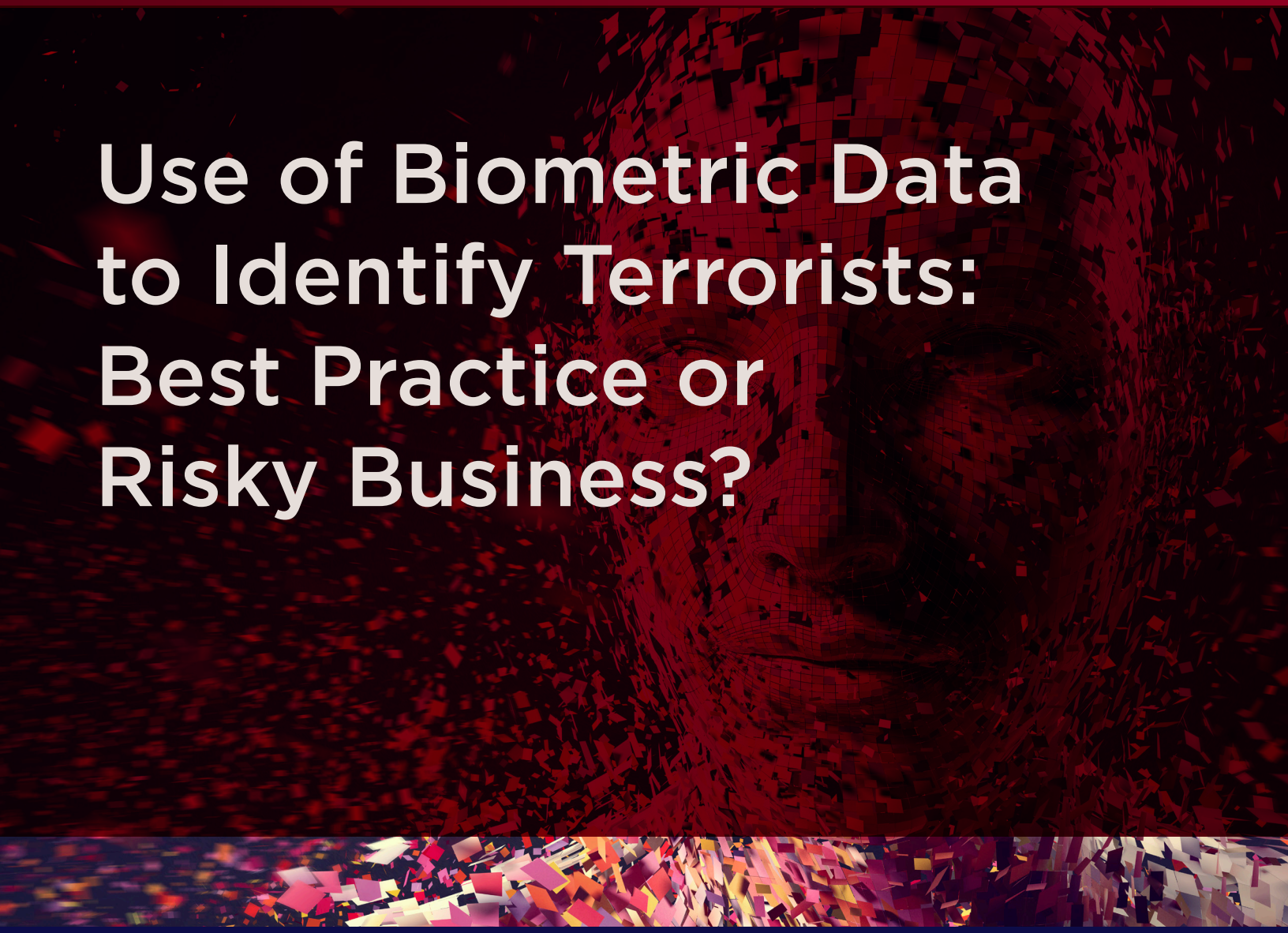
HUMAN RIGHTS CENTER
UNIVERSITY OF MINNESOTA



Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?

Report prepared under the aegis of the Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism

Dr. Krisztina Huszti-Orbán and Prof. Fionnuala Ní Aoláin

Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?

This report was written by Dr. Krisztina Huszti-Orbán, with Prof. Fionnuala Ní Aoláin.

Dr. Krisztina Huszti-Orbán is a Research Fellow at the Human Rights Center at the University of Minnesota Law School and Senior Legal Advisor to the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

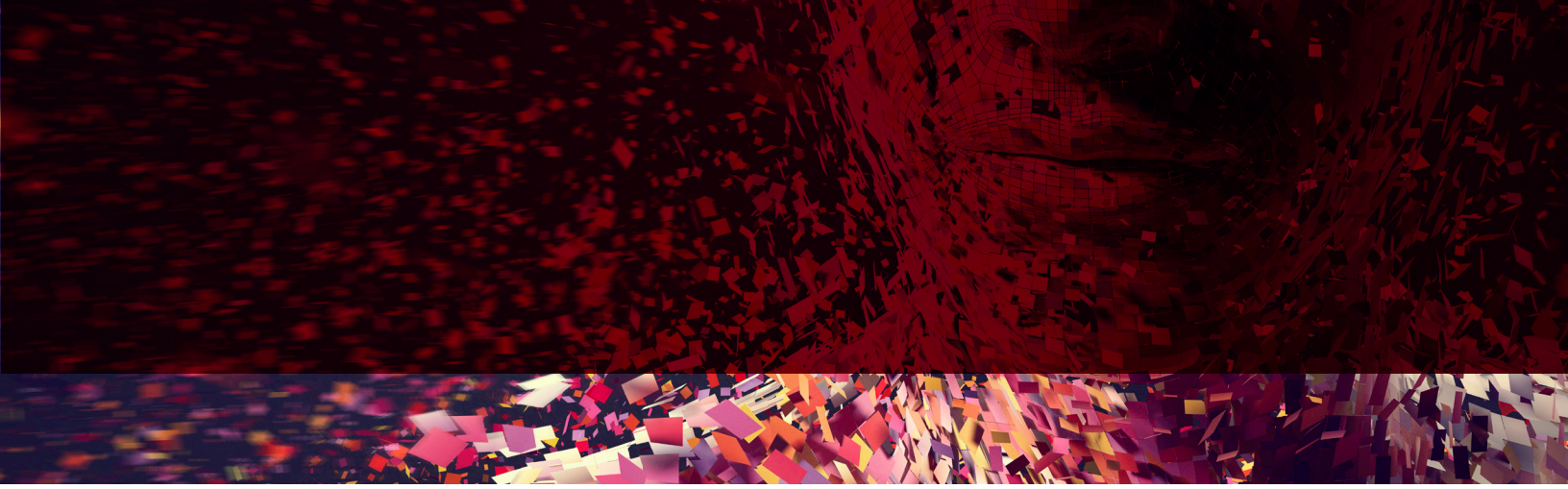
Prof. Fionnuala Ní Aoláin is Regents Professor and Robina Professor of Law, Public Policy and Society at the University of Minnesota Law School, Faculty Director of the University of Minnesota Human Rights Center, and jointly Professor of Law at the Queens University of Belfast, Northern Ireland. She is the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2017-).

The Human Rights Center would like to thank for the pro bono research support by the Minnesota Advocates and DLA Piper and for the research, translation and other support provided by Kathryn Campbell, Katie Smith, Caroline Sell, Zakaria Almulhim, Harry Gray Carvo and Lucas Morel.

The report benefited from multi-stakeholder consultations held at RightsCon 2019 in Tunis, Tunisia.

Undertaking this work would not have been possible without the financial support provided by the Knowledge Platform on Security and Rule of Law's Knowledge Management Fund.

TABLE OF CONTENTS



Introduction

The distinct value and practical benefits of the use of biometric data is increasingly acknowledged including in the context of addressing trans-border challenges in law enforcement and intelligence gathering, border management, evidentiary and forensic use. This trend is also reflected in the regulatory efforts by the United Nations Security Council via resolution 2396[1] requiring States to "develop and implement systems to collect biometric data" in order to "responsibly and properly identify terrorists, including foreign terrorist fighters".

Despite the rapid advancement of biometric technology and its widespread usage, human rights analysis and guidance on its use remains limited and underdeveloped. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (hereinafter: Special Rapporteur) has repeatedly highlighted this shortcoming, including in her report to the 73rd session of the General Assembly[2] and stressed the need for granular rule of law and human rights-based analysis in relation to the extensive obligations imposed by the Security Council, with particular emphasis on resolution 2396. She has highlighted the requirements relating to biometric systems and data as a distinct priority in light of the particular challenges raised in connection with their use.

Bridging the human rights guidance gap concerning the use of biometric tools in the counter-terrorism context is essential to advance compliance with existing State human rights obligations. Such guidance would contribute towards ensuring that legislative and policy efforts spurred by resolution 2396 uphold the rule of law as the bedrock of effective and sustainable counter-terrorism efforts. It is particularly salient given the changed international and regional peace and security risk environment linked to having foreign fighters, formerly affiliated with the Islamic State in Iraq and the Levant (ISIL/Da'esh) and its satellites, return to their countries of origin or travel to other conflict zones. This development has spawned challenges in developing and implementing effective screening, prosecution, rehabilitation, and reintegration strategies, in light of regulatory developments led by the United Nations Security Council.

Against this background, this report explores the human rights implications of the use of biometric tools and data, with particular focus on challenges to their human rights-compliant deployment in the context of preventing and countering terrorism and violent extremism. The report provides a summary of the ways in which biometric data and tools are employed, including in the context of counter-terrorism. It then sets out the human rights implications of the use of biometrics, including but not limited to, the rights to privacy and data protection and outlines both State obligations and business responsibilities in this regard. Finally, it presents a set of recommendations on measures towards promoting a human rights-based approach to the use of biometric tools and data.

A. Biometrics and their use

The use of biometric tools and data has garnered considerable attention in past years. News articles, analyses and discussion frequently mention 'biometrics', with fingerprints, facial and voice recognition, iris scans or DNA flagged as examples. But, what exactly are 'biometrics' and what is their use?

1 S/RES/2396 (2017).
2 A/73/361

Biometrics is the scientific discipline concerned with measurements and metrics related to biological or behavioral human characteristics, that are commonly possessed by all human beings while also being highly representative of a person, thus allowing for the identification of individuals.[3] Such markers may be related to a person's physiological characteristics, such as finger or palm prints, DNA, and facial, iris, or retina recognition (i.e. biological biometrics). Others are linked to behavioral patterns, such as recognition based on a person's gait (behavioral biometrics or 'behaviometrics'). As biometric identity attributes are both unique to a person and stable over time,[4] they provide for a singularly useful tool for accurate and efficient identification[5] and authentication.[6] These characteristics[7] are also what makes such data particularly sensitive, thus creating a need for secure systems for data storage and processing to mitigate the risk of unauthorized access.

1. The evolution of biometrics

Despite biometrics-related queries and concerns having entered public debates relatively recently, biometrics as a concept and tool are not novel, with the history of biometrics going back for centuries. "Early" biometrics, such as fingerprints or identification based on photographs, have been used by public authorities since the 19th century. Biometric systems have widely been adopted in the former colonial world, with colonial authorities advocating for the use of fingerprints for identification purposes, arguing problematically, *inter alia*, that "natives [were] too illiterate for the common use of signatures."[8] This has led to biometric registration becoming an alternative to documentary registration within the British Empire, at times also involving coercive biometric registration.[9] The use of biometrics was not restricted to colonial contexts: the Metropolitan Police in the United Kingdom started fingerprinting criminal suspects in 1901,[10] followed by French police in 1902,[11] and the New York state penitentiary system in 1903.[12]

Biometric tools have become a staple for contemporary use by security sector actors. This includes the military and law enforcement, in the context of criminal justice processes, border management, and civil identification, to name a few. In recent decades, automation has turned biometrics into even more powerful instruments.[13]

While biometric tools have successfully been used for legitimate public interest purposes and have played an important role in criminal justice processes, they have also been employed in connection with gross human rights violations, atrocity crimes, and by oppressive and authoritarian regimes. Nazi German practice included tattooing camp serial numbers on Jewish inmates held in concentration camps, a practice introduced in order to "identify the bodies of registered prisoners who had died."[14] Nazi authorities have also imposed identification cards that included identifying marks allowing for security forces to easily pinpoint those of Jewish origin.[15] The Rwandan genocide was similarly facilitated by the

3 The International Organization for Standardization (ISO) defines biometric characteristics as "biological and behavioural characteristic of an individual from which distinguishing, repeatable biometric features" that "can be extracted for the purpose of biometric recognition." *See* ISO/IEC 2382-37:2017(E). The Biometric Consortium set up by the US Government defines biometrics as "the automated recognition of individuals based on their behavioral and biological characteristics." *See* National Institute of Standards and Technology, 'Biometrics', available at https://csrc.nist.gov/glossary/term/Biometrics (visited 20 February 2020); 'A further note on the definition of biometrics', available at https://www.ncbi.nlm.nih.gov/books/NBK219892/box/bbb00012/?report=objectonly, (visited 20 February 2020). India's draft Personal Data Protection Bill defines biometrics as "facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person." *See* The Personal Data Protection Bill, 2019, Bill no. 373 of 2019, Chapter I, article 3(7), available at https://prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf (visited 20 February 2020). The UK's Biometrics Strategy offers the following definition: "the recognition of people based on measurement and analysis of their biological characteristics or behavioural data." *See* Home Office Biometrics Strategy (2018), Chapter 1.

4 They are however not necessarily immutable and may be subject to change during a person's lifetime. This is particularly pertinent when dealing with behavioral biometrics but may be relevant also in relation to biological biometrics which may also undergo alteration as a result of the growing or aging process as well as changes in a person's health (due to illness or accident).

5 For the purposes of this report, identification is used to mean a one-to-many comparison, namely querying whether a person's data or records can be found in the reference database.

6 For the purposes of this report, authentication is used to mean a one-to-one comparison, namely verifying that the data matches that which has been enrolled into the system.

7 "In principle, any human characteristic can be used as a biometric data source provided it meets the following four basic criteria (although others are also sometimes added): universality, uniqueness, permanence, and collectability (objectively measurable in a quantitative way)." Additional desirable criteria for biometric markers include resistance to circumvention and acceptability (meaning that it is acceptable to the community of users for whom it is intended). *See* Michael Fairhurst, *Biometrics: A Very Short Introduction* (OUP, Oxford, 2018), pp. 8 and 10.

8 *See* Keith Breckenridge, *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*, (CUP, Cambridge, 2014), p. 166; Francis Galton, 'Identification Offices in India and Egypt', Nineteenth Century 48, p. 119.

9 *See* Keith Breckenridge, *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*, p. 167.

10 IOL Business Report, 'Scotland Yard Marks 100 Years of Fingerprints', 27 June 2001, available at https://www.iol.co.za/business-report/technology/scotland-yard-marks-100-years-of-fingerprints-68739 (visited 20 February 2020).

11 Gemalto, 'Biometrics: Authentication & Identification (definition, trends, use cases, laws and latest news) - 2020 review', available at https://www.gemalto.com/govt/inspired/biometrics (visited 20 February 2020).

12 Stephen Mayhew, 'History of Biometrics', Biometric Update, available at https://www.biometricupdate.com/201802/history-of-biometrics-2 (visited 20 February 2020).

13 *Ibid*.

14 United State Holocaust Memorial Museum, 'Tattoos and Numbers: The System of Identifying Prisoners at Auschwitz', Holocaust Encyclopedia, available at https://encyclopedia.ushmm.org/content/en/article/tattoos-and-numbers-the-system-of-identifying-prisoners-at-auschwitz (visited 20 February 2020).

15 United State Holocaust Memorial Museum, 'The Nuremberg Race Laws, Holocaust Encyclopedia, available at https://web.archive.org/web/20140519233009/http://www.ushmm.org/outreach/en/article.php?ModuleId=10007695 (visited 20 February 2020).

obligation on citizens to carry identity cards that contained information about the person's ethnicity.[16]

Past months have seen detailed reporting on practices carried out by Chinese authorities in the Xinjiang Uyghur Autonomous Region in the context of the application of China's Counter-Terrorism Law and its Implementing Measures in the Xinjiang Uyghur Autonomous Region.[17] Among a slate of measures presenting serious human rights concerns, reports indicate that authorities have conducted mass collection of biometric data (such as DNA samples, fingerprints, iris scans, and blood types) of residents of the region, under guise of a public health program.[18] Authorities are further alleged to collect relevant data in the context of the passport application process and during police interviews.[19] Moreover, the government has reportedly increased the number of police checkpoints equipped with biometric sensors, iris scanners, and access to nearby CCTV cameras, enabling Chinese security services to monitor the movement and behavior of Xinjiang residents "in unparalleled detail."[20] While the most serious allegations have been made in relation to the Xinjiang region, concerning practices relating to the collection and use of biometric data have been reported throughout China,[21] considered by key commentators among the States with the weakest record when it comes to privacy and data protection standards.[22] Biometric information is, among others, one of the cornerstones of China's controversial social credit system.[23]

While the example of the widespread use of biometrics by the Chinese government is notable, many have voiced apprehension about the misuse of such tools and data in relation to a significant number of governments worldwide.[24]

Aside from the threat of misuse, in particular by oppressive and/ or authoritative governments, concerns have also been raised regarding the collection of biometric data on vulnerable populations and persons in vulnerable situations, in diverse contexts. In the context of their military response to the 9/11 attacks and the so-called "Global War on Terror", more broadly, the United States and some of its allies proceeded to collect biometric data of populations in conflict zones, such as Iraq and Afghanistan.[25] In 2007, human rights organizations flagged that the database compiling information collected in Iraq contained approximately 750,000 records, including fingerprints, photographs and iris scans and cautioned that the database could become a 'hit list' in the wrong hands due to the "particular risk of identification requirements in regions of the world torn by ethnic

16 Human Rights Watch, 'History', available at https://www.hrw.org/reports/1999/rwanda/Geno1-3-09.htm#P196_82927 (visited 20 February 2020); Prevent Genocide International, 'Indangamuntu 1994: Ten Years Ago in Rwanda this Identity Card cost a Woman Her Life', http://www.preventgenocide.org/edu/pastgenocides/rwanda/indangamuntu.htm (visited 20 February 2020).

17 Communication by the Mandates of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; the Working Group on Arbitrary Detention; the Working Group on Enforced or Involuntary Disappearances; the Special Rapporteur on the right to education; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health; the Special Rapporteur on the situation of human rights defenders; the Special Rapporteur on minority issues; the Special Rapporteur on the right to privacy; the Special Rapporteur on freedom of religion or belief; and the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, OL CHN 18/2019, 1 November 2019, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24845 (visited 20 February 2020).

18 *Ibid.*, p. 16; Human Rights Watch, '"Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims', 9 September 2018, available at https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs (visited 20 February 2020).

