Responsible use and sharing of biometric data in counter-terrorism

July 2020

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Cover image: Timo Wielink via Unsplash

CONTENTS

RESPONSIBLE USE AND SHARING OF BIOMETRIC DATA IN COUNTER-TERRORISM

INTRODUCTION

Identification systems across the world increasingly rely on biometric data. In the context of border management, security and law enforcement, biometric data can play an important role in supporting the investigation and prevention of acts of terrorism.

This is clearly reflected in UN Security Council resolutions on counter-terrorism. Notably, in Resolution 2396 (2017), the UN Security Council decided that states shall develop and implement systems to collect and share biometrics data for purposes of counter-terrorism. Similarly, the 2018 Addenda to the Madrid Guiding Principles note the usefulness of biometrics data.

However, biometric data is particularly sensitive and revealing of individual's characteristics and identity. As such it has the potential to be gravely abused.[1] Identification system relying on biometric data are also vulnerable to security breaches, whose consequences for the individuals concerned, and for the overall security of society are extremely grave.

The UN 2018 Addenda to the 2015 Madrid Guiding Principles agree that "biometric systems are a legitimate tool for the identification of terrorist suspects, but the expansive technical scope and rapid development of this technology deserves greater attention as it relates to the protection of human rights (including, but not limited to, the right to be free from arbitrary or unlawful interference with privacy)."

This briefing aims to map out some of the implications of the adoption of identification systems based on biometrics.[2]

[1] See report of the UN High Commissioner for Human Rights, 3 August 2018, UN Doc. A/HRC/39/29, https://undocs.org/A/HRC/39/29

[2] The following observations are based on the organization's long research and expertise on the use of biometrics technologies and their impact on the right to privacy and other fundamental human rights. They take into account and, in places, provide a critical assessment of the UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, compiled by CTED and UNOCT in 2018 in association with the Biometrics Institute, UN Compendium of Recommended Practices

GENERAL CONTEXT OF GOVERNMENTS' USE OF BIOMETRIC DATA

Scores of countries across the world have been rushing to adopt biometric technology for an ever-expanding range of purposes: biometric national identification system, biometric voters' registration; use of biometrics for the delivery of social services and access to health services and delivery of aid.[3]

Use of biometrics technologies for border management, security and surveillance is widespread. Current trends include:

- Employment of ever more sophisticated technologies to capture and analyse biometric data (fingerprints, iris, facial photographs, vein patters, DNA, behavioural biometrics, etc.)
- collection of such biometric data from an increasing number of physical (border crossing, public spaces) and digital (e.g. social media) spaces;
- development of large centralised databases of biometric data and increased interoperability of different databases;
- expansion of the number and type of officials with access to biometric data, including intelligence agencies, national and local police forces, border guards, private security contractors;
- support and pressure for the sharing of biometrics data across national jurisdiction (intelligence sharing.)

Powerful industry, often with closed ties with governments, offer biometrics technology and identification systems relying on biometrics data. For example, a London-based biometrics company was closely involved with the controversial use of biometrics in Venezuelan elections and food rationing.[4] The industry is also often far from transparent. For example, a leading player was banned from World Bank contracts for "corrupt and collusive practices" in Bangladesh.[5]

For the Responsible Use & Sharing of Biometrics in Counter Terrorism, In association with the Biometrics Institute, June 2018, https://www.un.org/sc/ctc/wp-content/uploads/2018/08/Compendium-Final-Draft-June-18.pdf (hereinafter UN Compendium)

[3] For an overview of the concerns, additional examples and references, see PI's work on biometrics, https://privacyinternational.org/learn/biometrics, and Biometrics: friends or foes to privacy, https://www.privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf

[4] See "Your fingerprint for a kilogram of flour: biometric and privacy in Venezuela", Digital Rights No 30, 16 December 2015, https://www.digitalrightslac.net/en/tu-huella-digital-por-un-kilo-de-harina-biometrica-y-privacidad-en-venezuela/

[5] World Bank announces settlement with Oberthur Technologies SA, World Bank https://www.worldbank.org/en/news/press-release/2017/11/30/world-bank-announces-settlement-with-oberthur-technologies-sa

HUMAN RIGHTS' ANALYSIS OF BIOMETRICS DATA IDENTIFICATION SYSTEMS

It is in the above context that the UN Security Council Resolution 2396 (2017) decision that states shall develop and implement systems to collect and share biometric data for purposes of counter-terrorism needs to be placed. This decision adopted under Chapter VII of the UN Charter is legally binding on UN member states. It raises important legal and policy issues with profound implications for the privacy of everyone and for the security of data.

