~~PRIVACY~~
~~INTERNATIONAL~~

Briefing

Biometrics: Friend or foe of privacy?

I. Biometric technology in the developing world

Advancement in technology has permitted socio-economic and political developments worldwide. This is particularly so in developing countries, where new technologies have often been portrayed as revolutionary tools for development.

One growth area that has attracted much attention and interest is the use of biometric technology.[1] Scores of developing countries across Africa, Asia and Latin America have been rushing to adopt biometric technology for a range of purposes: from conducting population registration in countries where birth registration has not previously been systematic, to conducting elections, or as a means of facilitating access and delivery of certain services such as food, health care and other basic social needs. Increasingly, identification-based systems are being developed using biometrics technologies, which are seen as an effective and secure tool for recognising and securing an individual's legal identity, and as means of facilitating access to socio-economic services and civic rights.

A brief scan of recent efforts to adopt biometric technologies in the developing world reveal the range of purposes to which the technology has been applied:

- National identification systems[2] to prevent identity fraud and theft: governments in Mexico[3], India[4], and Argentina[5] are all developing biometric national identification systems; Thailand[6] has launched a smart ID card that is believed to be the largest integrated circuit chip ID card project in the world;
- Delivery of social services[7] including e-health systems[8]: WHO[9] is running e-health programmes in collaboration with national partners across the world, other examples include TeleDoctor in Pakistan[10] or E Health Point in India[11] which enable access to health care

[1] Alan Gelb and Julia Clark, "Identification for Development: The Biometrics Revolution," *Center for Global Development*, Working Paper 315, January 2013.

[2] Further information available on Electronic Frontier Foundation (EFF) website, "Mandatory National IDs and Biometric Databases". Available at: https://www.eff.org/issues/national-ids

[3] Further information available here: http://www.renapo.gob.mx/swb/swb/RENAPO/home

[4] Further information available here: http://uidai.gov.in/

[5] Further information available here: http://www.prensa.argentina.ar/2011/11/08/25418-se-creo-el-sistema-de-identificacion-biometrica.php

[6] Further information available here: http://office.bangkok.go.th/ard/Manual_regis.html

[7] Szreter, S., (2007) 'The right to registration: development, identity and social security' World Development, 35 (1): 67-86

[8] Hosein, G., and Martin, A., (2010), *Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations*, The London School of Economics and Political Science. Available at: http://www2.lse.ac.uk/management/documents/electronic-health-privacy.pdf

[9] Further information available here: http://office.bangkok.go.th/ard/Manual_regis.html

[10] Further information available here: http://www.telenor.com/sustainability/initiatives-worldwide/bringing-social-services-to-pakistan/

[11] Further information available here: http://ehealthpoint.com/

professionals, Nacer in Peru[12] which uses telephone and internet technology to allow data management (collect, access, sharing, analysis) or m-Health (mobile-health) programmes such as VidaNet, the HIV patient reminder and information system in Mexico[13];

- Electoral registers[14] and supporting democratisation: the Philippines[15], Ghana[16] and Kenya[17], have all used biometric voter registration in their recent elections. China has set up a biometric data centre with the stated purpose of maintaining public security, but has allowed an online commercial enterprise offering biometric data-matching services access to the data;
- Aid delivery[18] and social protection programmes[19]: UNHCR[20]uses biometric technologies to process enrolment in refugee camps, the World Bank[21] to ensure effective targeting of beneficiaries, by funding biometric systems for registration of the urban poor in Benin and Kenya;
- Border management: Mauritania is implementing a biometric entry-exit border control system as part of its security and counter-terrorism strategy and Senegal[22] recently implemented a biometric visa process upon entry for nationals of certain countries.

II. Protecting privacy in biometric systems: the challenges

The issues outlined in other sections of this paper hereafter such as fraud, misuse and abuse are problems faced also by developed countries where data protection laws are already in place. These concerns and risks are especially acute however, in developing countries where the absence of

[12] Further information available here: http://healthmarketinnovations.org/program/nacer

[13] Further information available here: http://edit.voxiva.com/content/case_studies/VidaNet.pdf

[14] Evrensel, A., ed., (2010) *Voter Registration in Africa: A Comparative Analysis*, Electoral Institute for Sustainable Democracy in Africa. Available at: http://www.eisa.org.za/PDF/vrafrica.pdf

[15] Jaracz, J., *Philippine biometric voter registration becomes law*, SecureIDNews, 1 March 2013. Available here: http://secureidnews.com/news-item/philippine-biometric-voter-registration-becomes-law/

[16] Darkwa, L., *Ghana's Elections 2012: Some Observations*, Kujenga Amani, 15 August 2015. Available here: http://forums.ssrc.org/kujenga-amani/2013/08/15/ghanas-elections-2012-some-observations/

[17] Lewela, M., and Kisiangani, E., *Kenya's Biometric Voter Registration: New Solution, New Problems*, Institute for Security Studies, 29 October 2013. Available here: http://www.issafrica.org/iss-today/kenyas-biometric-voter-registration-new-solution-new-problems

[18] Hosein, G., and Nyst, C., (2013) *An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*, Privacy International. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229

[19] Devereau, S., and Vincent, K., (2010) *Using technology to deliver social protection: exploring opportunities and risks*, Development in Practice, Volume 20, Issue 3, pp. 367-379; Gelb, A., and Decker, C., (2011) *Cash at your fingertips: biometric technology for transfers in developing and resource-rich countries*, Center for Global Development

[20] Further information available here: http://www.bioidtech.co.uk/BioID/UNHCR.html

[21] Garcia, M., and Moore, C., (2012) *The Cash Dividend: The Rise of Cash Transfer Programs in Sub-Saharan Africa*, The World Bank. Available here: https://openknowledge.worldbank.org/bitstream/handle/10986/2246/672080PUB0EPI0020Box367844B09953137.pdf?sequence=1

[22] Further information on biometric visa procedure is available here: http://www.snedai.sn/fr/

laws or flawed legal frameworks are failing to uphold and ensure the protection of basic human rights.