19 Human Rights Watch, '"Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims', 9 September 2018, available at https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs (visited 20 February 2020).

20 Alina Polyakova and Chris Meserole, 'Policy Brief: Exporting Digital Authoritarianism', Foreign Policy at Brookings, available at https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf (visited 20 February 2020).

21 Human Rights Watch, 'China: Voice Biometric Collection Threatens Privacy', 22 October 2017, available at https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy (visited 20 February 2020); Paul Mozur, 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority', New York Times, 14 April 2019, available at https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (visited 20 February 2020).

22 *See* Paul Bischoff, 'Data privacy laws & government surveillance by country: Which countries best protect their citizens?', Comparitech, 15 October 2019, available at https://www.comparitech.com/blog/vpn-privacy/surveillance-states/ (visited 19 February 2020).

23 Charlie Campbell/ Chengdu, 'How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens', Time, Davos 2019, available at https://time.com/collection/davos-2019/5502592/china-social-credit-score/; https://www.wired.com/story/age-of-social-credit/ (visited 20 February 2020); Zhou Jiaquan, 'Drones, Facial Recognition and a Social Credit System: 10 Ways China Watches Its Citizens', South China Morning Post, 4 August 2018, available at https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china (visited 20 February 2020); Mara Hvistendahl, 'Inside China's Vast New Experiment in Social Ranking', WIRED, 14 December 2017, available at https://www.wired.com/story/age-of-social-credit/ (visited 20 February 2020).

24 *See*, for example, Pete Fussey and Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology', The Human Rights, Big Data and Technology Project, University of Essex Human Rights Centre (July 2019); Nila Bala and Caleb Watney, 'What Are the Proper Limits on Police Use of Facial Recognition?' Brookings TechTank, 20 June 2019, available at https://www.brookings.edu/blog/techtank/2019/06/20/what-are-the-proper-limits-on-police-use-of-facial-recognition/ (visited 20 February 2020); Amitai Ziv, 'This Israeli Face-recognition Startup Is Secretly Tracking Palestinians', Haaretz, 15 July 2019, available at https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359 (visited 20 February 2020); Rina Chandran, 'Mass Surveillance Fears as India Readies Facial Recognition System', Reuters, available at https://www.reuters.com/article/us-india-tech-facialrecognition-trfn/mass-surveillance-fears-as-india-readies-facial-recognition-system-idUSKBN1XH0S9 (visited 20 February 2020); BBC News, 'Russia's Use of Facial Recognition Challenged in Court', 31 January 2020, available at https://www.bbc.com/news/technology-51324841 (visited 20 February 2020).

25 *See* United States Government Accountability Office, 'DOD Biometrics and Forensics. Report to Congressional Committees', GAO-17-580 (August 2017); PM Department of Defense Biometrics, 'Mission', available at https://peoiews.army.mil/programs/pm-dod-bio/ (visited 20 February 2020). In these contexts, the DOD has capabilities to collect, match, store, share, analyze, reference, and manage contextual data and biometrics to include iris, fingerprint, facial images, palm prints, and voice on adversaries as well as known and suspected terrorists.

and religious division."[26] Related concerns seem to persist and have also been echoed by the US House Committee on Oversight and Reform as recently as June 2019 when the Committee raised questions about the military's wide-spread collection of biometric data of "millions of Afghan and Iraqi citizens who have never been accused of any wrongdoing."[27]

The United Nations and its specialized agencies, funds and programmes[28] as well as other humanitarian organizations have similarly grappled, in the context of their protection work, with reconciling efforts aimed at improving the efficiency of assistance delivery with ensuring that data processing methods and practices are protective of the privacy and other human rights of beneficiaries. These organizations have been under considerable pressure to increase efficiency of their services and consequently put in place heightened safeguards protecting against fraud and diversion of aid from legitimate beneficiaries. In this regard, donors have repeatedly pushed for the integration of biometrics in aid delivery.[29] As a result, assistance is at times linked to and conditioned on persons in vulnerable situations providing their biometric data. This raises questions as to the free, informed, and unadulterated nature of consent given by beneficiaries bearing in mind the implications of refusing consent[30] and the responsibility of humanitarian actors who act as data controllers and processors in this context. Moreover, related data collection and processing often happens in partnership with governments,[31] which may, in some circumstances, lead to such collaboration putting refugees, asylum-seekers, and other beneficiaries at risk.[32]

These developments are all the more troublesome considering the tendency on part of some governments to connect migration to the threat of terrorism,[33] despite such connection being "analytically and statistically unfounded."[34]

2. Implications of the use of biometric tools

The use of biometrics is becoming ubiquitous. This development manifests, on the one hand, through the expanded deployment of existing biometric tools, including their use for more diverse purposes and ends. On the other hand, relevant actors seek to develop tools using new measurements and metrics, to be employed for identification and authentication. For example, US defense agencies have recently developed a laser vibrometry tool that allows for identifying persons from a distance based on their "heart print."[35]

It is no wonder that in addition to highlighting positive implications of such tools and ways in which they contribute to societal development and the rule of law, public discourse evidences unease over their short- and long-term implications on individuals and societies. As noted above, biometric tools have traditionally been used by public authorities for military, law enforcement, criminal justice, and border management purposes. They are however increasingly employed in a variety of new ways. As such, they have been linked to the provision of government services and benefits in many jurisdictions. Biometric technology and data have been used to set

26 *See* Electronic Privacy Information Center, 'Iraqi Biometric Identification System', available at https://epic.org/privacy/biometrics/iraq.html (visited 20 February 2020); Electronic Privacy Information Center, Human Rights Watch and Privacy International, Letter to Secretary Robert M. Gates, 27 July 2007, available at https://www.epic.org/privacy/biometrics/epic_iraq_dtbs.pdf (visited 20 February 2020). *See also* Edward Wong, 'To Stay Alive, Iraqis Change Their Names', New York Times, 6 September 2006, available at https://www.nytimes.com/2006/09/06/world/middleeast/06identity.html (visited 20 February 2020).

27 House of Representatives Committee on Oversight and Reform, Letter to Acting Secretary Patrick Shanahan, Department of Defense, Secretary of the Army, Mark Esper, Secretary of the Navy, Richard Spencer, Secretary of the Air Force, Heather Wilson, 19 June 2019.

28 For example, Office of the United Nations High Commissioner for Refugees (UNHCR) uses the Biometrics Identity Management System that records fingerprints and iris scans. It is deployed in at least 52 countries, often in partnership with governments, and holds the biometrics data of at least 6 million refugees and asylum-seekers. The World Food Programme (WFP) has a system called SCOPE, which is a web-based platform acting as repository for beneficiary data, and uses relevant data provided by UNHCR to manage aid and assistance-related entitlements. *See*, for example, Ariel Bogle, 'Biometric Data Is Increasingly Popular in Aid Work, But Critics Say It Puts Refugees at Risk', ABC Science, available at https://www.abc.net.au/news/science/2019-06-21/biometric-data-is-being-collected-from-refugees-asylum-seekers/11209274 (visited 20 February 2020); Claire Walkey, Caitlin Procter and Nora Bardelli, 'Biometric Refugee Registration: Between Benefits, Risks, and Ethics', International Development LSE Blog, available at https://blogs.lse.ac.uk/internationaldevelopment/2019/07/18/biometric-refugee-registration-between-benefits-risks-and-ethics/ (visited 20 February 2020).

29 The Engine Room and Oxfam, *Biometrics in the Humanitarian Sector* (March 2018) available at https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf (visited 20 February 2020); Kristin Bergtora Sandvik, Katja Lindskov Jacobsen, and Sean Martin McDonald, 'Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation', International Review of the Red Cross, 99(904) (2017), pp. 319-344.

30 Dragana Kaurin, Data Protection and Digital Agency for Refugees, World Refugee Council Research Paper no. 12, Center for International Governance Innovation, 15 May 2019, available at https://www.cigionline.org/publications/data-protection-and-digital-agency-refugees (visited 20 February 2020).

31 It has been reported that, in 2009, the US encouraged the Kenyan government, working in partnership with the UN, to conduct biometric registration of all refuges and asylum-seekers near the Somali border and "to cross-check this data with the US' Terrorist Interdiction Program, on the basis that it would help 'catch terrorists posing as refugees'". In recent years it has been reported that the US Department of Health Services retained the biometric data of tens of thousands of asylum-seekers transmitted by UNHCR, including persons that will not come to the US as refugees. *See* Chris Burt, 'DHS to Store Tens of Thousands of Refugee Biometric Records from UNHCR', Biometric Update, 21 August 2019, available at https://www.biometricupdate.com/201908/dhs-to-store-tens-of-thousands-of-refugee-biometric-records-from-unhcr (visited 20 February 2020).

32 Elise Thomas, 'Tagged, Tracked and in Danger: How the Rohingya Got Caught in the UN's Risky Biometric Database', WIRED, 12 March 2018, available at https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh (visited 20 February 2020).

33 Fionnuala Ní Aoláin, 'Calling Out the Misuse of Terrorism Rhetoric Against Refugee and Asylum Seekers', Just Security, 18 November 2019, available at https://www.justsecurity.org/67289/calling-out-the-misuse-of-terrorism-rhetoric-against-refugee-and-asylum-seekers/ (visited 20 February 2020).

34 A/71/384.

35 Heartbeat patterns are distinctive enough to allow for the identification of a person. *See* The Economist, 'People Can Now Be Identified at a Distance by Their Heartbeat', 23 January 2020, available at https://www.economist.com/science-and-technology/2020/01/23/people-can-now-be-identified-at-a-distance-by-their-heartbeat (visited 20 February 2020).

up biometric identification systems, voter registration systems, to enable or facilitate access to social and health services, and, as such, have also been a staple in smart city initiatives.

These initiatives employ ever more sophisticated technologies to collect, process and analyze expanding categories of biometric data (in addition to fingerprints, DNA, and facial analysis, more and more systems work with additional biological and behavioral biometrics, such as gait recognition, voice recognition, etc., while others dabble in predictive biometrics as well).[36] Biometric data is collected in more spaces and contexts, both online and offline. For example, some facial recognition systems rely on cameras in public spaces, making it impossible for individuals to opt out of having their data captured. Moreover, voice recognition databases may use open source information such as audio from social media and other online platforms like YouTube. Keeping in mind that any person owning a smartphone likely uses fingerprint, facial, or voice recognition technology,[37] the options to tap into such data are endless (and, for the most part, inadequately regulated). The ever-growing datasets that governments can access are increasingly stored in central or interconnected/ integrated databases that are at time sought to function as "one-stop-shops,"[38] with access provided to various public authorities, including security sector actors.[39]

The use of biometrics has also rapidly increased in and by the private sector, including in the context of a series of initiatives involving diverse forms of government-business cooperation. Such cooperation is present in many public policy areas, including in relation to preventing and countering terrorism and violent extremism (to be addressed in Section D below).

B. The use of biometrics in the context of preventing and countering terrorism and violent extremism

While the security sector has a long history with the use of biometric systems, the potential of biometrics in the area of preventing and countering terrorism has received increased and sustained attention in the aftermath of the 9/11 attacks.

United Nations Security Council resolution 1373,[40] adopted in the aftermath of 9/11, requires Member States, under Chapter VII of the Charter to:

> *"[p]revent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents."*

While it does not articulate the precise tools that States are expected to use in this regard, border security is one of the areas where the use of biometrics is most common. Biometrics in this context are used for various purposes: to verify a person's identity, and to check whether the person in question figures in law enforcement and counter-terrorism databases, including through connection to relevant INTERPOL databases.[41] The primary biometric here are fingerprints but there is a trend towards using faces as the primary way for identifying travelers.[42]

Some States and international organizations have developed biometric traveler screening systems that they also put at the disposal of other States. For example, the US Personal Identification Secure Comparison and Evaluation System (PISCES) is used in at least 23 countries.[43] The International Organization for Migration (IOM) has developed the Migration Information and Data Analysis System (MIDAS) that ports of entry in at

36 *See* Michael Fairhurst, *Biometrics: A Very Short Introduction* (OUP Oxford, 2018), Chapter 5.
37 For the purposes of this report, a facial recognition system denotes technology able to identify or authenticate individuals through a mapping of their facial features.
38 For example, the Aadhaar database in India. *See* e.g. Michael Safi, 'Indian Court Upholds Legality of World's Largest Biometric Database', The Guardian, 26 September 2018, available at https://www.theguardian.com/world/2018/sep/26/indian-court-upholds-legality-of-worlds-largest-biometric-database (visited 20 February 2020).
39 These actors at times include private companies, in particular private security contractors. *See*, for example, Privacy International, 'Briefing to the UN Counter-Terrorism Executive Directorate on the Responsible Use and Sharing of Biometric Data to Tackle Terrorism' (June 2019).
40 S/RES/1373 (2001), adopted on 28 September 2001.
41 INTERPOL, 'Preventing Terrorist Travel' available at https://www.interpol.int/en/Crimes/Terrorism/Preventing-terrorist-travel (visited 20 February 2020).
42 US Department of Homeland Security, 'Biometric Pathway Transforming Air Travel', EPIC-17-10-17-CBP-FOIA-20180319-Production, available at https://epic.org/foia/dhs/cbp/biometric-entry-exit/Biometric-Pathway.pdf (visited 20 February 2020).
43 US Department of State, *Country Reports on Terrorism 2018*, available at https://www.state.gov/reports/country-reports-on-terrorism-2018/ (visited 20 February 2020).

least 20 countries, mostly in Sub-Sharan Africa,[44] have adopted. While IOM states that it "promotes the responsible use of biometrics, effective personal data protection and respect to privacy" and "[w]hen processing biometric data, IOM ensures that the data is collected in a lawful and fair manner with the consent of beneficiaries, and that the purpose of the processing is specified and legitimate,"[45] none of the publicly available documents providing information on MIDAS, consulted for this report, contain any references to human rights. They also provide no indication that a human rights-based approach is promoted by IOM in relation to MIDAS' use by governments.[46] This lack of an explicit human rights-based approach is of significant concern to the Special Rapporteur's mandate.[47]

Furthermore, many States are also experimenting with expanded use of biometrics at ports of entry. This includes in-motion facial recognition/ gait recognition that identify travelers on-the-go,[48] facial recognition for check-in and other airport services[49] and even predictive biometrics that can provide information on a person's mental or emotional state facilitating authorities to discern – however unreliably – whether the respective person poses a security threat.[50] Such expanded use of biometrics generally includes data-sharing between different actors (frequently between State and non-State actors), which would require a well-defined framework with sufficient safeguards to protect against unlawful or arbitrary use.

Biometric tools, such as identification based on fingerprints or DNA, have long been used for law enforcement and criminal justice purposes. The field of criminal justice has also seen a trend towards the expanded use of biometrics, both through novel uses of existing technology[51] and by adding new tools to the mix, such as facial or voice recognition. It is notable in this context that a number of States and international organizations and fora have launched initiatives exploring issues around data collected, handled, preserved, and shared by military actors in a battlefield context, with a view to facilitate the use of such data as evidence in domestic counter-terrorism criminal trials.[52] Information collected in this context likely contains biometric data, and such data collection, sharing, and use raises a series of particularly challenging questions under human rights law.[53] The Special Rapporteur takes the preliminary view that, in the absence of robust human rights protections which are institutionally embedded to oversee collection, storage, and use of such evidence, relevant practices are likely to infringe international human rights law standards.

Finally, biometric tools and data have been collected, retained and analyzed by diverse intelligence services. While some intelligence services do not have the legal authority to collect biometric data themselves, they do generally have access to such data, based on domestic and cross-border data-sharing arrangements. Albeit a potentially powerful and efficient intelligence tool,

44 Such countries include, among others, Burkina Faso, the DRC, Mali, Niger, Somalia, and South Sudan. International Organization for Migration, 'Migration Information and Data Analysis System/MIDAS. A Comprehensive and Affordable Border Management Information System', available at https://www.iom.int/sites/default/files/our_work/DMM/IBM/updated/midas-brochure18-v7-en_digital-2606.pdf (visited 20 February 2020). *See also* Giacomo Zandonini, 'Biometrics: The New Frontier of EU Migration Policy in Niger', The New Humanitarian, 6 June 2019, available at https://www.thenewhumanitarian.org/news-feature/2019/06/06/biometrics-new-frontier-eu-migration-policy-niger (visited 20 February 2020)

45 International Organization for Migration, 'Biometrics', available at https://www.iom.int/biometrics (visited 20 February 2020).

46 International Organization for Migration, 'Migration Information and Data Analysis System/MIDAS. A Comprehensive and Affordable Border Management Information System'; International Organization for Migration, 'IOM and Data Management, Intelligence and Risk Analysis', available at https://www.iom.int/sites/default/files/our_work/DMM/IBM/updated/07_FACT_SHEET_Data%20management%2C%20intelligence%20and%20risk%20management%202015.pdf (visited 20 February 2020).

47 It bears highlighting in this respect that, in line with the Agreement concerning the Relationship between the United Nations and the International Organization for Migration, IOM undertakes 'to conduct its activities in accordance with the Purposes and Principles of the Charter of the United Nations and with due regard to the policies of the United Nations furthering those Purposes and Principles and to other relevant instruments in the international migration, refugee and human rights fields.' *See* A/70/976, Article 2 (Principles), para. 5.

48 Arie Melamed, '2018 Biometric Predictions: Advanced Biometric Technologies Take Off', Biometric Update, 23 January 2018, available at https://www.biometricupdate.com/201801/2018-biometric-predictions-advanced-biometric-technologies-take-off (visited 20 February 2020).

49 Kelly Yamanauchi, 'As Delta Air Lines Expands Face Recognition, Criticism Grows', Government Technology, 18 September 2019, available at https://www.govtech.com/products/As-Delta-Air-Lines-Expands-Face-Recognition-Criticism-Grows.html (visited 20 February 2020); Allie Funk, 'I Opted Out of Facial Recognition at the Airport—It Wasn't Easy', WIRED, 2 July 2019, available at https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/ (visited 20 February 2020).

50 Jason Davis, 'Biometric Screening at Airports Is Spreading Fast, But Some Fear the Face-Scanning Systems', NBC News, 14 March 2019, available at https://www.nbcnews.com/mach/science/biometric-screening-airports-spreading-fast-some-fear-face-scanning-systems-ncna982756 (visited 20 February 2020); Katherine LaGrave, 'How Airlines and Airports Use Your Data, From Security to the Flight Itself', Condé Nast Traveler, 28 August 2019, available at https://www.cntraveler.com/story/how-airlines-and-airports-use-your-data-from-security-to-the-flight-itself (visited 20 February 2020).