While the Security Council demands that the development of such systems of collection, processing and sharing of biometric data is in compliance with domestic and international human rights law, it does not elaborate on these human rights standards.[6]

This is a significant gap. From the recognition that the collection, processing and sharing of biometric data are all interferences with the right to privacy stems a range of important consequences which needs to be considered prior and during any deployment of such technology.

The UN 2018 Addenda to the 2015 Madrid Guiding Principles concurred that "biometric technology creates particular challenges because of the gap created by technological innovation and the introduction of legislation regulating such technologies. Consequently, States should introduce effective privacy-impact assessments, or review or other oversight bodies, to anticipate and consider the potential impact of such new technologies or applications."[7]

Security or crime-prevention concerns are frequently given as a motivation for states to introduce biometric identity schemes for their populations; these concerns are often presented

[6] As noted by the SR on counter-terrorism "While references to international human rights law have multiplied, the actual impact of such generic language, without clear and explicit human rights guidance provided in the text, is questionable. Such concerns are particularly pertinent, recalling the extensive human rights implications of actions mandated by some of the Security Council resolutions. In the absence of a comprehensive assessment of human rights impact allowing for a meaningful integration of human rights considerations, language stressing the importance of compliance with human rights standards rings hollow and artificial." UN. Doc. A/73/361

[7] Addendum to the 2015 Madrid Guiding Principles, Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council, UN Doc S/2018/1177, https://www.un.org/sc/ctc/wp-content/uploads/2018/12/2018-Addendum-to-the-2015-Madrid-Guiding-Principles_as_adopted.pdf

in the abstract. They can lead to a 'security' argument being used even when there is actually little or no security advantage, for example biometric SIM card registration.[8]

Identification systems increasingly have an impact on people's lives, as the use of systems spreads: they affect many areas of people's lives including the financial system, health, education, and the social security system. In some instances, the use of biometrics excludes people from accessing services, for example the Kenyan government intended to make the Huduma Number a requisite to accessing public services. [9] In India, where Aadhaar is mandatory for government sponsored food rations, when rudimentary fingerprint scanners fail to read the worn fingerprints of manual labourers, such people are denied access to much needed food.[10] The design of a system also has consequences across all of these domains. Thus, the human rights implications of how a biometric identification system is designed and implemented stretch far beyond those within the realm of counter-terrorism. This means that the implications of a design of a system run deep in society, and design decisions made to support counter-terrorism have a far-reaching impact. For example, if a decision is made to design a system so that biometrics can be used for identification (i.e., asking the question, 'who is this?') as opposed to just authentication (i.e., asking the question, 'is this person who they say they are?'), this could have much broader implications for human rights abuses.

The sections below seek to explore some of the human rights aspects of the processing of biometric data that needs to be considered.

[8] See PI's work on SIM card registration, https://privacyinternational.org/topics/sim-card-registration

[9] No Huduma number, no services: Bill proposes, http://news.callapr.co.ke/no-huduma-number-no-services-bill-proposes/

10 India's Biometric ID System Has Led To Starvation For Some Poor, Advocates Say, https://www.npr.org/2018/10/01/652513097/indias-biometric-id-system-has-led-to-starvation-for-some-poor-advocates-say

INADEQUATE NATIONAL LEGAL FRAMEWORK

Processing of biometric data, including collection, analysis, storing, sharing, must be prescribed by law and limited to that strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the intrusion with someone's privacy.