Whilst the majority of developing countries include the right to privacy in their Constitution,[23] poor practical implementation of this right means that in practice few measures are in place to ensure mechanisms, such as data protection legislation, exist to safeguard this right. Although there have been some regional initiatives,[24] concrete legally binding outcomes are yet to be seen.

In the developing world, the adoption of new technologies is rarely preceded by the adoption and implementation of robust regulatory frameworks. Assessments to critically analyse and assess the impact of new technologies on human rights and the daily lives of individuals in the developing world are also infrequent. This failure means that the risks are not accessed and identified and thus corresponding risk mitigating measures are not implemented. This lacuna permits mass human rights violations, which directly deny individuals of their autonomy, their fundamental freedoms and – in extreme circumstances – their identity.

In addition to conceptual criticism of the use of biometric data in developing countries, more practical challenges question the appropriateness of using advanced technologies. In many countries in the developing world, an inconsistent electricity supply means that the reliance on such technologies to carry out key tasks such as public service delivery, identity checks and border management, means crucial tasks cannot be completed at all times. Consequently, back-up manual systems are still needed, something that was seen during the elections in Kenya and Ghana where the technology failed to meet the promises of its promoters.[25]

CASE STUDY: Kenyan elections, the failed promise of biometrics

In an attempt to redress its poor transparency record, in particular in the context of elections, Kenya decided to adopt a new voting system whereby voters would identify themselves biometrically. The cost of conducting Kenya's 2012 elections amounted to $293 million (with donors contributing

[23] Tynan, R., *What do constitutional privacy protections look like around the worl*d, Privacy International, 5 July 2013. Available at: https://www.privacyinternational.org/blog/what-do-constitutional-privacy-protections-look-like-around-the-world

[24] Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms

[25] Wrong, M., *Africa's Election Aid Fiasco*, The Spectator, 20 April 2013. Available at: http://www.spectator.co.uk/features/8890471/the-technological-fix/

$100 million) but the outcome was an utter fiasco with biometric kits failing to recognise thumbs, forcing ID card numbers to be typed laboriously by hand into the system. Further, classrooms routinely used as polling stations in Africa were not equipped with power sockets and when it came to the electronic transmission, voting officers had forgotten their identification numbers and were therefore unable to access the system or the system simply failed to function.[26]

III. Biometrics: An Introduction

Biometric technology is increasingly used for an array of public administration purposes ranging from identity registration to border control, as a means of administering and managing access to and enjoyment of civic rights such as voting, and social rights such as health care and education. These technologies are also being used for security purposes including tackling national security threats, conducting law enforcement, and as a general means of carrying out mass surveillance.

All of the above activities must be regulated and monitored in order to ensure they do not violate the right to privacy and related rights such as the rights to freedom of expression, association, and movement. Regulation and monitoring of biometrics has already proven to be a challenge for countries where data protection and other safeguards are in place. Consequently, there is increasing concern regarding the situation in the developing world, where legal safeguards to protect the right to privacy and data security are lacking and the deployment of new technologies such as biometric technology is increasingly popular.

This paper outlines what biometric technology is, identifies the risks linked to the collection, use and retention of biometrics, particularly in the developing world; analyses the impact biometric technology has on the right to privacy and other basic human rights; and outlines safeguards required to ensure the protection of the right to privacy in the face of new technologies.

IV. Biometrics: what, how and why?

Biometrics refers to the measurement of unique and distinctive physical, biological and behavioural characteristics used to confirm the identity of individuals.

Neither the concept of biometrics, nor their use, is new: fingerprints were used for identification in 14th century China, and in 1879 Alphonse Bertillon,

[26] Wrong, M., *Africa's Election Aid Fiasco*, The Spectator, 20 April 2013. Available at: http://www.spectator.co.uk/features/8890471/the-technological-fix/

a French police inspector, suggested the use of body measurements which included arm and foot length in order to identify repeat offenders. A decade later, through the work of Edward Henry, the British paved the way for the development of a fingerprint database, which up to this day remains the most preferred biometric identification system.[27] As technologies have advanced, however, biometrics have become an increasingly popular tool in the development arena, in the delivery and management of public services, and for law enforcement and surveillance purposes.

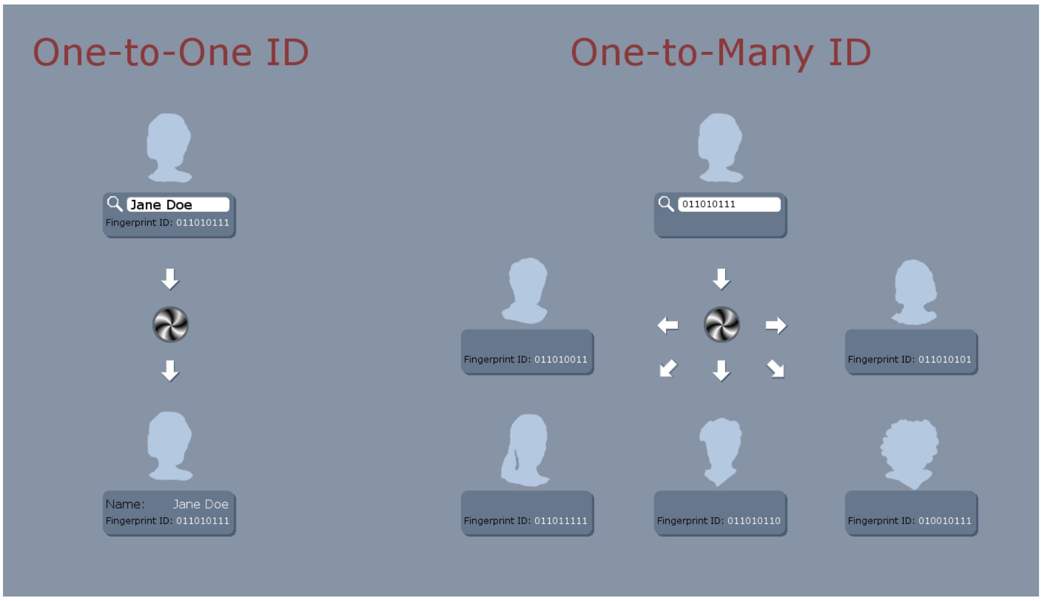
Fingerprints are the most commonly known and used biometric traits, but with improvements in technology, multiple sources of biometric information have emerged. These include data related to facial features, iris, voice, hand geometry and DNA. Each trait is collected using different technologies and can be used for different purposes separately or in combination, to strengthen and improve the accuracy and reliability of the identification process.