51 For example, the notorious 'Golden State Killer' has been identified with the help of a genealogical database run by a corporate entity. While the forensic evidence thereby generated led to a successful criminal conviction, the case caused such backlash among users and the public that the genealogy site had to change its terms of service regarding the use of its database by law enforcement. *See* Sarah Zhang, 'The Messy Consequences of the Golden State Killer Case', The Atlantic, 1 October 2019, available at https://www.theatlantic.com/science/archive/2019/10/genetic-genealogy-dna-database-criminal-investigations/599005/ (visited 20 February 2020); Megan Molteni, 'The Future of Crime-Fighting Is Family Tree Forensics', WIRED, 26 December 2018, available at https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/ (visited 20 February 2020).

52 *See*, for example, United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED), 'Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences ("Military Evidence Guidelines")', developed within the framework of the Working Group on Criminal Justice, Legal Responses and Countering the Financing of Terrorism of the United Nations Global Counter-Terrorism Coordination Compact, available at https://www.un.org/sc/ctc/wp-content/uploads/2020/01/Battlefield_Evidence_Final.pdf (visited 20 February 2020).

53 It is also acknowledged in relation to the Military Evidence Guidelines developed under the leadership of CTED that these "are merely intended to serve as a basis for discussion and to illustrate the issues that will need to be comprehensively addressed at the national level by those national authorities responsible for determining and enforcing the criteria for the admissibility of evidence in national criminal proceedings." *See* Military Evidence Guidelines, p. 1.

data-sharing arrangements often come with serious rule of law and human rights deficiencies, the implications of which will be addressed in Section C.4 infra.

Despite the broad use of biometric tools and data in a counter-terrorism context post 9/11, having such systems in place has not been a binding requirement under international law until the adoption of United Nations Security Council resolution 2396. The report now turns to outlining the standards set up by the Security Council in this regard, together with relevant United Nations efforts aimed at promoting their full implementation.

1. International standards: United Nations Security Council Resolution 2396

The United Nations Security Council unanimously adopted resolution 2396 in December 2017.[54] The resolution follows a record number of thematic counter-terrorism resolutions adopted in that year and builds on resolution 2178 (2014),[55] with the aim to address the evolving threat posed by so-called "foreign terrorist fighters" as a result of ISIL/ Da'esh having lost control over territory it once held. Territorial loss forced the group to change tactics and move towards a more decentralized approach to its operations and to the assumption by States that significant movement of its members as well as persons associated with the group, such as family members of "foreign terrorist fighters," would follow between and out of conflict zones.[56]

The resolution focuses on three themes identified as priorities: 1) improving border and aviation security;[57] 2) strengthening efforts aimed at the prosecution, rehabilitation, and reintegration of "foreign terrorist fighters"; and 3) improving coordination within the United Nations counter-terrorism architecture in its support to Member States in this context.

As such, the resolution requires States to "develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters."[58] It further imposes an obligation on all UN Member States to establish advance passenger information (API) systems "in order to detect the departure from their territories, or attempted travel to, entry into or transit through their territories, by means of civil aircraft, of foreign terrorist fighters" and other designated individuals, to collect, process and analyze passenger name record (PNR) data, as well as to develop "watch lists or databases of known and suspected terrorists, including foreign terrorist fighters, for use by law enforcement, border security, customs, military, and intelligence agencies to screen travelers and conduct risk assessments and investigations." The resolution encourages States to share such information to be used by all relevant national authorities, "with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offenses and related travel." The Special Rapporteur has set out her concerns with the process and substance of this resolution in her report submitted to the 73rd session of the General Assembly.[59] She reiterates those concerns here and urges that her recommendations be implemented by States and United Nations entities.

While this report focuses on an analysis of questions raised by the use of biometric tools in counter-terrorism, it must be flagged that the multifaceted obligations listed above are interconnected. Both API and PNR are frequently linked with biometric data, with watchlists and other relevant databases also commonly containing biometric information—an aspect that needs to be considered when addressing implications of these obligations separately.

The use of biometric data as a counter-terrorism tool was first referenced in Security Council resolution 2160 (2014),[60] which encouraged Member States to submit photographs and other biometric data to INTERPOL, for the inclusion in the INTERPOL-United Nations

54 S/RES/2396 (2017)

55 *See* A/73/361. *See also*, Martin Scheinin, 'A Comment on Security Council Res 2178 (Foreign Terrorist Fighters) as a "Form" of Global Governance', Just Security, 6 October 2014, available at https://www.justsecurity.org/15989/comment-security-council-res-2178-foreign-fighters-form-global-governance/ (visited 20 February 2020); Fionnuala Ní Aoláin, 'The UN Security Council, Global Watch Lists, Biometrics, and the Threat to the Rule of Law', Just Security, 17 January 2018, available at https://www.justsecurity.org/51075/security-council-global-watch-lists-biometrics/ (visited 20 February 2020)

56 While there is broad agreement among States that the return of such 'foreign terrorist fighters' poses a significant security threat, it bears flagging that the numbers of returnees are considerably lower than predicted. Furthermore, while States have the right and the obligation to take necessary and effective steps towards addressing the concrete threat posed by individual returnees and to ensure that such individuals are also held to account for criminal conduct while abroad, in particular in relation to crimes under international law, such as war crimes or crimes against humanity, any such measures must be based on an individualized assessment. *See*, for example, Fionnuala Ní Aoláin, 'Ensuring a Human Rights-Compliant Approach to the Challenge of Foreign Fighters', Just Security, 7 November 2018, available at https://www.justsecurity.org/61376/ensuring-human-rights-compliant-approach-challenge-foreign-fighters/ (visited 20 February 2020).

57 *See* Statement by the Representative of the United States at the 8116th meeting of the Security Council (8 November 2017), S/PV.8116.

58 S/RES/2396 (2017), para. 15.

59 *See* A/73/361.

60 Resolution 2160 was the first thematic counter-terrorism resolution to explicitly highlight biometrics as a counter-terrorism tool. *See* S/RES/2160 (2014), para. 18.

Security Council Special Notices.[61] This recommendation appeared in a number of subsequent counter-terrorism resolutions of the Council[62] and was expanded to data related to individuals, groups, undertakings, and entities included in the ISIL (Da'esh) and Al-Qaida Sanctions List[63] and the 1988 Sanctions List.[64] Resolution 2322 (2016) broadened the recommendation for biometrics-related data-sharing by calling upon States to share "information about foreign terrorist fighters and other individual terrorists and terrorist organizations, including biometric and biographic information, as well as information that demonstrates the nature of an individual's association with terrorism" via "bilateral, regional and global law enforcement channels," and underscored the importance of providing such information to national watch lists and multilateral screening databases.[65] Resolution 2322 included, for the first time, a recommendation that such data-sharing occur in compliance with both domestic and international law.[66]

This evolution culminated in resolution 2396 imposing a binding obligation to develop biometric capabilities while keeping calls for sharing such data at the level of a non-binding recommendation.[67] This approach is in line with the one taken by the Council when adopting resolution 2178[68] by 1) by turning recommendations contained in previous resolutions into binding obligations under Chapter VII of the UN Charter; and 2) imposing obligations that, prior to the adoption of resolution 2396, have not been established under international law. While regional standards[69] and other non-binding international guidelines[70] existed in relation to API and PNR, no comparable multilaterally negotiated instruments governing biometric data have been developed. Keeping in mind the sensitivity of such data and the far-reaching implications of its use, this is a critical point to flag and will be addressed in more detail below.[71]

The mandate of the Special Rapporteur highlights that:

- Resolution 2396 was adopted following limited and, by all accounts, inadequate engagement with relevant stakeholders,[72] including UN human rights mechanisms and other independent experts, among others civil society with specialist knowledge of international human rights law, humanitarian law, or refugee law.
- The United States, the penholder for counter-terrorism related thematic matters in the Security Council,[73] proposed that the Council adopt a new resolution addressing the evolving threat posed by so-called "foreign terrorist fighters" on 28 November 2017, less than a month before the resolution's date of adoption.[74]
- There are no indications of a human rights or international law impact assessment having been undertaken in this time and no detailed and explicit international law or human rights guidance reflected in the text of the resolution. Similarly, the resolution does not provide for any tools or mechanisms to monitor the human rights implications of the resolution's implementation.
- Resolution 2396 endorses and/ or imposes a series of practices that have already been implemented in US domestic policy,[75] thereby representing a clear example of the United States successfully exporting domestic policies to the international stage.

61 Note that para. 18 of S/RES/2160 encourages Member States to act "in accordance with their national legislation", without explicitly mentioning international law, including international human rights law standards.
62 S/RES/2161 (2104), para. 34; S/RES/2253 (2015) para. 47, Annex I (aa); S/RES/2255 (2015), para. 25, Annex I (x)
63 S/RES/2253 (2015) para. 79.
64 S/RES/2255 (2015), para. 45.
65 S/RES/2322 (2016).
66 In para. 3 of resolution 2322, the Security Council "*Calls upon* States to share, where appropriate, information about foreign terrorist fighters and other individual terrorists and terrorist organizations, including biometric and biographic information, as well as information that demonstrates the nature of an individual's association with terrorism via bilateral, regional and global law enforcement channels, in compliance with international and domestic national law and policy, and stresses the importance of providing such information to national watch lists and multilateral screening databases.
67 When it comes to data-sharing, a number of Security Council and other Member States would not welcome an obligation to share data as that would amount to obligatory intelligence-sharing removing State's discretion to choose the governments they cooperate with in this area. Furthermore, sharing data with governments that have lower rule of law or human rights standards would risk contributing to human rights violations, going against States' obligations under international human rights [and domestic] law.
68 For a more detailed analysis, *see* A/73/361, paras. 24-32.
69 *See*, for example, Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.
70 *See*, for example, International Civil Aviation Organization, Guidelines on Passenger Name Record (PNR) Data (Doc 9944); World Customs Organization/ International Air Transport Association/ International Civil Aviation Organization, Guidelines on Advance Passenger Information (API).
71 *See* Sections C and D.
72 A/73/361.
73 Security Council Report, 'Security Council Penholders', available at https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/working%20methods_penholders-1.pdf (visited 20 February 2020).
74 *See* 8116th meeting of the Security Council (8 November 2017), S/PV.8116. Security Council resolution 2396 was adopted on 21 December 2017.
75 In particular measures related to API/ PNR, biometric data and watchlisting. *See* Statement by the Representative of the United States at the 8148th meeting of the Security Council (21 December 2017), S/PV.8148.

The 2018 Addendum to the 2015 Madrid Guiding Principles

The 2015 Madrid Guiding Principles[76] were developed in follow-up to Security Council resolution 2178 with the purpose of aiding the implementation of the measures aimed at stemming the flow of "foreign terrorist fighters" by Member States. In December 2018, Member States negotiated an Addendum[77] to the Guiding Principles, providing non-binding but authoritative guidance towards the implementation of resolution 2396, particularly focused on addressing the screening, prosecution, rehabilitation, and reintegration of "foreign terrorist fighters" and other persons associated with terrorist groups.

Guiding Principle 3 of the Addendum focuses on the implementation of the obligation "to collect, use and share biometric data in order to responsibly and properly identify terrorists, including FTFs" and highlights the following recommended actions in this respect:

- Develop, use, and maintain biometric systems and data-sharing protocols;
- Compare the biometrics of individuals entering, departing, or seeking residence in their country against other national and international biometric databases, including those of known and suspected "foreign terrorist fighters";
- Employ biometric systems to authenticate/identify individuals and prevent the use of false particulars or attempts to impersonate other people;
- Adopt clear human rights-based frameworks for the use of biometric technology, which include procedural safeguards, effective oversight,[78] and remedy. Importantly, the guiding principle flags that human rights-based frameworks "could be supplemented by a review process that informs all national policy and decision-making regarding the use of biometrics for counter-terrorism purposes";
- Take into consideration specific issues that may arise with respect to protecting and promoting the rights of the child in the context of biometrics and put in place the requisite frameworks and safeguards (including when children's biometric data is collected for child-protection purposes);
- Conduct regular risk assessments to avoid security breaches, data being damaged or compromised;
- Ensure that biometric systems allow for interoperability between other national and international biometric databases, including INTERPOL and maximize the use of INTERPOL's biometric databases.

While the Addendum also expands on what the Security Council meant when requiring that Member States take measures mandated by the resolution in line with international and domestic law, including international human rights law, international humanitarian law, and refugee law, the human rights guidance contained in the Addendum is constrained. The Addendum helpfully flags a number of essential human rights requirements, including the need to set up human rights-compliant frameworks that incorporate procedural safeguards, effective oversight and guarantees the right to remedy in case of violations. At the same time, it does not provide the granular guidance that the human rights implications of the resolution warrant. The mandate of the Special Rapporteur has already expressed concerns that the lack of such detailed guidance on human rights was a hallmark of the regulatory approach of the global counter-terrorism architecture and the Security Council in particular.

76 S/2015/939
77 S/2018/1177.
78 Ensuring effective oversight may include, among others, "establishing, or expanding the remit of existing, appropriate oversight bodies to supervise the implementation of relevant legislation."

2. United Nations capacity-building

A significant component of resolution 2396 is technical assistance and capacity-building, to be led by relevant UN entities, members of the United Nations counter-terrorism architecture.[79] However, as noted by some members of the Security Council, such as Egypt[80] and Uruguay,[81] at the time of adoption, the obligations imposed by the resolution are consequential and onerous. Many Member States may thus find compliance challenging. This has also been highlighted in the 2018 Addendum to the 2015 Madrid Guiding Principles acknowledging that the implementation of the requirements of resolution 2396 "requires legal frameworks, skills, capacity, expertise and equipment that [some Member States] do not currently possess."[82]

States also highlighted that the resolution does not provide Member States with the tools needed for its implementation. This includes failing to provide compulsory support in terms of funding, technical assistance, and capacity-building. In this respect, it is worth emphasizing that while the relevant obligations under the resolution are to be formally implemented in compliance with international human rights law,[83] none of the UN human rights entities are explicitly mentioned as part of mandated United Nations efforts to offer capacity-building and technical assistance.[84] Furthermore, as these human rights entities struggle with lack of human, financial, and other resources, it would be challenging, if not impossible, for them to take up such role at their own initiative.[85]

Capacity-building and technical assistance responses on part of UN entities

In light of the newly imposed obligations and concerns expressed by Member States as to the difficulties their implementation poses, biometrics have also been identified by UN counter-terrorism entities, including the Counter-Terrorism Committee Executive Directorate (CTED), as a priority area for capacity building.

In 2018, in association with the Biometrics Institute,[86] the UN compiled and published a *Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism* (hereinafter "*Compendium*").[87] The intent of the Compendium is to provide "Member States with a high-level overview of biometric technology and operating systems in the context of counter-terrorism."[88] Specifically, it is intended to address "critical issues such as governance, regulation, data protection, privacy, human rights, and risk management and vulnerability assessments" along with recommended practices and case studies.[89]

While the Compendium underscores the need for governments to:

> ***"address the protection of those who are identified by such systems and ensure that the collection, storage and use of biometric data is conducted in accordance with international human rights and privacy laws (…)"***[90]

and includes a number of relevant recommendations, in particular relating to the right to privacy,[91] the mandate of the Special Rapporteur finds that in its current iteration, the Compendium falls short of comprehensively addressing human rights implications and providing

79 S/RES/2396 (2017), paras. 42-50.
80 8148th meeting of the Security Council (21 December 2017), S/PV.8148.
81 *Ibid.*
82 S/2018/1177.
83 Resolution 2396 contains 19 references to international human rights law and relevant obligations, including in relation to the use of biometrics (para. 15).
84 The resolution further highlights the need for compliance with international humanitarian law and refugee law but, similarly to human rights entities, no organizations or agencies specialized in humanitarian or refugee matters are explicitly referenced.
85 There are two UN human rights entities that are members of the UN Global Counter-Terrorism Coordination Compact, the Office of the United Nations High Commissioner for Human Rights (OHCHR) and the mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. The Special Rapporteur is explicitly mandated to oversee the interface between counter-terrorism and human rights (*see* A/HRC/RES/15/15). However, as a part-time, pro bono independent expert, the Special Rapporteur fulfils relevant activities within the Global Counter-Terrorism Coordination Compact without a corresponding budget or adequate staff. As OHCHR is the principal UN entity mandated to promote and protect all human rights for all people, its mission encompasses conducting relevant work at the intersection of human rights and counter-terrorism. However, the Office similarly does not have the resources needed to comprehensively cover developments in the counter-terrorism space.

Other UN human rights mechanisms, such as treaty bodies as well as relevant special procedure mechanisms also address issues related to counter-terrorism and human rights within the scope and confines of their respective mandates. The complementary contributions brought by these bodies are important and should be given due consideration by the counter-terrorism architecture. However, the limitations linked to their particular roles and mandates do not permit these bodies to consistently and systematically contribute to the mainstreaming of human rights in the counter-terrorism architecture.
86 The Biometrics Institute was founded in July 2001 with a mission to "promote the responsible and ethical use of biometrics through thought-leadership and good-practice guidance." *See* https://www.biometricsinstitute.org/. The Institute has developed a series of relevant guidelines, including on privacy and biometrics. As these documents are not publicly available, they have not been reviewed by the mandate of the Special Rapporteur.
87 *United Nations Compendium of Recommend Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism* (2018).
88 *A Summary of the United Nations Compendium of Recommend Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism*, available at https://www.un.org/sc/ctc/wp-content/uploads/2019/03/UNOCT-Biometrics-Summary-Bro_WEB.pdf (visited 20 February 2020).
89 *Ibid.*
90 *United Nations Compendium of Recommend Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism* (2018), page 9.
91 In addition to privacy-specific recommendations, the Compendium also addresses issues related to data protection and due process rights.

granular guidance to Member States in this regard. Such efforts would require a freestanding guiding document with a main focus on human rights concerns and ways in which compliance with resolution 2396 can be implemented in line with the international human rights norms that States have agreed to be bound by. The mandate of the Special Rapporteur is very concerned that in the absence of such comprehensive and free-standing human rights guidance, capacity-building and technical assistance in this area is conducted by UN entities with a significant human rights lacuna.

C. Biometric tools and data: Towards a human rights approach

The human rights impact linked to the use of biometric tools and data is enormous. Related consequences are felt across a range of fundamental rights, including, but not limited to, the rights to life, to liberty and security of person, the right to be free from torture, cruel, inhuman or degrading treatment, the rights to a fair trial, privacy and family life, freedom of expression or movement, etc. It is the scale of impingement, together with the universal, interdependent, and interconnected nature of these rights leading to manifold, interrelated effects across a series of individual and collective freedoms that makes the need for human rights compliant regulation of the use of biometric tools and data an imperative and urgent need.

The mandate of the Special Rapporteur recognizes that the capabilities linked to biometric data and technology turn them into powerful tools in the hands of law enforcement and intelligence agencies, with the potential to further border control and management and to be of great added value in the delivery of criminal justice. As such, these tools also have the potential to substantially contribute to making counter-terrorism efforts more targeted, more precise, and thereby more efficient.