Data protection law is a necessary but insufficient safeguard against abuse. As of January 2019, over 120 countries around the world have enacted comprehensive data protection legislation.[11] Modern standards of data protection recognise the need to afford extra protection to biometric data.[12] The most comprehensive data protection regulation in the world, the General Data Protection Regulation (GDPR), treats biometric data used for identification purposes as "special category data", meaning it is considered more sensitive and in need of enhanced protection.[13]

Many national laws, however, do not even mention biometric data, and do not explicitly characterise biometric data as personal and sensitive data. Additionally, many of these laws contain significant exemptions. Many do not apply to processing of data by intelligence agencies and law enforcement, and even when they do, they contain wide reaching exemptions for purposes such national security and prevention or investigation of crime.[14] Even country with modern data protection legislation, such as the United Kingdom of Great Britain and Northern Ireland, do not adequately regulate the processing of biometric data, such as the use of facial recognition technology by the police in public places.[15]

[11] Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (5th Ed 2017) (January 31, 2017). (2017) 145 Privacy Laws & Business International Report, pp 14-26.https://ssrn.com/abstract=2992986

[12] The Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data ("Convention 108 +"). Article 6, provides that biometric data uniquely identifying a person shall only be allowed where appropriate safeguards are enshrined in law, complementing those of Convention 108 +. The European General Data Protection law ("GDPR"). Article 9 prohibits the processing of biometric data for the purpose of uniquely identifying a natural person subject to limited exceptions. The Brazilian General Data Protection Law ("LGPD"), Federal Law no. 13,709/2018, Article 5 also provides special protections for biometric data.

[13] See UK ICO, Special Category Data, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

[14] See, for example, PI, UK Data Protection Act 2018 – 339 pages still falls short on human rights protection, 13 June 2018, https://privacyinternational.org/news-analysis/2074/uk-data-protection-act-2018-339-pages-still-falls-short-human-rights-protection

[15] See PI, Our response to the Westminster Hall Debate on Facial Recognition, 30 April 2019, https://privacyinternational.org/advocacy/2835/our-response-westminster-hall-debate-facial-recognition

PI believes that in most countries national laws do not adequately regulate the use and sharing of biometric data. They fall short of applicable international human rights law and they fail to effectively address the security risks arising from misuse of biometric data, especially at scale.

NECESSITY AND PROPORTIONALITY ASSESSMENT

Any interference with the right to privacy needs to comply with the principles of necessity and proportionality.

The principle of necessity "*implies that restrictions must not simply be useful, reasonable or desirable to achieve a legitimate government objective*," but rather, that "*a State must demonstrate in 'specific and individualized fashion the precise nature of the threat' that it seeks to address, and a 'direct and immediate connection between the expression and the threat'*."[16]

The use of biometric data presents a unique set of concerns. These are neatly summarised in the UN High Commissioner for Human Rights report on the right to privacy in the digital age, as biometric:

> 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.[17]

The report recommends that states, *inter alia*

> Ensure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim.[18]

It should be noted that the creation of a national biometric identification system is not, in itself, a legitimate aim for the collection of biometric data on scale. Such an identification system cannot be seen as a legitimate aim in itself.

16 UN CCPR, General Comment No. 34: General comment no. 34, Article 19, Freedoms of opinion and expression, UN Doc. CCPR/C/GC/34, 12 September 2011, para 35

[17] UN High Commissioner for Human Rights (2018) The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights, 3 August 2018, UN Doc. A/HRC/39/29, https://undocs.org/A/HRC/39/29

[18] UN High Commissioner for Human Rights (2018) The right to privacy in the digital age, report of the United Nations High Commissioner for Human Rights, 3 August 2018, UN Doc. A/HRC/39/29, https://undocs.org/A/HRC/39/29

In practice, applying the principles of necessity and proportionality mean adopting the least intrusive means to achieve the relevant legitimate aim, in this context: the prevention and investigation of acts of terrorism. It also requires that any measure is accompanied by legal, procedural and technical safeguards to minimise the interference with privacy.

Necessity and proportionality assessments should play a significant role in relation to decisions to create centralised databases, and in the rules that govern retention and access of biometric data.

CENTRALISED DATABASES OF BIOMETRIC DATA

Governments and industry are often supporting the creation of large centralised databases containing biometrics information. For example, the Aadhaar biometric identification system in India contains the fingerprints, iris scans, and photographs of over 1.1 billion people.

This trend is supported, for example, in the UN Compendium where it notes that the

> lawful integration of all national law enforcement biometric databases into a 'national watch list' configuration […] would expose the optimum amount of relevant data to watch list searches (...)[19]

However, large centralised databases of biometric data have often failed to pass a proportionality assessment under human rights law.