In general, biometric information is developed by processing extractable key features into an 'electronic digital template', which is then encrypted to regulate access to it, saved and stored in a database. The information is used when an individual enters a system, which requires him/her to identify and validate his/her identity. The 'electronic digital template' saved will be used to match the biometric information presented by the individual, be it fingerprints, facial features, or iris, and based on this comparison, the individual's identity will be confirmed or rejected.[28] This is the case, for example, when an individual presents herself at a border check. The traveller presents her ID or passport and the biometric information saved on that document is verified with the known biometric characteristics of the individual.

The intended purpose of biometric technology is to confirm the identity of individuals through a "one to one" identification check. This system compares a source of biometric data with existing data for that specific person. This is the system used at airport passport controls, and in targeted public service delivery systems (health care, pension schemes, etc.).

[27] McDowell, J., *Something You Are: Biometrics versus Privacy*, Sans Institute, 2000-2002. Available at: http://www.giac.org/paper/gsec/2197/are-biometrics-privacy/103735

[28] For further details on biometrics technology visit the International Biometrics & Identification Association (IBIA) available at: http://www.ibia.org/biometrics/technologies/


One-to-One ID
One-to-Many ID
Jane Doe
Fingerprint ID: 011010111
Name: Jane Doe
Fingerprint ID: 011010111
011010111
Fingerprint ID: 011010011
Fingerprint ID: 011010101
Fingerprint ID: 011011111
Fingerprint ID: 011010110
Fingerprint ID: 010010111

However, the use of such data in a "one to many" identification system has a greater and more serious privacy impact. Such a system does not confirm the identity of a known individual as through the "one-to-one" system but it aims to match biometrics measurements of an unknown identity to a mass biometric database. Such a system is used, for example, in identifying individuals in a crowd through the use of facial recognition identification technology, or the use of DNA databases in criminal investigations to compare DNA found at the crime scene against DNA samples saved in a database. This raises privacy concerns in relation to the risks of false matches and data breaches.[29] In the case of criminal investigations, for example, an individual could risk becoming a suspect based on a wrongly identified biometric data; or in the context of an asylum process, misidentification could hinder an asylum seeker's fundamental right to seek asylum if they are wrongly identified as someone else who has already had their asylum claim rejected.

Increasingly, an array of identification-based systems are founded on the use of biometrics technologies, which are seen as effective and secure tools to create an individual's legal identity. It is argued that such systems enable the effective provision (and monitoring) of rights, including social rights (health care, education), economic rights (bank accounts) and civic rights (voting) as well as for ensuring national security and maintaining public order (policing, border management).

Despite developed countries' uptake of such technologies in the 1980s and 1990s, recent trends have illustrated their reluctance to deploy biometric technology - or at least mass storage of biometric data because of privacy

[29] Office of the Privacy Commissioner of Canada, *Data at Your Fingertips: Biometrics and the Challenges to Privacy*, OPC Guidance Documents. Available at: http://www.priv.gc.ca/information/pub/gd_bio_201102_e.pdf

concerns.[30] Key examples in Europe have included the scrapping of the National Identity Register and ID cards in the UK,[31] and Germany decision to reject a centralised database when deploying biometric passports.

By contrast, in developing countries the deployment of biometric technology is on the rise and is being sold to citizens as a means to establishing their legal identity and provide them access services, as well as a tool for achieving economic development. However, too often these goals are prioritised at the expense of their right to privacy and other human rights.

V. The Right to Privacy, Technology and Biometrics

Privacy is a fundamental human right[32] and in today's digital world, it is the cornerstone that safeguards who we are and supports our on-going struggle to maintain our autonomy and self-determination in the face of increasing state power. The right to privacy is upheld by an array of global[33] and regional[34] international human rights treaties and guaranteed in numerous national constitutions.[35]

Technologies are developed and deployed in ways that empower people around the world to access information, express themselves, and participate in local and global discussions in unprecedented ways. The other side of the coin is that there are challenges that arise from the use (and the abuse) of these new unprecedented information and communication technologies. As technological advancements have outpaced legislative change, the safeguards necessary to ensure that rights are adequately protected are lagging behind. In practice this means that basic human rights such as the right to privacy and data protection are at constant risk. The lack of protection mechanisms, or creation of inadequate mechanisms, has also indirect societal and ethical consequences as the concepts of privacy, liberty and freedoms are misunderstood, eroded or devalued. These consequences are a particular risk in the deployment of

[30] Yet, the European Union is investing significant effort and money into deploying biometric border management systems to secure Fortress Europe through its Smart Border Package (Registered Traveller Programme and Entry/Exit System), as well as other databases such as EURODAC. For further information visit the EU Home Affairs website.