At the same time, as also emphasized in the 2018 Addendum to the 2015 Madrid Guiding Principles[92], "[t]hese technologies present complex legal and policy challenges that are relevant both to States' efforts to counter terrorism and to their human rights obligations." For this reason, "the expansive technical scope and rapid development of this [biometric] technology" is thought to deserve greater attention as it relates to the protection of human rights.[93]

The use of biometrics comes with salient human rights challenges:[94]

- **Some common to many means of information gathering and use;**
- **Others commonly arise in relation to the use of diverse data-driven technologies; and**
- **Again others are either specific to the use of biometric data and related technologies or amplified when biometrics are involved.**

This section will proceed to outline some of the pertinent human rights implications of the use of biometric tools at each vital stage of data usage:

- **Collection;**
- **Retention;**
- **Processing; and**
- **Sharing.**

It will lay out the ramifications of the use of biometric data and technology on the rights to privacy and data protection while also addressing ways in which such ramifications point beyond these rights.

1. The right to privacy

Discussions on the human rights impact of data gathering and use overwhelmingly focus on relevant implications on the right to privacy. Such implications have also been recognized and addressed at the international level, including by United Nations organs. The General Assembly has highlighted that:

> *"the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy."*[95]

92 S/2018/1177.
93 *Ibid.*, para. 15.
94 *See* e.g. 'The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights', A/HRC/39/29, para. 14; Privacy International, 'Biometrics: Friend or Foe of Privacy?' (2017), available at https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf (visited 19 February 2020).
95 A/RES/68/167; A/RES/69/166; A/RES/71/199.

Technological developments, together with the proliferation of and increased reliance on various consumer-facing technologies, have made interferences with the right to privacy both less noticeable to society and the individual subjects affected and, at the same time, more intrusive, with potentially far-reaching consequences that frequently include implications beyond the right to privacy.

The right to privacy is enshrined in international and regional human rights instruments[96] demonstrating a "universal recognition of [its] fundamental importance, and enduring relevance, […] and of the need to ensure that it is safeguarded, in law and in practice."[97] Notwithstanding the arguably universal nature of the right to privacy, about one third of the world's jurisdictions do not have adequate (or any) privacy protections incorporated in law and practice.[98] Even in the case of countries with relevant protections embedded in domestic law, a comparative analysis shows consistent shortcomings in safeguarding the right to privacy in practice, together with a trend towards stepping up data collection and retention, notably in relation to biometric data—a trend that risks "creating surveillance states."[99]

Despite these serious deficiencies, the mandate of the Special Rapporteur stresses that States have an obligation under international human rights law to safeguard the privacy of persons within their jurisdiction. In this sense, the International Covenant on Civil and Political Rights (ICCPR) guarantees a person's right not to be subject to "arbitrary or unlawful interference with his privacy, family, or correspondence."[100] Many States also have relevant obligations under regional human rights systems.[101]

Collection, retention, processing, sharing, and other uses of information relating to a person, particularly when done without the person's valid consent, amount to an interference with that person's right to privacy and thus must meet a set of conditions in order for such measures to be human rights-compliant. In particular, such interference must be implemented pursuant to a domestic legal basis that is sufficiently:

- **Foreseeable;**[102]
- **Accessible,**[103] **and**
- **Provides for adequate safeguards against abuse.**[104]

Restrictions taken must be:

- **Aimed at protecting a legitimate aim;**[105] **and**
- **With due regard for the principles of necessity, proportionality, and non-discrimination.**[106]

In case of infringements on the right to privacy in violation of international human rights standards, States must provide for an effective remedy.[107]

---

96 *See*, for example, Universal Declaration of Human Rights (article 12); International Covenant on Civil and Political Rights (article 17); Convention on the Rights of the Child (article 16); International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (article 14).

97 *See* 'The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights', A/HRC/27/37, para. 13. *See also* 'Report of the Special Rapporteur on the promotion and protection of the right to the freedom of opinion and expression, Frank la Rue', A/HRC/23/40, para. 20.

98 *See*, for example, United Nations Conference on Trade and Development, 'Data Protection and Privacy Legislation Worldwide', available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (visited 19 February 2020).

99 *See* Paul Bischoff, 'Data Privacy Laws & Government Surveillance by Country: Which Countries Best Protect Their Citizens?', Comparitech (15 October 2019), available at https://www.comparitech.com/blog/vpn-privacy/surveillance-states/ (visited 19 February 2020).

100 International Covenant on Civil and Political Rights, article 17.

101 At the regional level the right to privacy is protected by the European Convention on Human Rights (article 8) and the American Convention on Human Rights (article 11), among others

102 This means that the law must be "foreseeable as to its effects, that is, formulated with sufficient precision to enable the individual to regulate his conduct" and that the individual affected by it "must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail." See European Court of Human Rights, *Sunday Times v. The United Kingdom (no. 1)*, Application no. 6538/74, 26 April 1979, § 49. This requirement does not call for absolute foreseeability but rather that the law give individuals an "adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to interfere with their rights." The law must also provide sufficient guidance to those charged with its execution to enable them to ascertain when privacy can be restricted and indicate the scope of any discretion conferred on the competent authorities as well as the manner of its exercise. See, European Court of Human Rights, *Malone v. The United Kingdom*, Application no. 8691/79, 2 August 1984, §§ 66-68.

See also, European Court of Human Rights, *Roman Zakharov v. Russia* [GC], Application no. 47143/06, 4 December 2015, § 230; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, para. 35.

103 Accessibility implies that individuals that are to be affected by the respective legislation must have the possibility to become aware of its content. See European Court of Human Rights, *Groppera Radio AG and Others v. Switzerland*, Application no. 10890/84, Series A no. 173, 28 March 1990, §§ 65-68.

104 European Court of Human Rights, *Kruslin v. France*, Application no. 11801/85, 24 April 1990, §§ 33 and 35; European Court of Human Rights, *Huvig v. France*, Application no. 11105/84, 24 April 1990, §§ 32 and 34.

105 At the same time, relevant restrictions impacting on the right to privacy cannot be justified merely by a general reference to a protected interest, such as national security. *See*, for example, *Roman Zakharov v. Russia* [GC], Application no. 47143/06, 4 December 2015, § 269.

106 See, for example, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/37/52; Human Rights Committee, General Comment no. 34, CCPR/C/GC/34, para. 26; *Hirst v The United Kingdom* (GC), no. 74025/01, ECHR 2005-IX, 6 October 2005, § 62ff; *Georgian Labour Party v. Georgia*, no. 9103/04, 8 July 2008, § 119.

107 International Covenant on Civil and Political Rights, article 2(3), American Convention on Human Rights, article 25, European Convention on Human Rights, article 13.

Independent oversight

The collection and use of biometric data may happen in the context of surveillance operations, including as a component of mass surveillance systems. The mandate of the Special Rapporteur underscores that adequate protection of the right to privacy requires that surveillance measures are subject to robust, independent oversight systems as an effective safeguard against arbitrariness, as also consistently highlighted by UN and regional human rights mechanisms, including in respect of surveillance carried out pursuant to anti-terrorism powers.[108]

108 *See* 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin. Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight', A/HRC/14/46, para. 34. Oversight is best ensured by the judiciary or an independent body with a judicial component and must include the review of relevant evidence "by means of some form of adversarial proceedings." *See*, for example, *Janowiec and Others v. Russia* [GC], Applications nos. 55508/07 and 29520/09, 21 October 2013, §§ 213 and 214; *Roman Zakharov v. Russia* [GC], Application no. 47143/06, 4 December 2015, § 269.

Applying these considerations to biometric data is crucial but in practice frequently insufficient. This is particularly pertinent if one considers that certain aspects of our biometrics, such as a person's face and appearance, their movement, and voice are—unlike our online activity, emails, text messages, and diverse other kinds of information that law enforcement or intelligence services may target—if not inherently public, at least easily accessible. As a result, related data, despite allowing for the identification of the individual, may not enjoy protection, in law or in practice, under privacy frameworks in a number of jurisdictions. Such shortcomings also highlight the importance of comprehensive data protection regimes that extend legal protection to biometric information, even in cases when such information may not be characterized as inherently private.

Recommendation:

- **States must set up and implement comprehensive and efficient legal frameworks aimed at protecting the right to privacy and make sure that the easily accessible nature of some types of biometric data does not lead to insufficient protection under relevant domestic regulations.**

2. The protection of personal and sensitive data

Biometric data, as data relating to the physical, physiological or behavioural characteristics of a person, **must fall within the scope of data protection laws**. The European Union's General Data Protection Regulation (GDPR), heralded as the most comprehensive data protection framework in the world, categorizes biometric data as a "special category of personal data"[109] due to its sensitive character, requiring special protections when such data is collected or processed. Biometric data should be collected and handled in line with recognized data protection principles including:

- **The principles of lawfulness and fairness;**
- **Transparency in collection and processing;**
- **Purpose limitation;**
- **Data minimization;**
- **Accuracy;**
- **Storage limitation;**
- **Security of data; and**
- **Accountability for data handling.**[110]

In practice, however, domestic data protection frameworks frequently do not provide for adequate protection of biometric data, for diverse reasons. To this date, a large number of countries have not passed comprehensive data protection laws.[111] Due to the easy accessibility of certain types of biometric data, such information may not

109 General Data Protection Regulation, Regulation (EU) 2016/679, article 9. *See also*, Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), article 6; Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018 which also qualifies genetic or biometric data as sensitive personal data. India's draft Personal Data Protection Bill similarly defines biometric data as sensitive personal data. *See* PRS Legislative Research, 'The Personal Data Protection Bill, 2019', available at https://prsindia.org/billtrack/personal-data-protection-bill-2019 (visited 19 February 2020).

110 *See*, for example, Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GCPR)/ The Principles', available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (visited 19 February 2020); Data Protection Commission, 'Principles of Data Protection', available at https://www.dataprotection.ie/en/individuals/principles-data-protection (visited 19 February 2020); Renato Leite Monteiro, 'The New Brazilian General Data Protection Law – A Detailed Analysis', International Association of Privacy Professionals, 15 August 2018, available at https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/ (visited 19 February 2020).

111 DLA Piper, Data Protection Laws of the World, available at https://www.dlapiperdataprotection.com (visited 19 February 2020).

explicitly be recognized as sensitive or even personal data under the law. Some jurisdictions, while having established data protection frameworks, do not attach sufficient safeguards and protection to biometric information in this context, at times as a consequence of the gap between technological advances and regulation. There is overwhelming good governance rationale justifying stringent protection afforded to sensitive data in domestic systems. As outlined above, biometric data is linked to an individual's measurable characteristics that make this person unique and identifiable and consequently must be characterized and protected as such in domestic law, if we are to adequately address the risks attached to its collection and use.

Even in the case of countries with robust data protection frameworks, relevant protections and safeguards may not apply or apply in a modified format to information collected by law enforcement and, even more so, if data collection and processing happens in a national security context. The GDPR, flagged above, does not apply to data processed by law enforcement and criminal justice authorities. Such processing is governed by the Directive on the processing of personal data for authorities responsible for preventing, investigating, detecting and prosecuting crimes (the "Police Directive").[112] Furthermore, neither the GDPR or the Police Directive regulate data collection, retention, processing, and sharing to the extent this happens for purposes of national security.[113] The GDPR's approach in this respect seems to reflect the global norm as opposed to being an outlier.

While applying data protection rules in an amended format to national security processes may be warranted, such adjustments must not lead to curtailed safeguards, insufficient transparency or inadequate oversight. Importantly, the principle of purpose limitation must be respected. Purpose limitation requires data to be collected with a specific, defined, and legitimate purpose in mind (purpose specification) and not used for a purpose that is different from or incompatible with the original purpose (compatible use).[114] Furthermore, relevant authorities must pay due regard to data minimization by restricting collection and processing measures to data that is necessary or relevant for accomplishing the legitimate purpose for which data was collected.

Recommendation:

- **States must make sure that biometric data falls within the scope of data protection laws and that relevant protection is not unduly restricted even when such data is collected, retained, processed or shared in a national security context.**

3. There's more to it: the broader human rights implications

Biometric tools have been heralded for their promise to deliver positive outcomes in multiple regulatory contexts. Indeed, such tools can:

- Contribute to combating social exclusion or marginalization;
- Enhance economic, social, and cultural rights, among others, by facilitating access and delivery of services such as food, health care, and other basic social needs;
- Facilitate meaningful and equal participation of all in political and public life, including through the strengthening of election processes, for example via biometric voter registration systems;
- Aid the setting up of identification and registration systems aimed at preventing identity fraud and theft; and,
- Serve as a powerful tool to improve law enforcement efforts and the delivery of criminal justice.

But, biometric tools also come with a number of potential drawbacks that need close attention. As data-driven tools, they are powered by personal data of a sensitive nature and, as any data-driven tools, raise concerns relating to the right to privacy and lawful, fair and safe handling of data. Some salient concerns in this regard have been outlined above.

However, it is crucial to emphasize that questions on how technology and data usage encroach on privacy cannot be meaningfully addressed without relevant analysis and responses duly considering the universal, indivisible, interdependent, and interrelated nature of all human rights.

112 Directive EU 2016/ 680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

113 The EU lacks competence to directly legislate in this area as the Treaty on European Union provides that "national security remains the sole responsibility of each Member State." *See* Consolidated Version of the Treaty on European Union (TEU), article 4(2).

114 *See*, for example, Maximilian von Grafenstein, 'The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation', 1st ed., Nomos Verlagsgesellschaft MbH, 2018.

Both the General Assembly and the Human Rights Council have stressed that the right to privacy serves as one of the foundations of democratic societies and, as such, plays an important role for the realization of the rights to freedom of expression and to hold opinions without interference as well as to the freedoms of peaceful assembly and association.[115] Due to the interconnectedness of a range of human rights, the adverse impacts may, however, point even further and engage a broad spectrum of rights. These include, *inter alia*, the right to equal protection of the law without discrimination, the rights to life, to liberty and security of person, fair trial and due process, the right to freedom of movement, the right to enjoy the highest attainable standard of health, and to have access to work and social security. Such concerns are particularly well-grounded when exploring issues around biometric data and tools driven by such data.

In the context of measures aimed at preventing and countering terrorism and violent extremism, taking effective measures to protect the population against such security threats while at the same time ensuring the protection of human rights may raise practical challenges for States. However, States can effectively meet their obligations under international law by using the flexibilities built into the international human rights law framework. In case of a state of emergency "threatening the life of the nation," States may lawfully derogate from certain human rights obligations, subject to a set of conditions.[116] Moreover, even outside of a state of emergency, States can impose limitations on the exercise of certain rights.[117] Such limitations must be provided by law[118] and necessary to protect a legitimate aim (such as national security, public order, or the rights and freedoms of others).[119] Any measures must also be governed by the principles of necessity and proportionality and must respect the need for consistency with other guaranteed human rights.

115 A/RES/71/199; A/RES/73/179; A/HRC/RES/34/7.

116 While a detailed analysis of derogations under human rights law goes beyond the scope of this paper, article 4 of the ICCPR provides for the possibility for States to temporarily adjust certain obligations under the treaty in time of "public emergency which threatens the life of the nation," provided a number of conditions are met, including that such measures be limited to the extent strictly required by the exigencies of the situation. This obligation reflects the principle of proportionality which is common to derogation and limitation powers. Any measures thus taken need to be in genuine response to the situation, aimed at the restoration of a constitutional order respectful of human rights and be fully justified by the circumstances. For a detailed analysis on States' use of emergency powers post-9/11, *see* A/HRC/37/52.

117 Some human rights are absolute. Such rights include the prohibitions of torture and cruel, inhuman or degrading treatment or punishment, of slavery and servitude, as well as the principle of legality. The absolute character of these rights means that it is not permitted to restrict them by balancing their enjoyment against the pursuit of a legitimate aim or against any other consideration, including in case of armed conflict, or any case of public emergency. Other rights, though some of them derogable in a state of emergency, may not be limited. These include freedom of thought, conscience and religion, as well as freedom of opinion. It has to be noted in this respect however that the right to manifest one's religion or beliefs as well as the right to freedom of expression are not absolute and may be limited in line with relevant conditions imposed by human rights law. For a more detailed analysis, *see* A/HRC/37/52.

118 Such law must comply with the requirements foreseeability and accessibility and must contain sufficient safeguards to protect against arbitrary implementation. *See also* relevant analysis in Section C.1.

119 It should be noted in this respect that legitimate aims must be interpreted narrowly. For example, the creation of a biometric tool or system cannot be invoked as a legitimate aim in itself. In this sense, *see also* Privacy International, 'Briefing to the UN Counter-Terrorism Executive Directorate on the Responsible Use and Sharing of Biometric Data to Tackle Terrorism' (June 2019), p. 7.

COVID-19 and biometrics

Countries worldwide are currently grappling with the COVID-19 pandemic.[120] In response to the health and economic crisis caused by the pandemic, the number of countries having taken measures involving restrictions on a series of human rights,[121] or having declared a state of emergency[122] is on a continuous rise.

These measures include restrictions on movement such as shelter in place orders, curfews, travel restrictions, and diverse means of tracking the movement and whereabouts of the general population or of individuals diagnosed with or suspected of COVID-19 to monitor their compliance with relevant restrictions. Diverse iterations of surveillance measures have been implemented in a variety of countries,[123] with some jurisdictions adding biometric tools to the mix. Countries and territories using facial recognition to monitor public spaces and enforce quarantine include China,[124] Malaysia[125], Russia,[126] and Transnistria.[127] The broadest application of such tools has so far been reported in China where cameras equipped with facial recognition software have been employed to assist the authorities.[128] Several Chinese companies have reportedly developed software that can identify individuals wearing masks with a high level of accuracy.[129] In addition to facial recognition, body temperatures of individuals using public transit are also recorded.[130] Many other countries contemplate the use of facial recognition and diverse forms of bio-surveillance, such as temperature sensors.[131] Poland has released an application to be used by those in quarantine that requires individuals to periodically send geotagged selfies as a means of monitoring compliance.[132] Many jurisdictions, aided by business enterprises,[133] deploy or

120 *See* WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020, available at https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 (visited 15 April 2020).

121 Such measures are based on newly adopted laws and policies or on "repurposed" existing legislation. *See*, for example, ICNL, ECNL and the Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'COVID-19 Civic Freedom Tracker', available at https://www.icnl.org/covid19tracker/ (visited 15 April 2020); University of Oxford Blavatnik School of Government, 'COVID-19 Government Response Tracker', available at https://www.bsg.ox.ac.uk/research/research-projects/coronavirus-government-response-tracker (visited 15 April 2020); Privacy International, 'Tracking the Global Response to COVID-19', available at https://privacyinternational.org/examples/tracking-global-response-covid-19 (visited 15 April 2020).

122 *Ibid*.