That is because there is a significant difference between storing biometric data locally than storing them in a centralised database, with the latter being significantly more intrusive to privacy.[20] For example, biometric passports that store the biometric details of an individual on a chip in the passport, rather than a centralised database, are used in the UK. Storing biometric data locally allows for the use of biometrics for *authentication* (to be able to be sure that the person with the document is who they claim to be) but prevents its use from the far more intrusive process of *identification* (finding the identity of a person when it is not known).[21]

Data protection authorities in Europe have raised grave reservations about the proportionality of proposals that would lead to the storage of biometric data on all non-nationals applying for a visa or residence permit in centralised databases for the purpose of carrying out subsequent checks on illegal immigrants (particularly those without documents).[22]

---

[19] UN Compendium of Recommended Practices For the Responsible Use & Sharing of Biometrics in Counter Terrorism, In association with the Biometrics Institute, June 2018, p 61, https://www.un.org/sc/ctc/wp-content/uploads/2018/08/Compendium-Final-Draft-June-18.pdf

[20] As the London School of Economics report on the UK Identity Card, stated, "There is an enormous difference in the implications for the human right to privacy between this type of system, and one where a biometric is only stored locally in a smartcard ", LSE (2005) The Identity Project: an assessment of the UK Identity Cards Bill and its implications, p 255. http://www.lse.ac.uk/management/research/identityproject/identityreport.pdf

[21] See Research briefing, UK House of Commons, Biometric passports, 10 February 2012, researchbriefings.files.parliament.uk/documents/SN04126/SN04126.pdf

[22] Article 29 Working Party, Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS), the European Commission, August 11, 2004, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp96_en.pdf

Commenting on the Kuwaiti Law No. 78 (2015) on counter-terrorism, which requires nationwide compulsory DNA testing and the creation of a database under the control of the Minister of the Interior, the UN Human Rights Committee found that it imposes unnecessary and disproportionate restrictions on the right to privacy.

It is worth noting that the recommendations of the UN Human Rights Committee to the Kuwaiti governments included amending the law

> with a view to limiting DNA collection to individuals suspected of having committed serious crimes and on the basis of a court decision; (b) ensure that individuals can challenge in court the lawfulness of a request for the collection of DNA samples; (c) set a time limit after which DNA samples are removed from the database; and (d) establish an oversight mechanism to monitor the collection and use of DNA samples, prevent abuses and ensure that individuals have access to effective remedies.[23]

[23] Human Rights Committee, Concluding observations on the third periodic report of Kuwait, 11 August 2016, UN doc. CCPR/C/KWT/CO/3

RETENTION AND ACCESS OF BIOMETRIC DATA

Retention of biometric data

Under international law, indiscriminate retention of personal data, including biometric data, is never proportionate and necessary, even if when governments seek to justify it on grounds of protection of national security, including threat of terrorism acts.

In the case of *S and Marper v. UK*, the European Court of Human Rights found there had been a violation of the right to privacy by the UK, as a result of the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences which failed to strike a fair balance between the competing public and private interests.[24]

Access to biometric data and mission creep

Strictly linked to the necessity and proportionality assessment are the concerns related to the repurposing of biometric databases (often described as mission creep). The mere existence of biometric data in a centralised identification system could lead to the development of new justifications for its use and seeking to broaden the authorities with access to it.

Often in the name of national security and counter-terrorism, states have sought to allow law enforcement and security agencies access to databases designed for purposes unrelated to counter-terrorism and prevention or investigation of crimes.

For example, in 2004, the European Asylum Dactyloscopy Database ("EURODAC") was established to facilitate the application of the Dublin Regulation, which determines the EU

[24] The Court emphasised:

> The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ... The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse ...The above considerations are especially valid as regards the protection of special categories of more sensitive data ...and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family

S. and Marper v. The United Kingdom, App. Nos. 30562/04 and 30566/04, Judgment, 4 December 2008, European Court of Human Rights, para 103

Member State responsible for examining an asylum application. In 2009, EU Member States proceeded to decide that EURODAC should made accessible for law enforcement purposes in order to fight terrorism, a purpose for which the data processed was never intended, as noted by the European Data Protection Supervisor ("EDPS") in its Opinion on the matter. The EDPS's opinion also raised that the use of EURODAC for law enforcement purposes, and specifically for terrorism, means that a particular vulnerable group in society, namely applicants for asylum, could be exposed to further risks of stigmatisation, even though they are "not suspected of any crime" and "are in need of higher protection because they flee from persecution."[25]