[31] Green, D., *Scrapping ID cards is a momentous step*, The Guardian, 21 December 2010. Available at: http://www.theguardian.com/commentisfree/2010/dec/21/scrapping-id-cards-momentous-step

[32] Even if its absolutism is contested

[33] Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (ICCPR, art. 17), the Convention on the Rights of the Child (art. 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14)

[34] Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

[35] See Privacy International's "The Right to Privacy in World Constitutions", published on www.privacyinternational.org

biometric technology and its use in identification programmes that provide the necessary tools to enable surveillance and profiling. The case of India and the creation of the Unique Identity Scheme biometrics database (Aadhaar) of 1.3 billion people clearly reflects the dangers when a country decides to deploy technology as a means of social development but fails to consider the need for a legal framework to manage the protection of individual's data (see case study below). As noted by Gellman, "personal identification systems and all of their features affect the privacy of personal information."[36]

Both the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue[37] and the UN High Commissioner for Human Rights, Navi Pillay[38] have expressed shared concerns about violations of the right to privacy and the lack of effective protective measures in relation to biometric technologies.

Numerous historical incidents involving persecution on the basis of race, ethnicity and religion were facilitated through the use of identification systems, including the persecution of Jews by Germany in the 1930s, apartheid in South Africa, and the 1994 Rwandan Genocide. Given the tragic outcomes of these events, the on-going development of identification systems must be carefully monitored and take into account lessons learnt. By its very nature biometric data is intrinsically linked to what constitutes us as 'humans' as it brings together various elements, which make up our respective and unique identity (gender, size, skin colour, ethnic origin, etc.). It has been argued that the collection, analysis and storage of such innate and personal data is "de-humanising" as it reduces the individual, the human being, to a number.[39]

This is one of the many reasons why human rights organisations are so concerned about the increasing development and use of technology without appropriate safeguards. It is therefore crucial that lawmakers and those advocating for the use of such systems acknowledge this reality up front so that risk mitigation measures can be included to uphold individuals' right to privacy.

[36] Gellman, R., *Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries*, CGD Policy Paper 028 August 2013. Washington DC: Center for Global Development, pp. 11. Available at: http://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0.pdf

[37] A/HRC/23/40. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[38] UN News Centre, *UN rights chief urges protection for individuals revealing human rights violations,* 12 July 2013. Available at: http://www.un.org/apps/news/story.asp?Cr=asylum&NewsID=45399#.UhSMDmRgYSg

[39] Van den Hoogen, S. (2009), *Perceptions of Privacy and the Consequences of Apathy: Biometric Technologies in the 21st Century*, Dalhousie Journal of Interdisciplinary Management, Volume 4, Spring 2009, pp. 9. Available at: www.djim.management.dal.ca/issue_pdfs/Vol4/van_den_Hoogen_S.pdf

The very process of collecting biometric data raises concerns linked to cultural norms and personal fears or discomforts. The collection of facial features could be unacceptable in many cultures or religions[40]; an iris scan which requires an invasive camera to photograph the eye can be uncomfortable;[41] and children whose fingerprints were taken have expressed fear of the glowing infrared light which they associated with heat.

Additionally, the increasing use of surveillance technologies "risks centralizing an increasing amount of power in the hands of government authorities, often in places where democratic safeguards and civil society watchdogs are limited."[42] State-imposed requirements for identity can lay the foundations for systematic and extensive human rights violations including discrimination on a massive scale, and in some cases they can prevent access to basic services that guarantee human rights such as voting or receiving welfare benefits.[43]

CASE STUDY
India: Idealising biometrics as a tool for development

The development of India's Unique Identity Scheme (UID), known as Aadhaar, illustrates the worrying trend of idealising biometric technology and its (expected but not proven) capacity as a tool for development. A statement by Nandan Nilekani, co-founder of Infosys Ltd. (INFY) and one of the world's most successful information technology entrepreneurs, who is leading the UID, said the scheme "uses the most sophisticated technology … to solve the most basic of development challenges."[44]

The official intended purpose of implementing a national ID system is to streamline public services delivery and include marginalised members of Indian society who have fallen out of the welfare system or were never accounted for in the first place. The latter situation can be due to bureaucratic failings such as the lack of birth registration or socio-

[40] Gellman, R., *Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries*, CGD Policy Paper 028, August 2013, Washington DC: Center for Global Development, pp. 23. Available at: http://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0.pdf

[41] McDowell, J., *Something You Are: Biometrics versus Privacy*, Sans Institute, 2000-2002. Available at: http://www.giac.org/paper/gsec/2197/are-biometrics-privacy/103735

[42] Donovan, K. P. and Nyst, C., *Privacy for the Other 5 Billion*, Slate, 17 May 2013. Available at: http://www.slate.com/articles/technology/future_tense/2013/05/aadhaar_and_other_developing_world_biometrics_programs_must_protect_users.html

[43] Gellman, R., *Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries*, CGD Policy Paper 028, August 2013, Washington DC: Center for Global Development, pp. 10. Available at: http://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0.pdf

[44] Donovan, K. P. and Nyst, C., *Privacy for the Other 5 Billion*, Slate, 17 May 2013. Available at: http://www.slate.com/articles/technology/future_tense/2013/05/aadhaar_and_other_developing_world_biometrics_programs_must_protect_users.html

economic factors such as the legacies of the caste system. The system's instigators believe it could be the solution for including India's marginalised population in government and society.[45]
Such arguments are worrying as they can be used to appeal to individuals to give up their rights in return for economic development, which cannot be guaranteed. As Van den Hoogen has argued, "most individuals are willing to exchange personal information for the services and conveniences they offer"[46] but little consideration is given to explaining the process and impact of giving over this information and granting the government indefinite access to it.