123 *See*, for example, Yuval Noah Harari, 'The World After Coronavirus', Financial Times, 20 March 2020, available at https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (visited 15 April 2020); Jeremy Cliffe, 'The Rise of the Bio-Surveillance State', New Statesman, 25 March 2020, available at https://www.newstatesman.com/science-tech/2020/03/rise-bio-surveillance-state (visited 15 April 2020); Allie Funk, 'How to Protect Both Public Health and Privacy', Freedom House, 6 April 2020, available at https://freedomhouse.org/article/how-protect-both-public-health-and-privacy (visited 15 April 2020); Isobel Asher Hamilton, 'Compulsory Selfies and Contact-Tracing: Authorities Everywhere Are Using Smartphones to Track the Coronavirus, And It's Part of a Massive Increase in Global Surveillance', Business Insider, 14 April 2020, available at https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3 (visited 15 April 2020).

124 Yuval Noah Harari, 'The World After Coronavirus', Financial Times, 20 March 2020, available at https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 (visited 15 April 2020).

125 Chris Burt, 'Biometric Checks and Facial Recognition Payments to Support Social Distancing, Fight Spread of Covid-19', Biometric Update, 23 March 2020, available at https://www.biometricupdate.com/202003/biometric-checks-and-facial-recognition-payments-to-support-social-distancing-fight-spread-of-covid-19 (visited 15 April 2020).

126 Evan Gershkovich, 'How Russia Is Responding to the Coronavirus: Cameras, Deportations and Skepticism', The Moscow Times, 13 March 2020, available at https://www.themoscowtimes.com/2020/03/13/how-russia-is-responding-to-the-coronavirus-cameras-deportations-and-skepticism-a69616 (visited 15 April 2020); Reuters, 'Moscow Deploys Facial Recognition Technology for Coronavirus Quarantine', 21 February 2020, available at https://www.reuters.com/article/us-china-health-moscow-technology/moscow-deploys-facial-recognition-technology-for-coronavirus-quarantine-idUSKBN20F1RZ (visited 15 April 2020).

127 Privacy International, 'Moldova: Transnistria Uses Facial Recognition to Identify Quarantine Violators', 28 March 2020, available at https://privacyinternational.org/examples/3629/moldova-transnistria-uses-facial-recognition-identify-quarantine-violators (visited 15 April 2020).

128 Cynthia Brumfield, 'New Coronavirus-Era Surveillance and Biometric Systems Pose Logistical, Privacy Problems', CSO, 3 April 2020, available at https://www.csoonline.com/article/3535194/new-coronavirus-era-surveillance-and-biometric-systems-pose-logistical-privacy-problems.html (visited 15 April 2020); Takashi Kawakami, 'Coronavirus Gives China More Reason to Employ Biometric Tech', Nikkei Asian Review, 30 March 2020, available at https://asia.nikkei.com/Business/China-tech/Coronavirus-gives-China-more-reason-to-employ-biometric-tech (visited 15 April 2020).

129 Martin Pollard, 'China Firm Develops System to Recognize Faces Behind Coronavirus Masks', Reuters, 9 March 2020, available at https://www.reuters.com/article/health-coronavirus-facial-recognition/china-firm-develops-system-to-recognise-faces-behind-coronavirus-masks-idUSL8N2B20QP (visited 15 April 2020); Lindsey O'Donnell, 'Covid-19 Spurs Facial Recognition Tracking, Privacy Fears', Threat Post, 20 March 2020, available at https://threatpost.com/covid-19-spurs-facial-recognition-tracking-privacy-fears/153953 (visited 15 April 2020); Tom Simonite, 'How Well Can Algorithms Recognize Your Masked Face?', WIRED, 1 May 2020, available at https://www.wired.com/story/algorithms-recognize-masked-face/ (visited 1 May 2020).

130 Cynthia Brumfield, 'New Coronavirus-Era Surveillance and Biometric Systems Pose Logistical, Privacy Problems', CSO, 3 April 2020, available at https://www.csoonline.com/article/3535194/new-coronavirus-era-surveillance-and-biometric-systems-pose-logistical-privacy-problems.html (visited 15 April 2020).

131 *Ibid*.; Dave Gershgorn, 'Facial Recognition Companies See the Coronavirus as a Business Opportunity', Medium OneZero, 19 March 2020, available at https://onezero.medium.com/facial-recognition-companies-see-the-coronavirus-as-a-business-opportunity-6c9b99d60649 (visited 15 April 2020); Lindsey O'Donnell, 'Covid-19 Spurs Facial Recognition Tracking, Privacy Fears', Threat Post, 20 March 2020, available at https://threatpost.com/covid-19-spurs-facial-recognition-tracking-privacy-fears/153953 (visited 15 April 2020); Joseph Cox, 'Surveillance Company Says It's Deploying "Coronavirus-Detecting" Cameras in US', VICE, 17 March 2020, available at https://www.vice.com/en_us/article/epg8xe/surveillance-company-deploying-coronavirus-detecting-cameras (visited 15 April 2020).

132 Isobel Asher Hamilton, 'Compulsory Selfies and Contact-Tracing: Authorities Everywhere Are Using Smartphones to Track the Coronavirus, And It's Part of a Massive Increase in Global Surveillance', Business Insider, 14 April 2020, available at https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3 (visited 15 April 2020).

133 Joel Schectman, Christopher Bing, Jack Stubbs, 'Special Report: Cyber-Intel Firms Pitch Governments on Spy Tools to Trace Coronavirus', Reuters, 28 April 2020, available at https://www.reuters.com/article/us-health-coronavirus-spy-specialreport/special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-coronavirus-idUSKCN22A2G1 (visited 28 April 2020); Leo Kelion, 'Coronavirus: Apple and Google Team Up to Contact Trace Covid-19', BBC News, 10 April 2020, available at https://www.bbc.com/news/technology-52246319 (visited 15 April 2020); Natasha Lomas, 'An EU coalition of techies is backing a 'privacy-preserving' standard for COVID-19 contacts tracing', Tech Crunch, 1 April 2020, available at https://techcrunch-com.cdn.ampproject.org/c/s/techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/amp/ (visited 15 April 2020).

plan on deploying tracing technology to facilitate the easing of pandemic-related restrictions without triggering a second wave of infections.[134] The emergency nature of the situation may result in relevant tools being developed without a proper human rights risk assessment and deployed prematurely.

At the same time, the use of certain biometric tools such as fingerprint scanners has been scaled back due to the health safety risks that they pose. Numerous governments and organizations decided to, at least temporarily, replace such tools with other, preferably contactless, options (such as facial recognition or QR codes) or more low-tech means of identification and authentication.[135]

Action taken to address the challenges posed by COVID-19 does not belong in the realm of national security or counter-terrorism. However, various government representatives have used war rhetoric in their COVID-19-related public communication[136] and certain countries chose to resort to tools hitherto employed in a counter-terrorism context.[137] At the same time, surveillance-related measures taken to tackle the COVID-19 pandemic may similarly be expanded for use in other sectors or continued beyond the end of the pandemic.[138]

The mandate of the Special Rapporteur notes that the above outlined measures interfere with a series of human rights, including but not limited to, the rights to freedom of movement and assembly, freedom of religion and belief and the right to private and family life. As such, States must ensure that limitations to these rights are provided by law, are necessary, proportionate and non-discriminatory.[139] Measures taken need to be assessed against States' obligation to take necessary and feasible measures to protect their population from the threat posed by the COVID-19 pandemic and must provide for necessary and efficient means for tackling the threat. States should only resort to derogations to the extent public health and other legitimate public policy objectives cannot be met through restrictions on certain limitable rights.[140] The mandate of the Special Rapporteur stresses that the scope of relevant measures must be limited in time and warns of the risks associated with wide-ranging surveillance becoming a staple of post-COVID-19 societies.[141]

---

134 *See*, for example, Susan Landau, 'Location Surveillance to Counter COVID-19: Efficacy Is What Matters', Lawfare, 25 March 2020, available at https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters (visited 15 April 2020); BBC News, 'Coronavirus Privacy: Are South Korea's Alerts Too Revealing?' 5 March 2020, available at https://www.bbc.com/news/world-asia-51733145 (visited 15 April 2020).

135 For example, the World Food Programme has been using QR codes instead of fingerprints to authenticate beneficiaries. *See* https://twitter.com/WFPInnovation/status/1250336530561789952 (visited 15 April 2020).

136 *See*, for example, Adam Westbrook, 'Beware of Politicians Who Declare "War" on the Coronavirus', The New York Times, 20 April 2020, available at https://www.nytimes.com/2020/04/20/opinion/coronavirus-war-politicians.html (visited 20 April 2020); Jacob Hagstrom, 'Stop Calling Covid-19 a War', The Washington Post, 20 April 2020, available at https://www.washingtonpost.com/outlook/2020/04/20/stop-calling-covid-19-war/ (visited 20 April 2020).

137 Amir Cahane, 'The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers', Lawfare, 21 March 2020, available at https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers (visited 15 April 2020); Haaretz, 'An Epidemic of Surveillance', 18 March 2020, available at https://www.haaretz.com/opinion/editorial/an-epidemic-of-surveillance-1.8685396 (visited 15 April 2020).

138 *See* 'Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights', 2 April 2020, available at https://www.accessnow.org/cms/assets/uploads/2020/04/Joint-statement-COVID-19-and-surveillance-FINAL1.pdf (visited 15 April 2020).

139 For more information on the human rights dimension of COVID-19 and measures aimed at addressing the pandemic, see, for example, Office of the High Commissioner for Human Rights, 'COVID-19 and its human rights dimensions', available at https://www.ohchr.org/EN/NewsEvents/Pages/COVID-19.aspx (visited 15 April 2020); Special Procedures of the Human Rights Council, 'COVID-19 and Special Procedures', available at https://www.ohchr.org/EN/HRBodies/SP/Pages/COVID-19-and-Special-Procedures.aspx (visited 15 April 2020).

140 *See* Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/37/52; Human Rights Committee, 'Statement on derogations from the Covenant in connection with the COVID-19 pandemic', 24 April 2020, CCPR/C/128/2, available at https://www.ohchr.org/Documents/HRBodies/CCPR/COVIDstatementEN.pdf (visited 26 April 2020). *See also* the statement by UN Special Procedures mandate holders on 'COVID-19: States should not abuse emergency measures to suppress human rights', 16 March 2020, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E (visited 15 April 2020).

141 *See*, for example, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/37/52; Adam Klein and Edward Felten, 'The 9/11 Playbook for Protecting Privacy', Politico, 4 April 2020, available at https://www.politico.com/news/agenda/2020/04/04/9-11-playbook-coronavirus-privacy-164510 (visited 15 April 2020); Andrew Roth, Stephanie Kirchgaessner, Daniel Boffey, Oliver Holmes and Helen Davidson, 'Growth in surveillance may be hard to scale back after pandemic, experts say', The Guardian, 14 April 2020, available at https://www.theguardian.com/world/2020/apr/14/growth-in-surveillance-may-be-hard-to-scale-back-after-coronavirus-pandemic-experts-say (visited 15 April 2020).

Biometrics and the scope of human rights obligations: the question of jurisdiction

Several human rights treaties specify that the obligations contained therein extend to individuals that are, at any given moment, within the jurisdiction of a State Party.[142] The exercise of jurisdiction under human rights treaties is primarily territorial, meaning that everyone on the territory of a State is *ipso facto* under the respective State's jurisdiction and that jurisdiction is presumed to be exercised throughout the State's national territory.[143] However, under certain circumstances, States may also exercise jurisdiction extraterritorially[144] and have certain human rights obligations towards individuals that are under their effective control or otherwise within their power or authority. A somewhat simplified snapshot of relevant jurisprudence produced by international and regional courts and human rights mechanisms will distinguish two modalities of extraterritorial application of human rights instruments: extraterritorial jurisdiction based on a spatial model (i.e. control over territory) and extraterritorial jurisdiction based on a personal model (i.e. control over an individual). Traditionally, both approaches translate to the exercise of physical control in practice, at least to the extent that such extraterritorial jurisdiction is exercised with respect to non-citizens.[145]

However, as access to and use of information and communication technologies (ICTs) has become essential to the conduct of government operations, to business, and to individuals' day-to-day lives, exercise of power and authority in this context has increasingly been disjointed from the exercise of physical control. Data collection, processing, and sharing practices (including, but not limited to, trans-border data-sharing) result in States handling the personal and sensitive data of individuals that are not, and may have never been, under the respective State's jurisdiction if one is to employ a traditional conceptualization of extraterritorial jurisdiction revolving around the exercise of physical control. Relevant conduct is rarely effectuated outside of the State's territory but may come with far-reaching extraterritorial effects and results in the exercise of power or authority over at least certain implicated human rights of affected individuals. Promoting worldwide respect for universally guaranteed human rights requires a shift—albeit prudent and pondered—towards an "interference-based" approach to jurisdiction[146] and derived responsibilities. Such approach already has support in international and regional jurisprudence and expert opinion[147] and is expected to be further and authoritatively developed as relevant mechanisms are increasingly called to decide on questions reflecting the human rights challenges of the digital age.

---

142 It has to be noted in this respect that the notion of jurisdiction under human rights treaties has a particular meaning attached to it. As opposed to simply referring to the State's right under international law to exercise its powers and regulate conduct, it serves as a threshold criterion determining whether the State had an obligation to secure the rights guaranteed in the respective treaty.

143 *See*, e.g. *Ilaşcu and Others v. Moldova and Russia* [GC], Application no. 48787/99, 8 July 2004, § 312; *Al-Skeini and Others v. the United Kingdom* [GC], Application no. 55721/07, 7 July 2011, § 131. At the same time, State jurisdiction on its own territory can be restricted in certain matters, most notably due to immunities (in particular, diplomatic immunities – *see*, for example Article 22(1), Vienna Convention on Diplomatic Relations).

144 *See*, for example, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, ICJ Reports 2004, paras. 109-113; *Case Concerning Armed Activities on the Territory of the Congo, (Democratic Republic of the Congo v. Uganda)*, Judgment, 19 December 2005, ICJ Reports 2005, para. 179; *Case Concerning the Application of the Convention on the Elimination of All Forms of Racial Discrimination (Georgia v. the Russian Federation) Request for the Indication of Provisional Measures*, Order of 15 October 2008, para. 109; Human Rights Committee, General Comment 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant (2004), CCPR/C/21/Rev.1/Add.13, para. 10.

145 With respect to citizens, States may exercise power or authority over certain aspects of their human rights even when such persons are outside of the State's territory: for example the State may restrict their freedom of movement by revoking or refusing to issue travel documents (*see*, e.g., Human Rights Committee, *Samuel Lichtensztejn v. Uruguay*, Communication no. 77/1980, CCPR/C/OP/2 (1990), para. 1.2.). Arguably, interreferences with citizens' human rights, such as the right to privacy, including in the context of the use of biometric tools, that are not permissible when the person is within the territory of their State of citizenship would not be justifiable under international human rights law in case such persons find themselves outside of the State's territory.

146 *See*, for example, Carly Nyst, 'Interference-Based Jurisdiction over Violations of the Rights to Privacy', EJIL:Talk!, 21 November 2013, available at https://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/ (visited 19 February 2020); Beth Van Schaack, 'The Extraterritorial Right to Privacy: An Opportunity to Impact the Debate', Just Security, 27 March 2014, available at https://www.justsecurity.org/8654/extraterritorial-privacy-opportunity-impact-debate/ (visited 19 February 2020).

147 *See*, for example, Human Rights Committee, *Ibrahima Gueye et al. v. France*, Communication no. 196/1985, CCPR/C/35/D/196/1985; Committee on the Rights of the Child, Concluding observations on the second periodic report of the Holy See, 31 January 2014, CRC/C/VAT/CO/2; European Court of Human Rights, *Sejdovic v. Italy* [GC], Application no. 56581/00, 1 March 2006; *African Commission on Human and Peoples' Rights, Association Pour la Sauvegarde de la Paix au Burundi v. Tanzania, Kenya, Uganda, Rwanda, Zaire and Zambia*, Communication no. 157/96 (2003); United States Department of State, Office of the Legal Adviser, 'Memorandum Opinion on the Geographic Scope of the Covenant on Civil and Political Rights', 19 October 2010, available at https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf (visited 19 February 2020); Anne Peters, 'Surveillance without Borders: The Unlawfulness of the NSA Panopticon, Part II', EJIL:Talk!, 4 November 2013, available at https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/#more-9785 (visited 19 February 2020); Ryan Goodman, 'Forum on the Extraterritorial Application of Human Rights Treaties: Analyzing the State Department Memos', Just Security, 7 March 2014, available at https://www.justsecurity.org/7946/forum-extraterritorial-application-human-rights-treaties-analyzing-state-department-memos/ (visited 19 February 2020).

It must further be noted in this respect that in the cases relating to foreign and extraterritorial surveillance decided by the European Court of Human Rights, respondent States did not challenge the case on grounds of the State not having exercised jurisdiction.

The mandate of the Special Rapporteur highlights that relevant human rights implications are likely to be amplified in case of groups and persons who are already marginalized or discriminated against, such as women, members of ethnic, religious, racial, sexual, and other minorities as well as groups and persons in vulnerable situations, such as refugees and asylum-seekers or persons affected by armed conflict and other types of violence.

Among such categories, States and other stakeholders handling biometric data must pay particular attention to means and modalities for collecting, retaining, processing and sharing **children**'s data.[148] The mandate of the Special Rapporteur is unequivocal that such data use must always comply with the safeguards contained in the Convention on the Rights of the Child[149] and, in particular, with the requirement that any relevant measures be "in the best interest of the child."[150] This means that considerations related to the best interest of the child must inform the assessment as to whether the measure in question is necessary and proportionate. Relevant examinations must also address the appropriateness of using biometric markers that may be less stable in case of children (as they may undergo alteration as a result of the growing or aging process).

Finally, States bear an obligation to protect children against "all forms of discrimination or punishment on the basis of the status, activities, expressed opinions, or beliefs of the child's parents, legal guardians, or family members,"[151] a consideration of utmost importance when addressing children associated with terrorist groups, including family members of known or suspected "foreign terrorist fighters."

The use of biometric data may be uniquely helpful and serve the interest of the child in a number of instances. This includes cases when such data is employed to prove the child's parentage and reunite them with their family or with the aim of using such parentage information to ascertain the child's nationality in view of their repatriation. At the same time, concerns related to data usage and, in particular, long-term retention of biometric data of minors based on the child's family affiliation must be flagged. Data collection and retention, when it is for monitoring or surveillance purposes, must be based, among others, on a threat assessment, and the necessity for the data to be retained and for children to be included in databases or watchlists must be periodically reviewed. Relevant measures must also be subject to independent oversight. Such oversight should include review by a public authority specifically tasked with protecting the rights of the child (such as an ombudsperson) or ensure that experts duly specialized in children's rights are part of the oversight body's composition.