There have been some cases where privacy concerns about access to centralised databases by the police or security services have led to judgments limiting such access. For example, in India, Section 33(2) of the Aadhaar Act allowed, for the purpose of national security, access to the Aadhaar database (including biometrics) if authorised by an intelligence officer of Joint Secretary or above. The *Aadhaar* judgement ensured that anybody who's data was accessed in this way would be subject to a hearing.[26]

Interoperability and integration of biometric databases

Similar concerns apply in relation to the trend by governments to develop 'interconnectivity' of different biometric databases. This trend is generally noted as positive by security actors. The UN Compendium talks positively of this aggregation of

> the aggregation of disparate, single-mode databases and has evolved, in some countries and regions, into state-of-the-art, replacement networks that feature interconnected multi-modal databases designed to service a range of business needs across law enforcement, border management and other government functions at both a national and international level.[27]

In fact, the UN Compendium suggests the integration of biometric databases as a solution to predict terrorist activities:

> The traditional biometric databases […] were designed to be reactive and pose investigative questions based on identity and current or past activity such as "Are you known to us, who are your associates and what have you done?" Integrated biometric databases can obviously answer the same questions but they may also be used pro-actively to infer and predict potential future actions and associations i.e. "What are you and your associates planning or likely to do and when, where?" A comprehensive and careful analysis of all outputs across the network is therefore essential and can be a

[25] European Data Protection Supervisor, Opinions, 2010/C, C92/1, 10 April 2010, para 29m, https://edps.europa.eu/sites/edp/files/publication/09-10- 07_access_eurodac_en.pdf

[26] Dissenting judgement of Justice Chandrachud, Writ Petition (Civil) No. 494 Of 2012, Justice K.S. Puttaswamy (Retd.) and another versus Union of India and Others, para 219 (c) and (d), https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[27] UN Compendium of Recommended Practices For the Responsible Use & Sharing of Biometrics in Counter Terrorism, In association with the Biometrics Institute, June 2018, p 63, https://www.un.org/sc/ctc/wp-content/uploads/2018/08/Compendium-Final-Draft-June-18.pdf

> critical success factor in evaluating and anticipating terrorist activity when coupled with other intelligence.[28]

While there is some recognition of the need to develop legal framework in order to allow such interoperability of database, there is no reference to the limits that human rights law, and in particular data protection standards, impose to such measures. Limits that are necessary to prevent the mission creep and the accompanying human rights abuses.

[28] UN Compendium of Recommended Practices For the Responsible Use & Sharing of Biometrics in Counter Terrorism, In association with the Biometrics Institute, June 2018, p 67, https://www.un.org/sc/ctc/wp-content/uploads/2018/08/Compendium-Final-Draft-June-18.pdf

SECURITY AND BREACHES OF BIOMETRIC DATA

Unlike a password, an individual's biometrics cannot be easily changed.[29] As a result rectification of the unauthorised access to biometric data are either impossible or incurring a significant cost.

Biometric data breaches seriously affect individuals in a number of ways, whether identity theft or fraud, financial loss or other damage. The EU Fundamental Rights Agency found in relation to a central national database "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."[30]

In January 2018, it was reported that access to the entire Aadhaar database – including the names, addresses, phone numbers, and photographs, but not fingerprint or iris scan data – was being sold for 500 rupees on a WhatsApp group.[31]

A breach of the US government's Office of Personnel Management – the agency that handles the security clearances of civilian workers – was announced in 2015. The records of 21.5 million people were stolen, including the fingerprints of 5.6 million federal employees[32]. A security expert said that this risked undercover operatives: "A secret agent's name might be different. But they'll know who you are because your fingerprint is there. You'll be outed immediately."[33] The breach of one of the most sensitive biometric databases maintained by one of the most well-resourced and security-focused governments in the world with advanced access control

[29] The dissenting judgment from Justice Chandrachud of the Supreme Court of India when ruling on the Aadhaar case recognised that: "Once a biometric system is compromised, it is compromised forever.... Passwords and numbers can be changed, but how does one change the basic biological features that compromise biometrics in the event that there is a theft?" Dissenting judgement of Justice Chandrachud, Writ Petition (Civil) No. 494 Of 2012, Justice K.S. Puttaswamy (Retd.) and another versus Union of India and Others, para 132 https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