To date, the Aadhaar project has been conducted without a corresponding legislative implementation framework, even though the Supreme Court has been called to guide the process. This means that no protection mechanisms have been put in place to protect the rights of individuals whose information is being collected, or to secure the biometric data itself. Considering that the project is in the process of collecting, processing and storing the most personal data of 1.3 billion people, the lack of sufficient legal protections, or at the very least the recognition of the need for a robust legal framework, raises significant privacy concerns. The Supreme Court recently ruled in an interim order that people cannot be required to have the controversial Aadhaar identification to collect state funded benefits and services.[47] Yet the programme continues to be rolled out.

VI. Biometrics – the risks

Whilst biometric technology has improved, it is not infallible: its conceptual weaknesses and vulnerability to fraud and misuse, its margin for error and ability to be used for a wide range of purposes remain widely controversial and disputed.

1. Fraud and Misuse

The idea of using biometric data to remedy bureaucratic errors such as failing to register births, to make service delivery more efficient or accessible, or for justifiable law enforcement purposes, is laudable. However, the absence of strong regulations and safeguards means that the

[45] Schneider, H., I*ndia launches biometric data project to make every citizen count in official eyes,* 14 May 2013. Available at: http://www.theguardian.com/world/2013/may/14/india-biometric-data-identity-mapping

[46] Van den Hoogen, S. (2009), *Perceptions of Privacy and the Consequences of Apathy: Biometric Technologies in the 21st Century*, Dalhousie Journal of Interdisciplinary Management, Volume 4, Spring 2009, pp. 6. Available at: www.djim.management.dal.ca/issue_pdfs/Vol4/van_den_Hoogen_S.pdf

[47] *Aadhaar: Governmentt to go by Supreme Court ruling*, The Statesman, 24 September 2013. Available at: http://www.thestatesman.net/news/16813-Aadhaar--Govt-to-go-by-Supreme-Court-ruling.html?page=1

use of biometric data in national ID programmes and potentially for other unforeseen purposes is concerning. The privacy risks associated with ID and biometric systems are numerous, ranging from identity theft and fraud to social sorting and persecution. This has serious implications for individuals' rights to privacy, security and data protection.

It is important to note that one of the arguments in favour of biometrics information data is the protection of an individual's identity, as it is "harder to forge, copy, share, misplace and guess".[48] However, the use of biometric data does not guarantee the protection of one's identity. And unlike regular ID cards, the use of biometric data raises additional concerns and irreversible consequences; as such data is absolutely unique to an individual.[49] This means that if one's biometric data is stolen or misused it means their legal identity is compromised but yet they cannot be given a new one. This risk creates a context in which, in extreme circumstances, someone could be completely stripped of their identity without recourse or redress nor the possibility to get it back. The possibility of this actually happening is not far fetched when considering examples where fingerprints were copied onto latex as a means of forging authorised access[50] or DNA of another person was created from the blood and saliva of a donor.[51] These possibilities reflect the uncertainty of the uniqueness of biometrics data.

2. Misidentification and Inaccuracies

Notwithstanding significant advancements in biometric technology and proven successes, the technology is still evolving and its effectiveness and accuracy is constantly being challenged.

Imperfect matches are common with false confirmation[52] and false reject errors[53]. Despite being the cheapest biometric data system, finger printing has the highest rate of error. Facial recognition is increasingly used but numerous studies have shown that facial recognition systems are very

[48] Jain, A. K., and Pankanti, S., *Beyond Fingerprinting*, American Scientist, September 2008, pp. 78. Available at: http://libserver.wlsh.tyc.edu.tw/sa/pdf.file/en/e080/e080p082.pdf

[49] Van den Hoogen, S. (2009), *Perceptions of Privacy and the Consequences of Apathy: Biometric Technologies in the 21st Century*, Dalhousie Journal of Interdisciplinary Management, Volume 4, Spring 2009, pp. 8-9. Available at: www.djim.management.dal.ca/issue_pdfs/Vol4/van_den_Hoogen_S.pdf; Electronic Frontier Foundation, Mandatory National IDs and Biometric Databases, https://www.eff.org/issues/national-ids

[50] Farivar, C., *Digital fingerprint door lock defeated by photocopied 'print*, Engadget, 22 September 2006. Available at: http://www.engadget.com/2006/09/22/digital-fingerprint-door-lock-defeated-by-photocopied-print/

[51] Harmon, K., Lab creates fake DNA evidence, Scientific American, 18 August 2009. Available at: http://www.scientificamerican.com/blog/post.cfm?id=lab-creates-fake-dna-evidence-2009-08-18

Jain, A. K., and Pankanti, S., *Beyond Fingerprinting*, American Scientist, September 2008, pp. 79-81. Available at: http://libserver.wlsh.tyc.edu.tw/sa/pdf.file/en/e080/e080p082.pdf susceptible to the conditions in which the photo is taken (i.e. lighting, inside or outside, etc.). The use of the iris remains the most accurate and one of the least invasive systems but the method's dependency on algorithms still leaves rooms for (human) error.[54]

3. Exclusionary

Additionally, the universality of the technology itself is yet to be proven. Fingerprint processing technologies have shown failures to collect a usable template. For example, manual labour workers whose fingerprints are damaged due to the nature of their work, as well as people with very fine fingerprints. Facial recognition systems have encountered difficulties when scanning individuals with darker skin. In terms of the iris scan, which up to now, remains the most efficient and accurate, even if the most expensive technology, flaws have emerged over the inadequacy to process iris scans for physical impaired individuals and those suffering from cataracts. These types of cases raise concerns about the exclusionary impact of such technologies.