Recommendations:

- **States must carry out comprehensive *a priori* and *a posteriori* assessments of the human rights impact of biometric tools and data in the counter-terrorism context. Such assessments must consider impact on the whole spectrum of human rights. Suitable vehicles for relevant assessments include independent reviewers of terrorism-related legislation and policy, national human rights institutions, or other specialist government entities.**
- **The collection and processing of biometric data concerning children must be in the best interest of the child and, as such, limited, exceptional, and subject to strict review.**

4. Stages of the data lifecycle: a non-exhaustive inventory of human rights implications

a. Collection and retention of biometric data

Data collection, retention, processing, and sharing engage a range of human rights, including but not limited to, the right to privacy and data protection.

In order to ensure human rights compliant use of biometric data and relevant tools, the human rights compliance of measures must be assessed at every stage of data usage. While a human rights assessment is

148 The Convention on the Rights of the Child defines children as "every human being below the age of eighteen years." *See* Convention on the Rights of the Child, article 1.

149 The Convention on the Rights of the Child has 196 State Parties and as such is almost universally ratified (the only UN Member State that has signed but not ratified the Convention is the United States).

150 Convention on the Rights of the Child, article 3(1). The Convention requires States to ensure that in all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration. The Committee on the Rights of the Child stated that the child's best interests was a threefold concept, namely a substantive right; a fundamental, interpretative legal principle; and a rule of procedure. Any determination of what is in the best interest of a child "requires a clear and comprehensive assessment of the child's identity, including his or her nationality, upbringing, ethnic, cultural and linguistic background, particular vulnerabilities and protection needs." Relevant assessment processes must be carried out "in a friendly and safe atmosphere by qualified professionals who are trained in age and gender-sensitive interviewing techniques." *See*, for example, Committee on the Rights of the Child, General Comment no 14 on the right of the child to have his or her best interests taken as a primary consideration (2013), CRC/C/GC/14; and General Comment no. 6: Treatment of unaccompanied and separated children outside their country of origin (2005), CRC/GC/2005/6.

151 Convention on the Rights of the Child, articles 2 and 3.

commonly conducted at the data collection stage—at least with respect to the right to privacy—relevant evaluations are frequently omitted or carried out in an incomplete manner at subsequent stages. However, data having been collected in a human rights-compliant manner does not mean that the requirements imposed by human rights law are satisfied with respect to retention,[152] processing, and sharing of that data.

The data lifecycle

The ever-increasing length of the data lifecycle brought by the new and transformed means and modalities of usage makes addressing these concerns all the more critical. A violation at one stage of the data chain or in the data lifecycle will impact the lawfulness and human rights compliance of data usage at subsequent stages and may lead to a continuous violation unless the deficiency is duly remedied. For example, unlawfully collected data may not be lawfully retained, processed or shared. In case a violation occurs at the processing stage by aggregating datasets, some of which were unlawfully collected, obtained or retained, this deficiency will affect the legality of the resulting datasets and their subsequent use.

Lengthy or indefinite retention of diverse sets of personal data figures among the most pertinent and concerning current trends in this field. Both governments and companies seek to collect and store large troves of data, a trend aided by declining costs of data storage. With the advent of "datafication," the potential current and future uses of such information are practically endless.[153]

International human rights law does not allow for the indiscriminate retention of personal data, including biometric data, as such indiscriminate retention cannot satisfy the criteria of necessity and proportionality.[154] In this respect, the European Court of Human Rights has repeatedly held that blanket and indiscriminate retention of biometric data, such as fingerprints and DNA samples, were in breach of the right to privacy.[155] Importantly, the Court also ruled that indefinite retention of genetic data of persons convicted of criminal offences, including after the data subject's death, interfered with the right to privacy of individuals biologically related to the data subject[156] and stressed that there was a "narrowed margin of appreciation available to States when setting retention limits for the biometric data of convicted persons."[157]

Decisions to retain biometric data must also consider issues related to data security and the risk of biometric data being compromised. Certain storage modalities, such as the creation of central databases, pose a higher risk than localized storage of such data.[158] In this respect, due consideration must be given to the potential severe and at times irreversible consequences resulting from biometric data being misused or compromised. Furthermore, in addition to the risks related to security, prolonged retention periods also heighten the risk of

152 Retention of biometric data in line with international human rights law requires that such retention be provided by law and be necessary and proportionate. This also means that as soon as these conditions are not fulfilled, retention must be terminated through the safe and responsible disposal of the data. For the purposes of this report, such safe and responsible disposal is understood to be part of the obligations related to the human rights-compliant retention of biometric data.

153 Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data. The Revolution That Will Transform How We Live, Work and Think* (Mariner Books, Boston-New York, 2013), p. 15.

154 In the case of *S. and Marper v. The United Kingdom*, the European Court of Human Rights found that 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 competing public and private interests. European Court of Human Rights, *S. and Marper v. The United Kingdom* [GC], Applications nos. 30562/04 and 30566/04, 4 December 2008.
It must be noted that long retention periods are commonplace in many jurisdictions, including frequently outside of the scope of criminal justice processes. In this respect it is notable for example that the United States and Five Eyes countries retain photos and fingerprints of travelers for a period of up to 75 years. See US Department of Homeland Security, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), DHS/NPPD/PIA-002 (2012); US Department of Homeland Security, Privacy Impact Assessment for the Traveler Verification Service, DHS/CBP/PIA-056 (2018).

155 European Court of Human Rights, *S. and Marper v. The United Kingdom* [GC], Applications nos. 30562/04 and 30566/04; European Court of Human Rights, *M. K. v. France*, Application no. 19522/09, 18 April 2013; European Court of Human Rights, *Gaughran v. The United Kingdom*, Application no. 45245/15, 13 February 2020.

156 European Court of Human Rights, *Gaughran v. The United Kingdom*, Application no. 45245/15, §§ 81-82.

157 European Court of Human Rights, *Gaughran v.Tthe United Kingdom*, Application no. 45245/15, §§ 84 and 88.

158 For example, storing biometric data in the chip of the biometric identity document.
In relation to the option to store biometric data in a central national database, the European Union Fundamental Rights Agency noted that "due to [the] scale and the sensitive nature of the data which would be stored, the consequences of any data breach could seriously harm a potentially very large number of individuals. If such information ever falls into the wrong hands, the database could become a dangerous tool against fundamental rights." *See*, European Union Agency for Fundamental Rights, Fundamental rights implications of storing biometric data in identity documents and residence cards (2018), p. 14.

"mission creep" and may lead to use beyond the purpose for which the data was collected.[159]

Recommendations:

- **The human rights compliance of measures involving biometric data must be duly assessed at every stage of data usage.**
- **Data must be safely and appropriately discarded as soon its retention does not meet the requirements of lawfulness, necessity or proportionality. Indefinite retention of data is inconsistent with States' human rights obligations.**

b. Processing of biometric data: the human rights implications of automation, machine learning and artificial intelligence

In addition to its use for identification and authentication purposes, so-called primary biometric data also allows for deducing ancillary attributes, such as gender, age, ethnicity, appearance (hair or eye color, height, weight). Such data may provide complementary information for identification or authentication. These are called 'soft' or 'light' biometrics and refer to a set of physical or behavioral characteristics that may aid in recognizing individuals, but that are not sufficient for distinguishing between individuals, as they lack the necessary level of distinctiveness and/ or permanence.[160] For example, voice or iris recognition tools also provide information on the gender, age and race/ ethnicity of a person—all sensitive information that qualify as "protected grounds" on which discrimination is prohibited. The use of soft biometrics is associated with a risk of discriminatory use of such information through its potential to facilitate profiling based on protected grounds.[161]

In addition, technology allows for certain types of sensitive information not immediately detectable to the naked eye to be discerned from biometric data. For example, tools analyzing faces, irises, or a person's gait can derive information on the respective person's health.[162] While such advanced systems may make significant positive inroads as diagnostic tools, their use may raise red flags when employed without the data subject's consent and for purposes other than safeguarding the person's right to enjoy the highest attainable standard of physical or mental health. Biometric data may also be employed to divulge information on a person's sexual orientation, as demonstrated by a study conducted by two Stanford academics.[163] Unlike technology analyzing health conditions based on biometric data, it is challenging to imagine a legitimate use of such technology that is in line with public interest. However, as highlighted by the authors of the study, "given that companies and governments are increasingly using computer vision algorithms to detect people's intimate traits,"[164] and are "developing and deploying face-based prediction tools aimed at intimate psycho–demographic traits, such as the likelihood of committing a crime, being a terrorist or a pedophile,"[165] the findings also expose a threat to the privacy and safety of LGBTI+ persons."[166]

As the above examples also demonstrate, technology allows for increasingly sophisticated ways of processing biometric data through the use of automation, diverse machine learning algorithms, and artificial intelligence

159 *See also* subsection C(4)(c) below.
160 Antitza Dantcheva, Petros Elia and Arun Ross, 'What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics', 11(3) IEEE Transactions on Information Forensics and Security 441 (2015).
161 Roderick B. Woo, 'Challenges Posed by Biometric Technology on Data Privacy Protection and the Way Forward', Ethics and Policy of Biometrics, 2010, Volume 6005, pp. 1-6.
162 For example. body mass index (BMI) may be determined based on facial images, thereby suggesting the possibility of assessing health from biometric data. A person's DNA sample may similarly disclose sensitive health information, such as genetic predisposition to certain illnesses, affecting not only the data subject but also biological next of kin.
163 *See* Michal Kosinski and Yilun Wang, 'Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images', Journal of Personality and Social Psychology, Vol. 114, Issue 2, pp. 246-257. As the authors note, "[g]iven a single facial image, a classifier could correctly distinguish between gay and heterosexual men in 81% of cases, and in 71% of cases for women. Human judges achieved much lower accuracy: 61% for men and 54% for women. The accuracy of the algorithm increased to 91% and 83%, respectively, given five facial images per person."
See also, Tactical Tech, 'Quantifying Homosexuality: A Critique', available at https://ourdataourselves.tacticaltech.org/posts/40-quantifying-homosexuality-critique/ (visited 19 February 2020); Tristan Greene, 'The Stanford Gaydar AI is Hogwash', The Next Web, 20 February 2018, available at https://thenextweb.com/artificial-intelligence/2018/02/20/opinion-the-stanford-gaydar-ai-is-hogwash/ (visited 19 February 2020).
164 Michal Kosinski and Yilun Wang, 'Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images', Journal of Personality and Social Psychology, Vol. 114, Issue 2, p. 2.
165 *Ibid.*, p. 8.
166 *Ibid.*, p. 7.

(AI). These developments allow for the processing of large datasets and have contributed to making biometric tools and systems safer and more reliable.[167] At the same time, algorithms driving some of these tools have been shown to suffer from bias.[168] Studies have demonstrated that the majority of facial recognition technologies show gender and racial bias leading to less reliable results when identifying women and persons with darker skin tones.[169] This has real-life implications and may lead to false positives or false negatives, including in the counter-terrorism context, such as during screening at border checks or in the context of real-time surveillance using facial recognition. Moreover, facial recognition tools are increasingly used to assess a person's facial expressions with the aim of deducing the subject's emotional state,[170] including in a law enforcement context[171], despite such tools exhibiting insufficient levels of sensitivity to cultural and other differences in ways in which people behave and emote.[172]

167 For example, algorithms in biometric tools relating to fingerprint or facial recognition now can adjust for change in a person's biometrics over time, for example as part of the aging process.

168 *See*, for example, Ali Breland, 'How White Engineers Built Racist Code – And Why It's Dangerous for Black People', The Guardian, 4 December 2017, available at https://www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police (visited 19 February 2020); Matt Burgess, 'Holding AI to Account: Will Algorithms Ever Be Free from Bias If They're Created by Humans?', WIRED, 11 January 2016, available at https://www.wired.co.uk/article/creating-transparent-ai-algorithms-machine-learning (visited 19 February 2020).

169 Joy Buolamwini, 'Response: Racial and Gender Bias in Amazon Rekognition — Commercial AI System for Analyzing Faces', Medium, 25 January 2019, available at https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced (visited 19 February 2020); National Institute of Standards and Technology, 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software', 19 December 2019, available at https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software (visited 19 February 2020).

170 *See* Michael Fairhurst, Cheng Li and Márjory Da Costa-Abreu, 'Predictive Biometrics: A Review and Analysis of Predicting Personal Characteristics from Biometric Data', IET Biometrics, The Institution of Engineering and Technology 2017, pp. 369-378.

171 *United Nations Compendium of Recommend Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism* (2018), p. 75.

172 *See*, for example, Ivan Manokha, 'Facial Analysis AI Is Being Used In Job Interviews – It Will Probably Reinforce Inequality', The Conversation, 7 October 2019, available at http://theconversation.com/facial-analysis-ai-is-being-used-in-job-interviews-it-will-probably-reinforce-inequality-124790 (visited 19 February 2020); Alex Lee, 'An AI to Stop Hiring Bias Could Be Bad News for Disabled People', WIRED, 26 November 2019, available at https://www.wired.co.uk/article/ai-hiring-bias-disabled-people (visited 19 February 2020).

Restrictions on the use of facial recognition technologies

Many States and companies are stepping up the use of facial recognition. India is planning on setting up a nationwide facial recognition system.[173] A number of local authorities in Brazil have adopted the use of some kind of facial recognition software, with about half of these initiatives instituted in the past two years.[174] At the same time, opposite trends are also discernable. Due to concerns regarding the accuracy and the potential negative individual and societal impact linked to the use of facial recognition technologies, some governments and local authorities have recently taken steps aimed at imposing moratoria on the deployment of such technology. In the US, various pieces of draft federal legislation have been proposed in this respect,[175] with senators Jeff Merkley and Cory Booker having recently introduced a bill pursuing temporary restrictions on the use of facial recognition by federal authorities.[176] These developments follow repeated calls by civil liberties, privacy, and other groups arguing that the use of such technology should be suspended, pending further review.[177] The State of California and some US cities[178] already have temporary restrictions in place, with legislation pending elsewhere.[179] These developments are not unique to the US: many jurisdictions worldwide ponder ways to meaningfully address the challenges posed by the use of facial recognition technology. Morocco has recently introduced a rather short but comprehensive moratorium on the use of the technology, justified rightly on the grounds of Morocco's human rights obligations.[180] The European Union and its Member States have also grappled with finding the optimum way to approach the problem—however, the latest version of the European Commission's White Paper on AI walks back on a suggestion contained in previous versions to impose a 5-year moratorium on the use of relevant technologies.[181]

---

173 Vasudevan Sridharan, 'India Setting Up World's Biggest Facial Recognition System', Deutsche Welle, 7 November 2019, available at https://www.dw.com/en/india-setting-up-worlds-biggest-facial-recognition-system/a-51147243, (visited 19 February 2020).

174 Jonas Valente, 'Face Recognition Tech Gains Ground in Brazil', Agencia Brasil, 20 September 2019, available at http://agenciabrasil.ebc.com.br/en/geral/noticia/2019-09/face-recognition-tech-gains-ground-brazil, (visited 19 February 2020); The Christian Science Monitor, 'Brazil Takes a Page From China, Taps Facial Recognition to Solve Crime', 12 February 2020, available at https://cacm.acm.org/news/242783-brazil-takes-a-page-from-china-taps-facial-recognition-to-solve-crime/fulltext, (visited 19 February 2020).

175 As of March 2020, none have passed through Congress.

See also, Chris Mills Rodrigo, 'Booker, Merkley Propose Federal Facial Recognition Moratorium', 12 February 2020, available at https://thehill.com/policy/technology/482815-booker-merkley-propose-facial-recognition-moratorium, (visited 19 February 2020).

176 'A Bill to create a moratorium on the government use of facial recognition technology until a Commission recommends the appropriate guidelines and limitation for use of facial recognition technology', 116th Congress, 2nd Session, available at https://www.merkley.senate.gov/imo/media/doc/20.02.12%20Facial%20Recognition.pdf; (visited 19 February 2020).

See also, Richard Lawler, 'Senate Bill Would Place a Moratorium on Feds Using Facial Recognition', Endgadget, 13 February 2020, available at https://www.engadget.com/2020/02/13/ethical-use-of-ai-act-facial-recognition/, (visited 19 February 2020). It must be noted that this Bill would restrict use until Congress passes relevant legislation. At the same time, the Bill does not propose a full moratorium and allows for example for police authorities to continue make use of such technologies, subject to a warrant.

177 *See* Coalition letter to the US House Oversight and Reform Committee, available here: https://www.aclu.org/letter/coalition-letter-calling-federal-moratorium-face-recognition, (visited 19 February 2020); and Letter to the Privacy and Civil Liberties Oversight Board, available here: https://epic.org/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf, (visited 19 February 2020).

178 The cities include San Francisco and Oakland in California, and Somerville in Massachusetts. *See* Electronic Privacy Information Center, 'State Facial Recognition Policy', available at https://epic.org/state-policy/facialrecognition/, (visited 19 February 2020).

179 Khari Johnson, 'From Washington State to Washington, D.C., Lawmakers Rush to Regulate Facial Recognition', Venture Beat, 19 January 2020, available at https://venturebeat.com/2020/01/19/from-washington-state-to-washington-dc-lawmakers-rush-to-regulate-facial-recognition/, (visited 19 February 2020).

180 Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel, Délibération n° D-194-2019 du 30/08/2019 relative à un moratoire sur la reconnaissance faciale, available at https://www.cndp.ma/images/deliberations/deliberation-n-D-194-2019-30-08-2019.pdf, (visited 19 February 2020).

181 Financial Times, 'EU Backs Away from Call for Blanket Ban on Facial Recognition Tech', 11 February 2020, available at https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5, (visited 19 February 2020); 'Structure for the White Paper on Artificial Intelligence – A European approach', available at https://www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf, (visited 19 February 2020).

Facial recognition technologies are, of course, not the only ones shown to exhibit bias: voice recognition software, for example, regularly performs worse in recognizing women's voices, despite women on average having higher speech intelligibility than men.[182] Similar concerns are valid with recognition of non-standard accents which frequently includes racial or ethnic minorities.[183]

The above outlined examples may negatively affect protections for the right to non-discrimination and equal treatment before the law[184] and may have further implications on rights such as the right to liberty and security of person, freedom of movement, freedom of assembly, the prohibition of arbitrary deprivation of liberty as well as due process and fair trial rights. Furthermore, as also highlighted above, these implications are likely to be amplified in case of groups and persons who are already marginalized or discriminated against, as well as groups and persons in vulnerable situations.

Recommendations:

- **The potential for fundamentally discriminatory impact of biometric data is exceptionally high and requires State action aimed at ensuring and safeguarding transparency and accountability of automated processes.**
- **Human rights impact assessment as well as relevant monitoring and evaluation processes must address the disparate impact of such technologies and data usage on underprivileged and marginalized groups as well as persons and groups in a vulnerable situation.**

c. Domestic and cross-border sharing of biometric data

Human rights concerns dominate with respect to the means and modalities of sharing biometric data,[185] both domestically and internationally. As flagged earlier, Security Council resolution 2396 also encourages "responsible" sharing of biometric data domestically, with Member States, and international bodies.