[30] European Union Agency for Fundamental Rights, Fundamental rights implications of storing biometric data in identity documents and residence cards, FRA Opinion –3/2018, 5 September 2018, p 14 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-opinion-biometric-data-id-cards-03-2018_en.pdf

[31] See "Rs 500, 10 minutes, and you have access to billion Aadhaar details", *the Tribune*, 4 Jan 2018, https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html

[32] See Associated Press Washington, "US government hack stole fingerprints of 5.6 million federal employees", The Guardian, 23 September 2015, https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints

[33] See https://money.cnn.com/2015/07/10/technology/opm-hack-fingerprints/

protocols raises urgent questions about the ability of less well-resourced actors to appropriately defend against such breaches.

In August 2019, the fingerprints of over 1 million people and facial recognition information, was discovered when a database belonging to Suprema, a company used by the UK Metropolitan police, was breached. Suprema's Biostar 2 platform was integrated to the AEOS access control system which is used by an estimated 5,700 organisations in 83 countries including banks, defence contractors and governments. Security researchers found that the database was unprotected and mostly unencrypted. The researchers had access to 23 gigabytes-worth of data which included fingerprint data, facial recognition data and face photos of users.[34]

The risks associated with unauthorised access to biometric data also threaten the effectiveness of the counter-terrorism measures, particularly when such breaches are not promptly reported and notified to independent oversight bodies and individuals concerned.

The 2018 Addenda and the UN Compendium include among the recommended practices conducting regular risk assessments of the end-to-end process of the biometric applications. Periodic risk assessments are fundamental, but as fundamental is the need to conduct risk assessment prior to the implementation and application of identification systems based on biometric data and embed a privacy and security in the design of such systems.

[34] Josh Taylor, "Major breach found in biometrics system used by banks, UK police and defence firms", *The Guardian*, 14 August 2019, https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

INTERNATIONAL SHARING OF BIOMETRIC DATA AND ACCESS TO BIOMETRIC DATABASES

The UN Security Council resolution 2369(2017):

> encourages Member States to share this [biometric] data *responsibly* among relevant Member States, as appropriate, and with INTERPOL and other relevant international bodies. (*emphasis* added)

PI recognises the importance and benefit of intelligence sharing in the context of preventing and investigating terrorism or other genuine, serious threats to national security. The organisation is concerned, however, that unregulated, unfettered and unwarranted intelligence sharing poses substantive risks to human rights and to the democratic rule of law.

Regulation of the sharing of personal data, such as biometric data, across jurisdiction is within the purview of international human rights law, and in particular data protection. However, the qualification of the sharing of biometric data with the word "responsibly" in the UN Security Council resolution 2369(2017) offers little guidance on states, particularly of how they should comply with their existing obligations under international human rights law.

The UN Compendium identifies some principles that should regulate such sharing of biometric data, focusing on the necessity of a clear legal framework and the limits on the use of such data. However, its recommended practice clearly favour the maximum sharing of biometric data across borders.[35]

In its November 2018 briefing to the UN Counter-Terrorism Executive Directorate,[36] PI identified some additional minimum safeguards that states must introduce in order to ensure their intelligence sharing laws and practices are compliant with applicable international human law (notably Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Right.[37] Biometric data, because of its sensitivity (as

[35] UN Compendium of Recommended Practices For the Responsible Use & Sharing of Biometrics in Counter Terrorism, In association with the Biometrics Institute, June 2018, p 72, https://www.un.org/sc/ctc/wp-content/uploads/2018/08/Compendium-Final-Draft-June-18.pdf

[36] PI, Minimum safeguards on intelligence sharing required under international human rights law: A report to the UN Counter-Terrorism Committee Executive Directorate, November 2018, https://privacyinternational.org/sites/default/files/2019-07/Submission%20to%20UNCTED_Minimum%20standards%20on%20intelligence%20sharing.pdf

[37] PI is mindful that intelligence sharing may facilitate a range of other serious human rights abuses as well as violations of international humanitarian law.

noted above) requires even stricter limitations and safeguards to ensure its sharing across jurisdiction comply with international human rights law.

FOREIGN ASSISTANCE IN THE PROMOTION OF BIOMETRIC TECHNOLOGIES

The UN Security Council Resolution 2369(2017):

> calls upon other Member States, international, regional, and sub-regional entities to provide technical assistance, resources, and capacity building to Member States in order to implement such systems [to collect biometric information].

