-5739628>).

- Merrett, N. (2017b). Pensions Dashboard prototype standards launched, *Government Computing Network* (available at <http://central-government.governmentcomputing.com/news/pensions-dashboard-prototype-standards-launched-for-development-drive-5786151>).
- Moss, D. (2016a). RIP IDA – are GDS talking to themselves?, (available at <http://www.dmossesq.com/2016/04/rip-ida-are-gds-talking-to-themselves.html>).
- Moss, D. (2016b). Matt Hancock: 83 + 83 = 71, (available at <http://www.dmossesq.com/2016/06/matt-hancock-83-83-71.html>).
- NAO (2016). Protecting information across government, *National Audit Office* (available at <https://www.nao.org.uk/report/protecting-information-across-government/>).
- NAO (2017). Digital Transformation in Government, *National Audit Office* (available at <https://www.nao.org.uk/report/digital-transformation-in-government/>).
- NCSC (2018). About Us, (available at <https://www.ncsc.gov.uk/about-us>).
- Nyst, C., Pannifer, S., Whitley, E. A., and Makin, P. (2016). Digital Identity: Issue analysis, No. PRJ.1578, , *Consult Hyperion for Omidyar Network* (available at [http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1\\_6-1.pdf](http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf)).
- OECD (1980). Guidelines: On the Protection of Privacy and Transborder of Personal Data, Paris: *Organisation for Economic Co-Operation and Development* (available at [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html)).
- OIXUK (2016a). JustGiving and GOV.UK Verify: Exploring JustGiving information as part of the GOV.UK Verify process, (available at <http://oixuk.org/blog/2016/05/28/justgiving-and-gov-uk-verify/>).
- OIXUK (2016b). Verify Sandbox Environment, (available at <http://oixuk.org/blog/2016/12/13/verify-sandbox-environment/>).
- OIXUK (2016c). UK private sector needs for identity assurance, (available at <http://oixuk.org/blog/2016/06/28/uk-private-sector-needs-for-identity-assurance/>).
- OIXUK (2017a). Micro Sources of Data Aggregators, *OIXUK* (available at <http://oixuk.org/blog/2017/02/21/micro-sources-of-data-aggregators/>).
- OIXUK (2017b). Achieving Frictionless Customer Onboarding, (available at <http://oixuk.org/blog/2017/07/03/achieving-frictionless-customer-onboarding/>).
- OIXUK (2018). Published Papers – OIX – Open Identity Exchange, (available at <http://oixuk.org/papers/>).
- OPSI (1998). Data Protection Act 1998, (available at [http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)).
- OPSI (2018). Data Protection Act 2018, Text, (available at <https://www.legislation.gov.uk/ukpga/2018/12/contents>).
- Orlikowski, W. J. (2000). Using Technology and Constituting Structures: A Practice Lens for Studying Technology in organizations, *Organizational Science* 11(4), 404–428.
- Orlowski, A. (2015). Silicon Valley now “illegal” in Europe: Why Schrems vs Facebook is such a biggie, (available at [http://www.theregister.co.uk/2015/10/06/silicon\\_valley\\_after\\_max\\_schrems\\_safe\\_harbour\\_facebook\\_google\\_analysis/](http://www.theregister.co.uk/2015/10/06/silicon_valley_after_max_schrems_safe_harbour_facebook_google_analysis/)).

- Otjacques, B., Hitzelberger, P., and Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing, *Journal of management information systems* 23(4), 29–52.
- Parliament (2010). House of Commons Hansard Written Answers for 16 Jun 2010 (pt 0003), (available at <http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm100616/text/100616w0003.htm>).
- Parliament (2016). Statutory Instruments, *UK Parliament* (available at <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06509>).
- Pauli, D. (2016). Standards body warned SMS 2FA is insecure and nobody listened, *The Register* (available at [http://www.theregister.co.uk/2016/12/06/2fa\\_missed\\_warning/](http://www.theregister.co.uk/2016/12/06/2fa_missed_warning/)).
- Pieri, E. (2009). ID cards: A snapshot of the debate in the UK press, *ESRC National Centre for e-Social Science* (available at [https://danishbiometrics.files.wordpress.com/2009/08/pieri\\_idcards\\_full\\_report.pdf](https://danishbiometrics.files.wordpress.com/2009/08/pieri_idcards_full_report.pdf)).
- Public Administration Select Committee (2011). Government and IT- “A Recipe For Rip-Offs”: Time For A New Approach, (available at <http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpublicadm/715/715i.pdf>).
- Reuters, T. (2016). 3 priorities for managing KYC and on-boarding challenge, (available at <http://blog.financial.thomsonreuters.com/3-priorities-for-managing-kyc-and-on-boarding-challenge/>).
- Schonberg, A. (2016). GB Group’s shares fall on sluggish GOV.UK Verify roll-out, *DigitalLook* (available at <http://www.digitallook.com/news/aim-bulletin/gb-groups-shares-fall-on-sluggish-govuk-verify-roll-out--1771884.html>).
- Sir James Crosby (2008). Challenges and opportunities in identity assurance, *HM Treasury* (available at [http://webarchive.nationalarchives.gov.uk/20120906144256/http://www.hm-treasury.gov.uk/d/identity\\_assurance060308.pdf](http://webarchive.nationalarchives.gov.uk/20120906144256/http://www.hm-treasury.gov.uk/d/identity_assurance060308.pdf)).
- Strasburger, L. P. (2016). Investigatory Powers Bill: A force for good – if done right?, *The Register* (available at [http://www.theregister.co.uk/2016/01/11/strasburger\\_on\\_draft\\_investigatory\\_powers\\_bill/](http://www.theregister.co.uk/2016/01/11/strasburger_on_draft_investigatory_powers_bill/)).
- The Sunday Times (2006a). ID Cards doomed, say officials, London.
- The Sunday Times (2006b). Emails from Whitehall officials in charge of ID Cards, London (available at [http://webarchive.nationalarchives.gov.uk/20090415101745/http://www.ips.gov.uk/identity/downloads/foi/3905\\_URN\\_129.pdf](http://webarchive.nationalarchives.gov.uk/20090415101745/http://www.ips.gov.uk/identity/downloads/foi/3905_URN_129.pdf)).
- Thomson, I. (2014). Feds dig up law from 1789 to demand Apple, Google decrypt smartphones, slabs, *The Register* (available at [http://www.theregister.co.uk/2014/12/01/feds\\_turn\\_to\\_1789\\_law\\_to\\_force\\_smartphone\\_makers\\_to\\_decrypt\\_handsets/](http://www.theregister.co.uk/2014/12/01/feds_turn_to_1789_law_to_force_smartphone_makers_to_decrypt_handsets/)).
- Thomson, I. (2015). SIX MILLION fingerprints of US govt workers nicked in cyber-heist, *The Register* (available at [http://www.theregister.co.uk/2015/09/23/opm\\_loses\\_millions\\_more\\_fingerprints/](http://www.theregister.co.uk/2015/09/23/opm_loses_millions_more_fingerprints/)).