Broad data-sharing practices between diverse domestic authorities, public and private actors, and between States themselves, are becoming normalized. This means that purpose limitation-related safeguards are increasingly challenging to meaningfully implement and implies that:

- Data gathered for counter-terrorism purposes may be shared with broader stakeholders, including public authorities and potentially also private actors; and
- Data gathered for purposes other than counter-terrorism may be shared with security sector actors to be used in preventing or countering terrorism.

Such practices need sustained attention to ensure that they comply with requirements related to legality, transparency, purpose limitation, and data minimization.

At the domestic level, law enforcement and counter-terrorism actors are often given access to databases set up and operated by other public authorities. While regulated targeted access to relevant data can greatly facilitate law enforcement and counter-terrorism operations, allowing sweeping access for a broad range of actors raises necessity and proportionality concerns. The question of such access has arisen in relation to the Aadhaar database in India, commonly understood to be the largest database of biometric information that the world currently knows.[186] Domestic courts recognized that access to the data by multiple actors raised legitimate concerns and held that such access must be linked to effective safeguards that protect against abuse, including in relation to authorization and oversight.[187]

With reference to domestic sharing of data, the *United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism* makes the case that "lawful integration of all national law enforcement biometric databases into a 'national

182 Caroline Criado Perez, *Invisible Women*, (Abrams Press, New York, 2019); Tina Tallon, 'A Century of "Shrill": How Bias in Technology Has Hurt Women's Voices', The New Yorker, 3 September 2019, available at https://www.newyorker.com/culture/cultural-comment/a-century-of-shrill-how-bias-in-technology-has-hurt-womens-voices, (visited 19 February 2020).

183 Joan Palmiter Bajorek, 'Voice Recognition Still Has Significant Race and Gender Biases', Harvard Business Review, 10 May 2019, available at https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases, (visited 19 February 2020).

184 The right to equality and non-discrimination is part of the foundations of the rule of law and human rights. It is protected in all core human rights treaties as well as in the Universal Declaration of Human Rights (articles 1 and 7).

185 Please note that the observations related to data-sharing contained in this report are equally valid to any arrangements concerning providing access to data. While permissions linked to access differ (they may allow or prohibit copying; include or preclude data editing privileges, etc.), the authors consider providing access a modality of data-sharing.

186 *See*, e.g., Michael Safi, 'Indian Court Upholds Legality of World's Largest Biometric Database', The Guardian, 26 September 2018, available at https://www.theguardian.com/world/2018/sep/26/indian-court-upholds-legality-of-worlds-largest-biometric-database (visited 20 February 2020).

187 Writ Petition (Civil) No. 494 of 2012, Justice K.S. Puttaswamy (Retd.) and another versus Union of India and others, paras. 219 (c) and (d), available at https://indiankanoon.org/doc/127517806/, (visited 19 February 2020).

watch list' configuration […] would expose the optimum amount of relevant data to watch list searches."[188] In addition to traditional authentication and identification purposes, such integrated databases can be used to "pro-actively to infer and predict potential future actions and associations."[189] The mandate of the Special Rapporteur emphasizes that States opting for an integrated national database would need to justify why this alternative is necessary and proportionate for effectively addressing existing threats. It is notable that the Compendium does not address necessity and proportionality considerations, or ways to ensure that such measures comply with the principles of purpose limitation and data minimization in its analysis. The mandate of the Special Rapporteur takes the position that, from a human rights point of view, optimum levels of data-sharing are rarely synonymous with sharing the data as broadly as feasible.[190]

The 2018 Addendum to the 2015 Madrid Principles recommends that "systems operating biometric data and the legal frameworks associated with their use allow for interoperability between other national and international biometric databases, including INTERPOL."[191] While efficient international and regional cooperation may serve as a potent tool for successfully countering terrorism, such cooperation, whether in the area of judicial assistance or intelligence-sharing, is not a rights-free zone. The need for measures taken to combat terrorism, notwithstanding their nature or the context in which they were enacted, to be in compliance with obligations under international law, in particular international human rights, refugee and humanitarian law has also been underscored by the General Assembly, the Human Rights Council, and the Security Council.[192]

As highlighted earlier, Security Council resolution 2396 also encourages "responsible" sharing of biometric data domestically, with Member States, and international bodies. In the context of international data-sharing arrangements and practices, governments will be faced with dilemmas. These include:

- State sovereignty considerations;
- Jurisdictional complexities; and
- Complications caused by the diverging legal and policy frameworks and standards applicable in different jurisdictions.

In the absence of protective parity, the implementation of measures advocated for States by the Security Council is likely to contribute to greater privacy intrusions, which in turn lead to enhanced risk to the protection of interlinked rights. For this reason, the mandate of the Special Rapporteur takes the view that States must avoid any form of cooperation that may facilitate human rights violations or abuses. State must also be mindful that state responsibility under international law may be triggered through the sharing of information that contributes to the commission of gross human rights violations.

Cross-border intelligence-sharing arrangements raise particular human rights concerns. International human rights mechanisms, including the mandate of the Special Rapporteur have repeatedly warned against such arrangements falling short of international human rights norms and standards, particularly the lack of a human rights-compliant legal basis and of adequate oversight.[193] However, relevant information-sharing agreements are frequently not only not based on law but are classified and as such not subject to any democratic or public scrutiny.[194] The lack of such scrutiny may also be manifest in case of Security Council-mandated measures where ordinary domestic regulatory processes may be entirely sidestepped. Therefore, private or sensitive information concerning individuals may be shared with foreign intelligence agencies without the protection of a publicly available legal framework and without proper safeguards,[195] making the operation of such regimes unforeseeable for those affected by it.[196] Moreover, such arrangements may lead to information gathered for one purpose being used for other unrelated governmental objectives. This "purpose creep" presents concerns not

188 *United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism*, p. 61.
189 *Ibid.*, p. 67.
190 *See also* Privacy International, 'Briefing to the UN Counter-Terrorism Executive Directorate on the Responsible Use and Sharing of Biometric Data to Tackle Terrorism' (June 2019), p. 7.
191 2018 Addendum to the 2015 Madrid Guiding Principles, S/2018/1177, Guideline 3 (h).
The UN Compendium has a similar recommendation noting that "the aggregation of disparate, single-mode databases […] 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." *See United Nations Compendium of Recommend Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism*, p. 63.
192 *See* S/RES/1373 (2001), 1456 (2003), 1566 (2004), 1624 (2005), 2178 (2014), 2341 (2017), 2354 (2017), 2368 (2017), 2370 (2017), 2395 (2017), 2396 (2017) 2462 (2019) and 2482 (2019); A/RES/68/167; A/RES/69/166; A/RES/71/199; A/RES49/60; A/RES 51/210; A/RES/72/123; A/RES/72/180; A/HRC/RES/28/16; A/HRC/RES/34/7.
193 *See*, for example, A/69/397 and A/ HRC/13/37.
194 *See* 'The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights', A/HRC/27/37. See also, Privacy International, 'Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards' (April 2018).
195 A/HRC/27/37, para. 30.
196 A/69/397, para. 44.

only because of reducing foreseeability, but also because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another.[197]

In addition to the above addressed shortcomings, intelligence-sharing arrangements tend to be—more often than not—exempted from the supervision of an independent authority.[198] Oversight bodies are typically not informed of the conclusion of intelligence-sharing agreements and therefore unlikely to review the compatibility of such agreements with domestic and international law. Due to limitations justified by state sovereignty, they have very little or no oversight over the use of information shared with foreign agencies. Moreover, they are limited in their powers to seek or verify information about the means and methods of collection, retention, and processing of information shared by another State, particularly as intelligence-sharing arrangements regularly prohibit the disclosure of such information to third parties.

Recommendations:

- **Data-sharing arrangements and practices must be provided for by law and strictly comply with the principles of necessity and proportionality.**
- **States must take necessary and effective measures to avoid any form of international cooperation that may facilitate human rights violations or abuses.**
- **Independent oversight of the activities of intelligence agencies must encompass all forms of data usage, including cross-border data-sharing cooperation.**

5. The obligation to develop and implement biometric systems under UNSCR 2396

Complying with the above set out requirements put in place under human rights law would require that competent domestic authorities develop comprehensive national legal frameworks regulating the use of biometric tools and data. Such regulation should follow a threat assessment and a human rights impact assessment and provide for measures that are necessary and adequate for efficiently tackling relevant threats. Due to the obligations imposed under Security Council resolution 2396, such domestic assessments may be considered moot and sidestepped. This would be a concerning development considering the lack of any meaningful human rights risk assessment conducted by the Security Council in the context of developing the resolution. Such approach would also go against the obligation of States to implement duties pursuant to Security Council resolutions with due respect for binding human rights obligations of States, a requirement explicitly contained in para. 15 of the resolution.

Recommendation:

- **Competent domestic authorities must develop comprehensive national frameworks regulating the use of biometric tools and data as a matter of best practice and to ensure compliance with international human rights norms and standards.**

D. State-business cooperation in law enforcement and national security contexts and the human rights-compliant developments and deployment of biometric tools

Technology employed to collect and process biometric data is overwhelmingly developed by private companies at their own initiative or following solicitation of commission by government authorities. Indeed, in the context of surveillance technology, the growing reliance by States on the private sector to conduct and facilitate digital surveillance is well-established.[199] The capacity of States to conduct surveillance may even "depend on the extent to which business enterprises cooperate with or resist such surveillance."[200]

1. International standards applicable to business conduct

The broad human rights implications linked to the use of biometrics, highlighted above,[201] means that the companies developing and deploying biometric tools and their business relationships (whether State or non-State) have far-reaching influence on ways in which human rights of large categories of persons are safeguarded. Such influence may be employed to further the fulfilment of diverse human rights in the context of the services that

197 A/HRC/13/37, para. 50; A/69/397, para. 56.
198 A/HRC/13/37, A/69/397.
199 A/HRC/27/37, para. 3ff.
200 A/HRC/32/38, para. 57.
201 *See*, in particular, Section C.

they provide but can equally be used to limit the enjoyment of those rights.

The growing role of corporate actors and their increased impact on the enjoyment of human rights is addressed by the UN Guiding Principles on Business and Human Rights (UNGPs), providing an authoritative global standard for preventing and addressing adverse human rights impacts linked to business activity. While the UNGPs have been endorsed by the Human Rights Council in resolution 17/4 of 16 June 2011,[202] they are not formally legally binding. They represent however an important step towards matching the impact of business on human rights with corresponding levels of corporate responsibility. They further represent the course of development under international law, as many soft law norms contained in the UNGPs are expected to crystalize to hard law obligations over time and use. As such, they are being recognized, accepted, and implemented by a growing number of private companies.

At the same time, as the Interpretive Guide to the UNGPs specifies, "[t]he responsibility of business enterprises to respect human rights is distinct from issues of legal liability and enforcement, which remain defined largely by national law provisions in relevant jurisdictions."[203] As the responsibilities entailed in the UNGPs are not legally enforceable, applicable domestic legislation frequently falls short of ensuring full corporate accountability.

a. Responsibility to create a due diligence framework

Under the UNGPs, the responsibility to respect internationally recognized human rights[204] implies that businesses must "[a]void causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur" and "[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships" (including users of products and services), even if they have not contributed to those impacts.[205]

Corporate responsibility in the context of the UNGPs is independent of State obligations and thus "exists over and above compliance with national laws" and irrespective of States' abilities and/or willingness to fulfil their own duties under human rights law.[206] Businesses therefore cannot invoke the host or other involved States' poor human rights record as a justification for their own conduct. This is further evidenced by the requirement that companies exercise due diligence in preventing and mitigating adverse human rights impact resulted through actions of their business relationships.[207] Companies may therefore risk contributing to human rights violations and may under certain circumstances be morally or legally complicit in such violations, if they supply States with technology or data without complying with their due diligence obligations to safeguard against abuse, or provide data pursuant to requests that violate international human rights standards or where the data is otherwise used in violation of international human rights law.[208]

Policy commitment

In line with the UNGPs, businesses should adopt an explicit and public policy commitment to meet their responsibility to respect human rights and the commitment should be reflected in operational policies and procedures governing their activities.[209] To aid this process, businesses should identify the human rights the enterprise's activities are most likely to impact and effective ways to prevent and/or mitigate such impact.[210]

Risk assessment

Human rights due diligence on part of businesses involves conducting risk assessments examining actual and potential human rights impacts, both direct and indirect, of the business's operations.[211] Risk assessments should encompass all phases and aspects of business activities

202 A/HRC/17/4.
203 Office of the High Commissioner for Human Rights, *The Corporate Responsibility to Respect Human Rights. An Interpretive Guide* (2012), at 14. *See also* P. Simons and A. Macklin, The Governance Gap (Routledge, 2014), p. 4.
204 These are understood to include, at a minimum, the rights expressed in the International Bill of Human Rights (comprising the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights, and the International Covenant on Civil and Political Rights) and the principles concerning fundamental rights set out in the International Labour Organization's Declaration on Fundamental Principles and Rights at Work. *See* UNGPs, Principle 12.
205 UNGPs, Principle 13.
206 *See The Corporate Responsibility to Respect Human Rights. An Interpretive Guide*, p. 13.
207 UNGPs, Principle 13.
208 At the same time, business responsibility in no way affects or diminishes the State's role as the primary duty-bearer when it comes to ensuring human rights protection for all persons within the State's jurisdiction. This is reflected in the UNGPs in Principles 1-10.
209 UNGPs, Principle 15.
The policy commitment should clearly set out expectations from employees of the company (including management) and their business relationships.
210 *The Corporate Responsibility to Respect Human Rights. An Interpretive Guide*, p. 28.
211 See ibid., at 15ff. See also Shift and Institute for Human Rights and Business, 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights' (European Commission, 2013).

and monitor how the nature and scope of the risks may change over time. Such comprehensive monitoring allows for a timely and effective response on part of the company.

In this vein, companies should make sure that human rights considerations are given due weight at all operational stages. In the context of data-handling, this would include collection, retention, processing and sharing as well as disposal of data. When it comes to relevant technological tools, due diligence responsibilities cover all phases of technology development and deployment, including in relation to the sale or transfer of the product, as well as after-sales support and maintenance. Companies should have a policy in place setting up minimum standards regarding the existing legal and policy framework, including regulatory safeguards and oversight that must be in place in countries where they operate or the government or public authorities of which they have developed business relations with. As part of their due diligence process, companies must also assess any potential business relationships, including public authorities, to identify, prevent and mitigate potential human rights impact prior to entering contractual relationships. Such arrangements should incorporate end-user assurances against unlawful or arbitrary use of technology or infrastructure.

The findings resulting from the human rights due diligence process, including from risk assessments, should inform action taken by the company to prevent adverse impact or mitigate the effects where the impact occurs. The impact of such efforts should also be monitored and evaluated for efficiency.

Accountability mechanisms

Companies are required to set up internal accountability mechanisms for the implementation of human rights policies.[212] Furthermore, in line with the "respect, protect, remedy" framework set out under the UNGPs, companies should have processes in place that enable the remediation of adverse human rights impacts that the company caused or contributed to.[213] In this sense, operational-level grievance mechanisms may be an effective means to ensure access to remedies for stakeholders whose legitimate interests have been infringed upon by the company.[214] The existence of such mechanisms may be of particular significance in contexts where access to effective judicial and quasi-judicial remedies is restricted or lacking.

Reporting and other forms of external communication

The UNGPs also stipulate that corporations should communicate externally how they address human rights impacts linked to their operations, particularly when concerns are raised by or on behalf of affected stakeholders.[215] Companies should report on their business relationship with governments and public authorities, unless such reporting is prohibited under national law.[216] However, States themselves should also be transparent about technology purchases and transfers and other relevant transactions related to acquiring biometric tools and data and should refrain from imposing blanket prohibitions on companies to reveal information about technology sales and transfer.[217] Importantly, meaningful transparency would further include public reporting on lobbying activities of companies active in this space.

212 UNGPs, Principles 22, 29 and 31.

213 *See The Corporate Responsibility to Respect Human Rights. An Interpretive Guide*, Section III; 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights', Section VI.

214 In accordance with Principle 31, such grievance mechanisms can be considered effective if they are 1) legitimate, 2) accessible, 3) predictable, 4) equitable, 5) transparent, 6) rights-compatible, 7) a source of continuous learning and 8) based on engagement and dialogue.

215 UNGPs, Principle 21. In addition to the Guiding Principles, reporting requirements have been set up by interest groups and regional organizations. For example, companies acceding to the UN Global Compact are to "embrace, support and enact, within their sphere of influence", the principles of the Global Compact and they are to report annually on the initiatives taken to make those principles part of their operations. In this sense, *see* United Nations Global Compact, 'Reporting' at https://www.unglobalcompact.org/participation/report.
Directive 2014/95/EU of the European Parliament and of the Council amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups requires companies of a certain size that can be classified as public interest entities to report on a number of issue areas, including respect for human rights.

216 In instances where the domestic legal or policy framework hinders such reporting, companies should use their leverage with the government and other relevant stakeholders (such as the diplomatic representation of their own government in case they are operating abroad) and advocate for the possibility to make such information available, including through changes in the law.

217 While restrictions on reporting may, under certain circumstances and for a limited time, be warranted, such limitations should only be imposed to the extent they are strictly necessary and proportionate to the protection of a legitimate interest.

b. Importance of a corporate due diligence framework

Setting up a due diligence framework that complies with the above considerations goes a long way towards enabling companies to act in line with their responsibilities under the UNGPs. The existence of such policies and mechanisms is particularly important in situations where companies have limited opportunity to monitor ways in which State authorities use technology or data acquired from the business.

Many companies operate in environments where domestic legislation and policies fall short of requirements under international human rights law. This phenomenon is distinctly noticeable in the national security context, particularly with respect to measures aimed at preventing and countering terrorism-related offences, and has a considerable negative impact on the ability of companies to comply with their responsibilities under the "respect, protect, remedy" framework set up by the UNGPs.

Operating in these conditions may cause the companies to contribute to human rights violations and may result in moral or legal complicity. The challenges raised in this context come with no straightforward solutions. They however highlight the importance of stepping up corporate efforts to prevent, mitigate, and challenge the adverse human rights impact that companies may be contributing to, including through collaborative efforts, such as interest groups and public-private partnerships.

At the same time, there is extremely limited publicly available information on whether companies producing, selling or transferring biometric tools or data have an adequate due diligence framework in place and whether carrying out human rights risk assessments of their activities and evaluating the human rights record of business relationships is a regular part of relevant corporate processes. While a number of such companies publicly state their commitment to human rights,[218] they do not provide information on ways in which such commitment is operationalized, including with respect to their business relationships. This, at the very least, points to an incomplete due diligence framework that is missing mechanisms and processes aimed at ensuring transparency. Moreover, the widespread concerns raised concerning a number of biometric tools and ways in which these are employed by public authorities, including in a national security or surveillance context, make skepticism in relation to corporate due diligence in this area warranted.