Indeed, there is recognition that developing identification system to support border security and information-sharing requires significant resources and expertise. As noted by the UN 2018 Addenda to the 2015 Madrid Guiding Principles "many States have found that implementation of their obligations relating to […] biometric systems requires legal frameworks, skills, capacity, expertise and equipment that they do not currently possess."[38]

However, providing such technical assistance without adequate consideration for the human rights impact of this technology on individuals in the receiving state is of significant concern.

By way of example, the US National Strategy to Combat Terrorist Travel[39] as a very strong focus on advancing the use of biometric technologies to detect and prevent suspected terrorists from travelling into the US. The strategy envisages supporting foreign governments to deploy biometric technologies. It foresees an approach whereby the US government support the development of these technologies together with the establishment of information exchange.

The US Department of State has provided biometric traveller screening systems developed by defence contractor Booz Allen Hamilton – the Personal Identification Secure Comparison and Evaluation System - to Burkina Faso, Cameroon, Chad, Djibouti, Ethiopia, Kenya, Mali, Niger, Tanzania, Uganda, Iraq, Jordan, Yemen, Maldives, Afghanistan, and North Macedonia.[40] The US Department of Defense has funded a biometric system for the Afghan National Defense and Security Forces consisting of numerous components, including computers; webcams; and fingerprint, palm, and iris scanners. The biometrics system is used to store and manage personal

[38] See Addendum to the 2015 Madrid Guiding Principles, Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council, UN Doc S/2018/1177, https://www.un.org/sc/ctc/wp-content/uploads/2018/12/2018-Addendum-to-the-2015-Madrid-Guiding-Principles_as_adopted.pdf

[39] US Whitehouse Strategy, December 2018 https://www.whitehouse.gov/wp-content/uploads/2019/02/NSCTT-Signed.pdf

[40] Bureau of Counterterrorism and Countering Violent Extremism, Country Reports on Terrorism 2016, US Department of State, Washington DC, https://www.state.gov/j/ct/rls/crt/2016/index

identification information that can be used "to support law enforcement, security, and intelligence operations".[41]

At the same time, the EU and some European member states are spending billions of Euros transferring surveillance and border control capabilities to foreign countries to ensure they stop people migrating to their countries. Not only have such policies facilitated human rights abuses, they have allowed authoritarian leaders to use migration control to gain political and economic support.[42]

The EU's Trust Fund for Africa provided €28 million to develop a universal nationwide biometric ID system in Senegal by funding a central biometric identity database, the enrolment of citizens, and the interior ministry in charge of the system.[43] Under the EU Trust Fund for Africa, €55 million was also allocated for enhancing border control measures in Tunisia and Morocco for the 'purchase and maintenance of priority equipment, capacity building and development of necessary standards and procedures at national level', which includes the development of "an IT infrastructure collecting, archiving and identifying digital biometrics."[44] Similarly, €30 million was allocated to fund Cote d'Ivoire's a universal biometric identity system with the explicit aim of doing so in order to identify Ivorians irregularly residing in Europe in order "to organize their return more easily".[45]

The Trust Fund also provided €5 million to:

> increase security levels and migration management capabilities in Cape Verde and Guinea Bissau' by providing technical assistance, training programmes, institutional capacity building, legislation, and equipment. Specific objectives include training government agencies in issuing and checking identity documentation and increasing 'the automatic collection of biographical and biometric elements of citizens.[46]

[41] See US Government Accountability Offcie (Gao), Afghanistan Security: U.S.-Funded Equipment for the Afghan National Defense and Security Forces, 10 August 2017, https://www.gao.gov/assets/690/686477.pdf

[42] Malik, N, "Bashir Comes in From the Cold", *Foreign Policy*, 31 July 2016, http://foreignpolicy.com/2016/07/31/europes-new-best-friend-in-africa-is-an-indicted-genocidal-war-criminal/

[43] See DEC - Programme d'appui au renforcement du système d'information de l'état civil et à la création d'un fichier national d'identité biométrique, T05-EUTF-SAH-SN-07, https://eutf.akvoapp.org/en/project/5620/#report

[44] See Action Document for the implementation of the North Africa Window, T05-EUTF-NOA-REG-07, https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/t05-eutf-noa-reg-07.pdf