4. Biometrics as a tool for surveillance

Biometric technology in and of itself is not harmful but in the context of flawed or non-existent legislation, its use can be detrimental to individuals. As Crook argues in the case of ID cards in India, this powerful technology can be used for good and evil purposes.[55]

Whilst in the West, increased collection of individual data and the development of ID cards are viewed as an attack on privacy, in developing countries they are seen as a tool for empowerment and to improve access to public services.[56] Yet, criticisms have been raised as to the dual uses and purposes of this initiative including state surveillance.[57]
The technology provides the State with the ability to establish a precise tracking system enabling it to monitor and analyse every element that makes up one's life (sometimes even without an individual's consent or

[54] Jain, A. K., and Pankanti, S., *Beyond Fingerprinting*, American Scientist, September 2008, pp. 79-81. Available at: http://libserver.wlsh.tyc.edu.tw/sa/pdf.file/en/e080/e080p082.pdf

[55] Crook, C., *India's Biometric IDs Put Its Poorest on the Map*, Bloomberg, 23 April 2013. Available: http://www.bloomberg.com/news/2013-04-23/india-s-biometric-ids-put-its-poorest-on-the-map.html

[56] Schneider, H., *Could a program tracking identities of 1.3 billion Indians be the secret to ending poverty?*, The Washington Post, 24 April 2013. Available at: http://www.washingtonpost.com/blogs/wonkblog/wp/2013/04/24/could-a-program-tracking-identities-of-1-3-billion-indians-be-the-secret-to-ending-poverty/

[57] Joshi, D., *India's Biometric Identification Programs and Privacy Concerns*, The Centre for Internet and Society, 31 March 2013. Available at: http://cis-india.org/internet-governance/blog/indias-biometric-identification-programs-and-privacy-concerns

knowledge). This potential directly threatens the right to privacy.[58] "Dataveillance",[59] a term coined by Roger Clarke, expresses the essence of this argument, referring to the systematic monitoring of people's actions or communications through the application of information technology.[60] It is the fact that such surveillance is or could be possible which raises concerns regarding the use of biometric technologies and the storage of the data collected.[61]

To put it simply, such technologies have the power to strip an individual of their identities and humanity by reducing them to data profiles to be followed, monitored and watched.

CASESTUDY: Biometrics, the privacy solution to fast and efficient refugee enrolment?

Biometrics has been part of the work of UNHCR since the early 2000s, but it was in 2010 that the UNHCR announced its policy on biometrics[62], indicating that it should introduce the collection of biometric data as a systematic feature of the registration/enrolment process across UNHCR registrations.[63]

Since then, UNHCR has adopted biometrics enrolment in many of its operations through its "ProGress" system[64] to identify and track refugees including in Burundi, Ethiopia, Kenya, Egypt, Ethiopia, Macedonia, Malaysia, Pakistan, Tanzania[65], and more recently in Liberia[66], Senegal[67], South Sudan[68], and Syria[69].

[58] Van den Hoogen, S. (2009), *Perceptions of Privacy and the Consequences of Apathy: Biometric Technologies in the 21st Century*, Dalhousie Journal of Interdisciplinary Management, Volume 4, Spring 2009, pp. 9. Available at: www.djim.management.dal.ca/issue_pdfs/Vol4/van_den_Hoogen_S.pdf

[59] Roger Clarke, *Information Technology and Dataveillance*, 5 Commun. ACM 498-512, May 1988. Available at: http://www.rogerclarke.com/DV/CACM88.html

[60] Gellman, R., *Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries*, CGD Policy Paper 028, August 2013. Washington DC: Center for Global Development, pp. 20. Available at: http://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0.pdf

[61] Crowe, A., *Development and humanitarian aid initiatives enable surveillance in developing countries*, Privacy International, 11 November 2013. Available at: https://www.privacyinternational.org/blog/development-and-humanitarian-aid-initiatives-enable-surveillance-in-developing-countries

[62] UNHCR, *Policy on biometrics in refugee registration and verification processes*, 20 December 2010, IOM/083/2010 - FOM/083/2010, (Internal)

[63] Vrankulj, A., *UNHCR posts an RFP as it looks to procure a new biometric identity management system*, Biometric Update, 5 March 2013. Available at: http://www.biometricupdate.com/201303/unhcr-posts-an-rfp-as-it-looks-to-procure-a-new-biometric-identity-management-system

[64] Microsoft, *Applying ICT to Support Refugees.* Available at: http://www.microsoft.com/about/corporatecitizenship/en-us/partnerships/united-nations-agencies.aspx

[65] Gelb, A., and Clark, J., *Identification for Development: The Biometrics Revolution*, Center for Gobal Development, Working Paper 315, January 2013. Available at: http://www.cgdev.org/files/1426862_file_Biometric_ID_for_Development.pdf

The use of biometrics technology without comprehensive legal frameworks and protection mechanisms as deployed by UNHCR reflects the risks outlined above. Poor quality data and possibilities of misidentification as a result could mean some refugees would be refused access to health care, food aid and other basic services if they fail to be identified correctly within the biometric database. A field study conducted by Privacy International in 2008 outlined key concerns regarding the poor quality of the data collected for refugees with many not having well-defined fingerprints, and process not being harmonised across camps with different systems being used. One of the key concerns was also the poor reliability of the technology, with systems breaking down without qualified staff to repair them, and staff having to resort to manual registration until biometrics enrolment could be done at a later date.

In addition, because of the nature of refugees, it is even more important that their data is protected and does not fall into the wrong hands. As highlighted in a recent report published by Privacy International, *Aiding Surveillance,*[70] the amassment of data in the context of armed conflict and humanitarian disaster can facilitate surveillance. The result in these circumstances can be tragic if the country of origin is able to access information that identifies refugees.