- Tsakalakis, N., Stalla-Bourdillon, S., and O'Hara, K. (2017). Identity Assurance in the UK: technical implementation and legal implications under eIDAS, *The Journal of Web Science* 3(3), 32–46.
- tScheme (2017). tScheme Website, (available at <http://www.tscheme.org/>).
- UKAuthority.com (2016). Verify can work in private sector, says OIX chief, *UKAuthority.com* (available at <http://www.ukauthority.com/news/6289/verify-can-work-in-private-sector-says-oix-chief>).
- UKIPS (2006). Strategic Action Plan for the National Identity Scheme: Safe guarding your identity, (available at <http://webarchive.nationalarchives.gov.uk/20090415101316/http://www.ips.gov.uk/identity/downloads/Strategic-Action-Plan.pdf>).
- Veridu (2016). The use of online activity in identity verification: A summary of our recent experience of working with the Government Digital Service (GDS) and the Open Identity Exchange (OIX) on a research project related to GOV.UK Verify., *Medium* (available at <https://medium.com/@VeriduHQ/the-use-of-online-activity-in-identity-verification-87443401834c#.izv7mkcj5>).
- Virgo, P. (2016). Now that Verify has lost its head, will the corpse be decently buried? - When IT Meets Politics, *Computer Weekly* (available at <http://www.computerweekly.com/blog/When-IT-Meets-Politics/Now-that-Verify-has-lost-its-head-will-the-corpse-be-decently-buried>).
- Whitley, E. A. (1994). Too many errors on the cards, Letters to the Editor, *Daily Telegraph*, .
- Whitley, E. A. (2014). REF Impact Case Study: Scrapping costly and controversial proposals for identity cards, (available at <http://www.lse.ac.uk/researchAndExpertise/researchImpact/caseStudies/whitley-scrapping-costly-controversial-proposals-identity-cards.aspx>).
- Whitley, E. A. (2015). The government's Verify service demonstrates the benefits of focusing on user needs, (available at <http://blogs.lse.ac.uk/politicsandpolicy/the-governments-verify-service-demonstrates-the-benefits-of-focusing-on-user-needs/>).
- Whitley, E. A., and Hosein, G. (2010a). *Global challenges for identity policies*, Palgrave Macmillan Basingstoke.
- Whitley, E. A., and Hosein, G. (2010b). Opposition policies on identity cards, (available at <http://blogs.lse.ac.uk/politicsandpolicy/opposition-policies-on-identity-cards/>).
- Whitley, E. A., and Manby, B. (2015). Questions of legal identity in the post-2015 development agenda, (available at <http://blogs.lse.ac.uk/humanrights/2015/05/28/questions-of-legal-identity-in-the-post-2015-development-agenda/>).
- Whitley, E. A., Martin, A. K., and Hosein, G. (2014). From surveillance-by-design to privacy-by-design: Evolving identity policy in the UK, in *Histories of State Surveillance in Europe and Beyond* K. Boersma, R. Brakel, C. Fonio, and P. Wagenaar (eds.), Routledge London, 205–219.
- Winner, L. (1980). Do artifacts have politics?, *Daedalus* 109(1), 121–36.
- Woolgar, S., and Cooper, G. (1999). Do artefacts have ambivalence? Moses' bridges, Winner's bridges and other urban legends in S&TS, *Social studies of science* 29(3), 433–449.
- World Bank (2017). Principles on identification for sustainable development: Toward the digital age, *World Bank* (available at

<http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-WP-PUBLIC-IDDIentificationPrinciples.pdf>.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology* 30(1), 75–89.