[45] See Document d'action du Fonds Fiduciairede de l'UE, Annexe IV à l'Accord Instituant le Fonds Fiduciaire 'European Union Emergency Trust Fund for stability and addressing root causes of irregular migration and displaced persons in Africa', et ses règles internes, https://ec.europa.eu/trustfundforafrica/sites/euetfa/files/t05-eutf-sah-ci-01.pdf

[46] See DEC - Modernizing and strengthening secure identity chains and documental security (GESTDOC), T05-EUTF-SAH-REG-14, https://eutf.akvoapp.org/en/project/7139/#report

Meanwhile, Chinese companies export highly invasive facial recognition and other biometric identification technology around the world, often supported by technical assistance and loans provided by government authorities.[47] According to Freedom House, Chinese firms have provided high-tech tools of surveillance to governments that lack respect for human rights. In 18 of the 65 countries assessed by Freedom House, enterprises such as Yitu, Hikvision, and CloudWalk are combining advances in artificial intelligence and facial recognition to create systems capable of identifying threats to "public order." [48]

As PI's recent report revealed this commercial export of Chinese technology is part of China's formalised cyber diplomacy which has focused on the fight against 'cyberterrorism,' a category of online activities that corresponds with China's unusually broad definition of terrorism. Cyber terrorism initially centred on the activities of the Shanghai Cooperation Organisation but has recently extended to include the utilisation of multilateral bodies such as the UN, BRICS, and APEC.[49]

These examples are part of the broader trends identified by PI where countries with the most extensive security and military agencies are transferring electronic surveillance capabilities, including biometric technology, around the world, without due regard to human rights impact. While such cooperation and assistance can strengthen the capacity in recipient states to investigate and prevent terrorist acts, there are also huge human rights and security risks.

Many of the recipient countries and agencies have a documented history of human rights abuses, meaning that in many cases, without appropriate safeguards and accountability, such assistance can facilitate gross abuses - something recognised by the US Government Accountability Office and by a UK Parliamentary Home Affairs Committee. Assistance can reinforce authoritarianism, undermine governance, facilitate corruption, can illegitimately equip non-state actors, and exacerbate inter- communal tensions.[50]

[47] See Paul Mozur, Jonah M. Kessel and Melissa Chan, "Made in China, Exported to the World: The Surveillance", *The New York Times,* 24 April 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

[48] See Freedom on the Net 2018, The Rise of Digital Authoritarianism https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

[49] PI, How China is supplying surveillance technology and training around the world, February 2019, https://privacyinternational.org/sites/default/files/2019-09/Privacy%20International_Survey2.1.pdf

[50] See PI, Teach 'em to Phish: State Sponsors of Surveillance, 2018, https://privacyinternational.org/report/2159/teach-em-phish-state-sponsors-surveillance

Recommendations

The UN counter-terrorism strategy and the broad UN counter-terrorism agenda strongly support the introduction of biometric identification systems as measures to counter terrorism.

UN Security Council resolutions, the UN Addenda and the UN Compendium all include, with various degrees, references to the need to respect human rights but their recommended best practices are by-and-large supportive of governments and industry trends towards ever expanding application of biometric systems and the sharing of biometric data within states, internationally and regionally.

In light of the above, PI makes the following recommendations:

- There is need for the UN Counter-Terrorism Executive Directorate to develop, in cooperation with the UN Special Rapporteur on counter-terrorism and human rights, precise and comprehensive human rights guidelines on the implementation of the decision by the Security Council 2369 (2017) demanding that states develop and implement systems to collect biometric data, with particular focus on ensuring compliance with international human rights and promoting the security of personal data.
- The processing of biometric data, including collection, analysis, storing, sharing must be prescribed by law and limited to what is strictly and demonstrably necessary to achieve a legitimate aim.
- Laws that protect biometric data must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the intrusion with someone's privacy.
- There is need to guard against function creep, which is the unqualified support for ever expanding biometric databases (and the integration of existing ones) coupled with expanding access to the data to a wider range of law enforcement and security agencies.

States adopting biometric technologies for counter-terrorism purposes must not only receive technical assistance but must also receive assistance in the development of robust human rights safeguards/due diligence, ending in supporting the policies of states which are exporting surveillance technology with little regards to their implication for human rights.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org