Such factors must be considered by humanitarian agencies when designing their aid delivery and protection programmes. Privacy and data protection is a right regardless of socio-economic and political contexts. Refugee protection is UNHCR's primary obligation and responsibility.

5. Retention of data: who and why?

The collection of biometric data raises two distinct yet interlinked questions: first, why it needs to be stored in the first place and secondly, who manages and owns the data and for what purpose it will be used.[71]

Recognising the risks of mass data retention, those opposed to biometric databases have argued that there is no need even for their creation to achieve the intended purpose of identification. For example, the Privacy

[66] UNHCR, *UNHCR Begins Biometrics Registration,* 11 March 2013. Available at: http://www.unhcr.org/cgi-bin/texis/vtx/refdaily?pass=463ef21123&id=4f5daf678

[67] UNHCR, *UNHCR distributes biometric ID cards to refugees in Senegal*, 22 October 2013. Available at: http://www.unhcr.org/508536389.html

[68] UNHCR, *Modern technology helps meet the needs of refugees in South Sudan*, 27 December 2012. Available at: http://www.unhcr.org/50dc5a309.html

[69] UNHCR, *UNHCR slashes waiting time, clears backlog of Syrian registrations in Jordan*, 3 October 2013. Available at: http://www.unhcr.org/524d5e4b6.html

[70] Hosein, G., and Nyst, C., (2013) *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries*, Privacy International. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229

[71] Jain, A. K., and Pankanti, S., *Beyond Fingerprinting*, American Scientist, September 2008, pp. 81. Available at: http://www.scientificamerican.com/article.cfm?id=beyond-fingerprinting

Commissioner for Canada encourages local storage of data, particularly biometric data, on smart cards or chips rather than the creation of central databases, arguing that local storage provides the individual with more control over the stored data and who has access to it than a centralised database.[72] This is an approach shared by Germany, which decided not to create a biometric database when it implemented its new biometric passports in 2005.

CASESTUDY – Israel: why a database?

The implementation of a biometric identification system has been discussed in Israel since 2008 and a pilot programme was launched in July 2013. Advocates justify the initiative by arguing it would make forgery and misuse of Israeli citizens' identity more difficult.

Despite the inclusion of privacy safeguards in the programme, critics have argued that the creation of a biometric database was unnecessary. They contend that the simple creation of a smart chip would be sufficient to achieve the programme's objective. The creation of a database not only renders the personal data of millions of Israelis vulnerable to theft, misuse and abuse[73] but also creates avenues for its use for state surveillance purposes.[74]

The mere existence of biometric data could lead to the development of new justifications for its use. This is known as '*mission or function creep*'. As noted in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* personal data should only be used or disclosed for purposes specified at the time of collection.[75] If the data is given solely by an individual for a known purpose, its use for other purposes will violate their rights.

There are also concerns around possible future developments that could permit further assumptions to be drawn from existing biometric data, particularly DNA, such as specific physical features such as hair/eye colour,

[72] Office of the Privacy Commissioner of Canada, *Data at Your Fingertips: Biometrics and the Challenges to Privacy*, OPC Guidance Documents. Available at: http://www.priv.gc.ca/information/pub/gd_bio_201102_e.pdf

[73] Kisch, S., *Israel launches controversial biometric database*, 23 July 2013. Available at: https://www.privacyinternational.org/blog/israel-launches-controversial-biometric-database

[74] Sobelman, B., *Israel launches pilot for ID with biometric database*, Los Angeles Times, 8 July 2013. Available at http://www.latimes.com/news/world/worldnow/la-fg-wn-israel-pilot-id-program-20130708,0,50568.story

[75] Organisation for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Available at: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

height, skin colour, age, as well as genetic dispositions. These additional elements would take profiling to a new level.[76]

Furthermore, the retention of data in databases raises questions as to who can access this information, under what circumstances and for what period of time. The management of access is a particularly difficult and challenging area when multiple agencies can access the data for varying purposes and even more so when these agencies are in different countries. This argument has been made by the UN Special Rapporteur in the context of communications data, but biometric data raises similar concerns:

> *"the United Kingdom, over 200 agencies, police forces and prison authorities are authorized to acquire communications data under the Regulation of Investigatory Powers Act, 2000. As a result, it is difficult for individuals to foresee when and by which State agency they might be subjected to surveillance."*[77]

The case of Mongolia[78] also exemplifies the danger, as the new national identity scheme will be accessible to officials in the electoral commission, tax department, military recruitment office, police, customs, local registrar, and passport office.[79]

Beyond access by governmental and inter-governmental bodies, human rights organisations have raised the alarming prospect of private sector actors having access to data, as private companies are increasingly providing biometrics to developing countries. There is little in place in the current policy and legislative framework on data protection and privacy protection of States and regional entities (i.e. EU, Africa Union, etc.) to protect data from being used in the private sector and to hold companies accountable for human rights violations that result from the technology they develop and sell to governments in developing countries.

VII. Protecting privacy in biometric systems: the opportunities

As argued above, the technology itself can have both positive and negative uses. The aim of this paper is not to discredit the technology or the potential advantages of its use but rather to raise awareness as to its risks and the consequent need for the collection, deployment and storage of biometric data to be regulated. Biometric data will always be at risk of being misused and abused and the rights of individuals will continue to be

[76] Murphy, E., *The government wants your DNA,* Scientific American, March 2013., pp. 76 Available at:

[77] A/HRC/23/40, paragraph 56. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[78] Shinebayar, P., *Mongolia to Roll Out New Smart I.D Card System*, Ub Post, 2011, available at: http://ubpost.mongolnews.mn/index.php?option=com_content&task=view&id=5902&Itemid=36

[79] Hosein. G., *Privacy and developing countries*, September 2011. Available at:

violated unless lawmakers start taking into consideration the privacy impact of biometrics technology.[80]

As identified by Gellman, the increasing use of technology and in particular biometric identification systems has not resulted in corresponding legislation and policy.[81] The Universal Declaration of Human Rights includes the right to privacy but the scope of the right's application is vague. As the UN Special Rapporteur Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue has noted, more entrenched and specific legislation must be adopted to guarantee the recognition of the right to privacy as a human right and to ensure its respect, protection and promotion in all aspects and contexts as well as the need for data protection. [82]

Safeguards must be set down for every step of the process from collection to retention with the right to privacy of individuals at the centre. When collecting biometric data, individuals must be informed about the collection procedure, the intended purpose, and the reason why the particular data is requested and who will have access to their data.

From the onset of the decision to use biometric data, for whatever purpose, the right to privacy and its protection must be at the centre of the debate. In addition, individuals must be given the rights to access, correct and delete data saved in their name at any point. The retention period should be justified and guided by the intended purpose in order to prevent the data's use for new, unintended, purposes.[83] Suggested safeguards to minimise abuse and fraud by limiting who has access to it and the form of the data which is accessible include using encryption systems or saving only the 'template' (digital data) and not the image itself in the case of fingerprints, DNA and iris.

Beyond the biometric data itself, the physical or digital structure in which it is stored must be developed to ensure the safety of the data it contains. If they are to be used, centralised mass data systems must be regulated by strict legislation in order to eliminate the possibility of the government or third parties (i.e. private sector actors) taking advantage of the existence of the data for (new) unforeseen purposes. With regards to DNA data, Murphy has put forward several suggestions to safeguard the right to

[80] McDowell, J., *Something You Are: Biometrics versus Privacy*, Sans Institute, 2000-2002. Available at: http://www.giac.org/paper/gsec/2197/are-biometrics-privacy/103735

[81] Gellman, R., *Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries*, CGD Policy Paper 028, August 2013. Washington DC: Center for Global Development, pp. 1. Available at: http://www.cgdev.org/sites/default/files/privacy-and-biometric-ID-systems_0.pdf

[82] A/HRC/23/40. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[83] Organisation for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Available at: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

privacy, which could be easily adopted for all forms of biometric data. These include:[84]

- Ensuring that stored data is not subject to new tests without explicit permission from a court;
- Requesting that a biological sample is destroyed after being used for its intended purpose or once the 'template' is recorded.

Lastly, along the lines of the OECD principle of accountability[85], an interesting suggestion put forward by Ashbourn includes the development of a biometric constitution, which would establish norms and guidelines to ensure ethical and responsible use of the technology.[86] Even if such a document would not be legally binding, its existence would raise awareness and alert policymakers and individuals as to the impact of the use of such technologies on the right to privacy.

VIII. Conclusion

In developing countries, biometric technology is increasingly seen as an effective tool for facilitating access to social rights but also as a means to strengthen democracy through establishing legal identities for all individuals, thus facilitating access to rights such as voting and opening bank accounts.

However, its deployment in developing countries raises several serious concerns for the human rights of citizens.

First, such technologies are currently often being in deployed in a legal void as privacy rights upheld in national constitutions are not being respected in practice and additional data protection safeguards are failing to match the technological advancements or are simply inexistent.
Secondly, the accuracy and universality of the technology is yet to be proven, but it is developed and used as an infallible system, which means little is done to address the errors that result.

Thirdly, biometric technology provides the necessary data and tools to carry out mass surveillance and profiling of populations. The poor regulation of biometric data means that it is at risk of being used for

[84] Murphy, E., *The government wants your DNA,* Scientific American, March 2013, pp. 72-77. Available at: http://physics.scsu.edu/~dscott/gen/ScientificAmerican/The%20Government%20Wants%20Your%20DNA.pdf

[85] Organisation for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Available at: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[86] Ashbourn, J., *Lack of biometrics standards, loss of personal privacy, Euroscientist Webzine, 27 May 2013.* Available at: http://euroscientist.com/2013/05/lack-of-biometrics-standards-loss-of-personal-privacy/

unintended purposes, which violate the rights of individuals by exposing them to profiling, surveillance, and discrimination.

Biometric data consists of the innate characteristics that make us who we are as human beings and allow us to exist as individuals in a society. The use and misuse of such data has the tragic possibility of denying an individual their identity with no possibility of getting it back and without the possibility of redress for the harm suffered. It is thus essential that biometric technology is regulated and monitored at every level of its use starting with the data collection phase up until it is stored and every time the data is used it must be guaranteed that it is only being used for the intended purpose.

IX. Recommendations

Privacy International calls for the development of standards around the use of biometrics, particularly in developing countries. To this end, we propose an initial set of recommendations that should act as a launching off point for discussion around how to implement biometric technologies in a way that ensure the protection and promotion of the right to privacy.

States should:

1. Prioritise a one-to-one identification procedure in lieu of the one-to-many by evaluating the actual need and added value for data to be stored on a database
2. Establish enforceable safeguards pertaining to every step of the biometrics process, from collection to retention, with individuals' right to privacy as the guiding principle;
3. Develop strict collection and storage systems which ensure that the original biological sample is destroyed once the digital template is created;
4. Ensure individuals have access to about their privacy and personal data rights, including by informing them upon collection of their data of the purpose and use of the data collected, as well as their right to access, correct and delete any data saved on their profile;
5. Limit authorised access to biometric data to specific actors, which access must be strictly based on the purpose for the collection, i.e. information collected for border management should only accessed by migration authorities;
6. Establish strict data retention permissions outlining the fixed time period for the destruction of each data set;
7. Develop secure physical and digital structure infrastructure;
8. Set up independent oversight and monitoring mechanisms to ensure accountability and responsibility of those collecting, storing and retaining biometric data.