Recommendations:

- **Business enterprises must ensure that their operations are guided by international human rights law, including the "respect, protect, remedy" framework set up under the United Nations Guiding Principles on Business and Human Rights.**
- **Businesses should adopt an explicit and public policy commitment to meet their responsibility to respect human rights and the commitment should be reflected in operational policies and procedures governing their activities.**
- **Business enterprises must conduct human rights due diligence. This includes conducting risk assessments examining actual and potential human rights impacts, both direct and indirect, of the business's operations. Risk assessments must encompass all phases and aspects of the business's operations and monitor how the nature and scope of the risks may change over time.**

2. State duties vis-à-vis third-party conduct

In the context of their obligations under international human rights law, States have the duty to protect persons within their jurisdiction from undue interference with

218 For example, the Booz Allen Hamilton Code of Business Ethics and Conduct states that the company "honors" and "celebrates" human rights and emphasize their support for the UNGPs but granular information on how such commitment is operationalized is largely lacking. *See* 'Booz Allen Hamilton Code of Business Ethics and Conduct', available at https://investors.boozallen.com/static-files/f708a2e9-5fb1-4ba2-9850-0233b683716c (visited 20 February 2020). Amazon's Global Human Rights Principles state that the company is guided by the UNGPs and supports the Universal Declaration of Human Rights. *See* Amazon, 'Global Human Rights Principles', available at https://sustainability.aboutamazon.com/governance/amazon-global-human-rights-principles (visited 20 February 2020). Again, detailed information on how such values are reflected in their operations is not readily available. It is also notable in relation to Amazon's biometrics-related operations that Amazon investors have recently voted against limiting the sale of facial recognition technology to public authorities and rejected a proposal aimed at commissioning an independent report on the impact of their software, Rekognition. *See* Kris Holt, 'Amazon Investors Reject Call to Limit Facial Recognition System Sales', Endgadget, 22 May 2019, available at https://www.engadget.com/2019/05/22/amazon-facial-recognition-law-enforcement-shareholders-climate-change/ (visited 20 February 2020). Cyber-intelligence company NSO Group has recently adopted a human rights policy document stating the firm's commitment to the International Bill of Rights and the UNGPs. It also provides information about due diligence processes and states, among others, that NSO Group thoroughly evaluates human rights impact arising from the misuse of their products by considering the specific customer, their past human rights performance and governance standards in the country involved. *See* NSO Group, 'Human Rights Policy' (September 2019), available at https://www.nsogroup.com/wp-content/uploads/2019/09/NSO-Human-Rights-Policy_September19.pdf (visited 20 February 2020). Human rights actors are however skeptical about the level of commitment on part of the company to meaningfully implement the policy, due to the company's history with its products repeatedly used to commit human rights violations, particularly as its current business relationships also seem to include governments with problematic human rights records. *See*, for example, Eva Galperin and Cindy Cohn, 'Private Companies, Government Surveillance Software and Human Rights', Electronic Frontier Foundation, 28 October 2019, available at https://www.eff.org/deeplinks/2019/10/applying-human-rights-framework-sale-government-surveillance-software (visited 20 February 2020).

their human rights by third parties, including private actors such as business enterprises. States' duty to ensure respect for human rights implies the obligation to enact legislation on the basis of which they can take necessary and adequate measures to prevent, investigate, and punish activities that endanger these rights and to offer redress in case abuses have occurred.[219] This is also reflected in the "protect, respect, and remedy" framework of the UNGPs which urge States to "exercise adequate oversight when they contract with, or legislate for, business enterprises to provide services that may have an impact on the enjoyment of human rights."[220] The obligation to safeguard human rights against interference by third parties is particularly important in the context of biometrics keeping in mind the high human rights risk associated with 1) use of sensitive personal information, combined with 2) the use of automated tools, many powered by algorithms or artificial intelligence software.

In line with their human rights obligations, States must set up a domestic framework that requires businesses operating within their jurisdiction (including with respect to their activities with transnational impact) to:

- Create a due diligence framework and carry out human rights risk assessment and monitoring with respect to their activities and the activities of their business relationships;
- Commit to human rights-compliant policies;
- Commit to public reporting on ways in which these policies are implemented as well as their efficiency; and
- Set up accountability mechanisms.[221]

Draft UN Treaty on Business and Human Rights

The above requirements are also highlighted in the draft *Legally binding instrument to regulate, in international human rights law, the activities of transnational corporations and other business enterprises.*[222] The draft instrument includes a provision requiring States to adopt "measures necessary to ensure that all persons conducting business activities, including those of transnational character, undertake human rights due diligence." Human rights due diligence includes "identifying and assessing any actual or potential human rights violations or abuses that may arise from their business activities or from their contractual relationships." It further requires taking appropriate actions to prevent these violations or abuses, monitor human rights impact, publicly account for corporate policies and the results and implications of those policies, including through reporting publicly and periodically.

219 International Covenant on Civil and Political Rights, article 2.
220 UNGPs, Principle 5.
221 Similar recommendations are also contained in the OECD Guidelines for Multinational Enterprises, available at http://mneguidelines.oecd.org/guidelines/ (visited 20 February 2020).
222 Revised Legally binding instrument to regulate, in international human rights law, the activities of transnational corporations and other business enterprises, OEIGWG Chairmanship Revised Draft (16 July 2019) available at https://www.ohchr.org/Documents/HRBodies/HRCouncil/WGTransCorp/OEIGWG_RevisedDraft_LBI.pdf (visited 20 February 2020).

The challenge of future-proofing laws and policies

To paraphrase the 2018 Addendum to the 2015 Madrid Guiding Principles, **as Member States' use of biometric tools and data continues to expand, the parameters for their human rights-compliant use continue to evolve accordingly**. Bridging the gap between technological developments and legal and policy responses is a constant challenge for governments and one that comes with a set of problems with no obvious solutions. The nature and pace of technological developments impacts foreseeability of the implications of technology. This highlights the importance that human rights principles and safeguards, including independent oversight, are duly reflected in the legal and policy framework and, as a result, meaningfully incorporated in relevant processes. Critically, robust human rights assessments, including effective monitoring and evaluation processes, are a *sine qua non* of safeguarding against negative human rights ramifications resulting from the use of technology. A human rights-conscious approach also necessitates due attention to implementing strong protections on data-sharing and use; reduced foreseeability of future implications also means that consequences of data use may not have been foreseeable at the time the data was collected. This raises challenges relating to the adequacy of informed consent as the basis for processing personal data, fairness and transparency in collection and processing, purpose limitation, and accountability in the handling of data. It further highlights the importance of assessing the lawfulness and human rights compliance of data use at every stage.

Against this background, the precautionary principle has the potential to provide for a useful tool in addressing challenges related to regulating the future impact of technologies. A "guiding principle of modern international law,"[223] the principle advocates for State decision-making to be guided by precaution in circumstances where there is scientific uncertainty around the potential impact of relevant activities, tools, and technology.[224] Importantly, the scope of the principle covers situations where there is insufficient information to prove an activity or tool unsafe. While the precautionary principle has primarily been applied in international environmental law[225] and international humanitarian law in relation to rules concerning the environmental impact of weapons,[226] adopting an analogous approach to technological development may be of considerable added value. Various stakeholders and experts have expressed support for expanding the precautionary principle to the governance of emerging technologies.[227] Stringent application of responsibilities and obligations under human rights law, including the duty of care connected to the prevention and mitigation of negative human rights impact, could provide for an essential component of the principle's operationalization.

223 Meinhard Schröder, 'Precautionary Approach/ Principle', Max Planck Encyclopedia of Public International Law, available at https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1603 (visited 20 February 2020).

224 *See, e.g.*, Sonia Boutillon, 'The Precautionary Principle: Development of an International Standard', 23 Michigan Journal of International Law 429 (2002); Owen McIntyre and Thomas Mosedale, 'The Precautionary Principle as a Norm of Customary International Law', Journal of Environmental Law, Volume 9, Issue 2, (1997) pp. 221–241.

225 *Ibid.*

226 Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law—Volume II*: Practice (ICRC/Cambridge University Press, 2005), Chapter 14, Section B.

227 *See, e.g.*, UNESCO and World Commission on the Ethics of Scientific Knowledge and Technology, 'The Precautionary Principle' (2005); Gregory E. Kaebnick, Elizabeth Heitman, James P. Collins et al., 'Precaution and Governance of Emerging Technologies', Science, Vol. 354, Issue 6313 (2016); Claudia Som, Lorenz M. Hilty and Andreas R. Köhler, 'The Precautionary Principle as a Framework for a Sustainable Information Society', Journal of Business Ethics, Vol. 85 (2009), pp. 493-505.

3. Challenges of State-business 'cooperation' and potential ways forward

As noted above, biometric tools are overwhelmingly developed and sold by private companies, frequently in the context of processes lacking transparency and not benefitting from human rights input. There is, for example, rising scrutiny towards initiatives by a large number of companies to develop facial recognition software. These companies are not limited to companies specializing in cyber-security but also include major tech companies, such as Amazon, Facebook, Google, and Microsoft.[228] While these companies may not be developing such tools with the primary aim of employing them for national security purposes, tools developed by them are used by security sector actors in a number of jurisdictions.[229] These companies are also very well-positioned to collect data of millions of users to power their algorithms, a concern that has been consistently flagged by privacy advocates. Governments also enter diverse partnerships with businesses in the context of which one party may provide the technology while the other the data to feed into the algorithm.[230]

The US border control database system[231] is based on biometrics developed by US security contractor Booz Allen Hamilton. This system is employed at US entry ports but has also been put at the disposal of other States and, based on the 2018 Country Reports on Terrorism, compiled by the US Department of State, has been used at 227 ports of entry in 23 countries to screen more than 300,000 travelers each day.[232] Other technology companies similarly partner with the US government as well as numerous other governments worldwide to assist with the development and implementation of biometric systems.

The role of Chinese facial recognition and biometric surveillance companies in facilitating data collection, surveillance and the implementation of initiatives by Chinese authorities, such as the social credit system, is well established.[233] Some of these companies have further partnered with public authorities in other countries, not only in Asia but also in Africa, Europe and Latin America.[234] Similarly, Russian firms have built sophisticated algorithms feeding the government's facial recognition network project,[235] and biometric technology developed by Russian companies has reportedly been transferred to various Central Asian governments.[236] Israeli companies are likewise at the forefront of such developments, with surveillance technology company, NSO Group having achieved notoriety in recent years for recurring reports about the misuse of its technology by some governments to target, among others, human rights defenders and journalists.[237] While there seems to be a certain level of unease on part of some (mostly European) governments to authorize transfer of surveillance technology to at least some governments with particularly poor rule of law and human rights records, this concern does not seem to be shared by a number of other governments playing significant roles in spyware transfers and companies operating under their jurisdiction.[238]

---

228 BBC News, 'US Lawmakers Concerned by Accuracy of Facial Recognition', 16 January 2020, available at https://www.bbc.com/news/technology-51130904 (visited 20 February 2020).

229 *See* AI Now Institute, 'AI Now Report 2018', New York University, available at https://ainowinstitute.org/AI_Now_2018_Report.pdf (visited 20 February 2020). *See also*, Matt Cagle and Nicole Ozer, 'Amazon Teams Up With Government to Deploy Dangerous New Facial Recognition Technology', American Civil Liberties Union, 22 May 2018, available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new (visited 20 February 2020); Kade Crockford, 'Over 150,000 People Tell Amazon: Stop Selling Facial Recognition Tech to Police', American Civil Liberties Union, 18 June 2018, available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/over-150000-people-tell-amazon-stop-selling-facial (visited 20 February 2020).

230 For example, US Customs and Border Protection partners with a number of airlines, including American Airlines, Delta and JetBlue. Airlines photograph each passenger when boarding and use the government's Biometric Exit Program's software to authenticate passengers in the process. While the use facial recognition in this context has been described as an opt-out system, travelers have reported that no information was provided in this regard during the boarding process.
See Kelly Yamanauchi, 'As Delta Air Lines Expands Face Recognition, Criticism Grows', Government Technology, 18 September 2019, available at https://www.govtech.com/products/As-Delta-Air-Lines-Expands-Face-Recognition-Criticism-Grows.html (visited 20 February 2020); Allie Funk, 'I Opted Out of Facial Recognition at the Airport—It Wasn't Easy', WIRED, 2 July 2019, available at https://www.wired.com/story/opt-out-of-facial-recognition-at-the-airport/ (visited 20 February 2020).

231 Personal Identification Secure Comparison and Evaluation System (PISCES), a project that falls under the Terrorist Interdiction Program (TIP) of the US Department of State.

232 Partner countries include Cameroon, Chad, Ethiopia, Iraq, Niger, Yemen, among others. *See* US Department of State, *Country Reports on Terrorism 2018*, available at https://www.state.gov/reports/country-reports-on-terrorism-2018/ (visited 20 February 2020).

233 Jon Fingas, 'Chinese Surveillance Company Found Tracking 2.5 Million People', Endgadget, 17 February 2019, available at: https://www.engadget.com/2019/02/17/chinese-surveillance-company-tracks-2-5-million-people/ (visited 20 February 2020).

234 These countries include Italy, Singapore, Ecuador, Malaysia, Zimbabwe, UAE, Ethiopia, South Africa, Bolivia, Saudi Arabia, Rwanda, etc. *See*, for example, Council on Foreign Relations, 'Authoritarians Are Exporting Surveillance Tech, And With it Their Vision for the Internet', 5 December 2018, available at https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet (visited 20 February 2020); Jun Mai, 'Ecuador Is Fighting Crime Using Chinese Surveillance Technology', South China Morning Post, 22 January 2018, available at https://www.scmp.com/news/china/diplomacy-defence/article/2129912/ecuador-fighting-crime-using-chinese-surveillance (visited 20 February 2020).

235 BBC News, 'Russia's Use of Facial Recognition Challenged in Court', 31 January 2020, available at https://www.bbc.com/news/technology-51324841 (visited 20 February 2020); Felix Light, 'Russia Is Building One of the World's Largest Facial Recognition Networks', The Moscow Times, 12 November 2019, available at https://www.themoscowtimes.com/2019/11/12/russia-building-one-of-worlds-largest-facial-recognition-networks-a68139 (visited 20 February 2020).

236 *See*, for example, Peter Bourgelais, 'Commonwealth of Surveillance States: on the Export and Resale of Russia Surveillance Technology to Post-Soviet Central Asia', Access Now, available at https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf (visited 20 February 2020).

237 *See* Amnesty International, 'Israel: Stop NSO Group Exporting Spyware to Human Rights Abusers', 14 January 2020, available at https://www.amnesty.org/en/latest/news/2020/01/israel-nso-spyware-revoke-export-license/ (visited 20 February 2020); Lucie Krahulcova and Isedua Oribhabor, 'New Report Shows 100+ Members of Civil Society Targeted as NSO Group Continues to Evade Scrutiny', Access Now, available at https://www.accessnow.org/new-report-shows-100-members-of-civil-society-targeted-as-nso-group-continues-to-evade-scrutiny/ (visited 20 February 2020).

238 Council on Foreign Relations, 'Authoritarians Are Exporting Surveillance Tech, And With it Their Vision for the Internet', available at https://www.cfr.org/blog/authoritarians-are-exporting-surveillance-tech-and-it-their-vision-internet (visited 20 February 2020).

These are but a few examples of companies active in this space developing, employing, selling, and transferring biometric tools and collecting, retaining, and processing relevant data. By all accounts, the number of companies active in the area of biometrics may at the very least be in the hundreds.[239] Mapping the commercial space comes with challenges, for a number of reasons. While considerable (and deserved) criticism has been directed at the human rights record and insufficient level of transparency of activities of Internet platforms, including social media companies, the businesses active in the "biometrics game" tend to be even less transparent about relevant operations, initiatives, and business partnerships. Many such companies are less "public-facing" than major Internet platforms[240] and, as such, are less sensitive to public opinion as this is less likely to affect their business.[241]

When addressing the human rights and rule of law implications of state-business cooperation in relation to biometrics, two main aspects need distinguishing: 1) implications related to transfer or sale of relevant technology; and 2) concerns raised by different means and modalities of sharing biometric data. In the following, this section will look into these two questions in more detail.

a. Transfer or sale of biometric technology

It is well established that the potential of biometric technologies to influence the enjoyment of a broad range of human rights is substantial. While the extent of such influence varies depending on the technology in question, many biometric tools, and definitely those used in a national security/ surveillance context, are, from a human rights perspective, high-risk technologies. As set out above, government obligations and business responsibilities under international human rights law imply a comprehensive due diligence duty aimed at ensuring that the development and deployment of such technology is compliant with international human rights norms and standards. It also mandates that necessary and adequate steps are taken to mitigate the risks of negative human rights impact at every stage of the product lifecycle.

Meaningful due diligence requires improved efforts on part of both governments and private companies. Due diligence implies conducting a comprehensive risk assessment to guide product development and deployment. This process should translate into a "human rights by design" approach[242] to the development of biometric tools, starting with the earliest stages of such processes. Whereas businesses should develop and implement relevant policies and processes at their own initiative, international human rights law requires States to set up enforcement frameworks in this regard. While some jurisdictions have taken steps towards ensuring more human-rights-conscious technology development by the private sector,[243] such initiatives are few and far between and frequently lack bite.

While the truism that technology was inherently neutral has been discredited,[244] in particular as concerns data-driven technologies, it is nonetheless true that most tools can be used in ways that uphold rule of law and human rights and in ways that violate them. This underscores the importance of due diligence obligations in relation to transfer and sale of technologies. The UNGPs clearly call on businesses to examine the human rights record of business relationships and analyze the possible negative human rights impact of doing business with them. To the extent such risks exist, businesses are required to implement necessary and effective mitigating measures and even to cease relevant transactions if mitigating measures prove insufficiently effective.

---

239 According to Privacy International, in 2016 there were well over five hundred companies developing, marketing and selling such products to government purchasers. *See* Privacy International, 'The Surveillance Industry and Human Rights. Privacy International submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (February 2019) available at https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx (visited 20 February 2020).

240 Even in case of 'public-facing' companies, such as Amazon, their operations concerning the development, deployment, sale and transfer of biometric tools tend to be less transparent than other aspects of the company's operations.

241 Companies such as Nexa Technologies (formerly known as Amesys), The Gamma Group, Hacking Team, or the NSO Group have been subject to considerable criticism relating to the use of their technology by governments to commit human rights violations, with relatively limited reaction on part of these businesses. *See*, for example, DJ Pangburn, 'The Secretive Billion-Dollar Company Helping Governments Hack Our Phones', Fast Company, 30 November 2017, available at https://www.fastcompany.com/40469864/the-billion-dollar-company-helping-governments-hack-our-phones (visited 20 February 2020); International Federation of Human Rights (FIDH), 'Amesys and Qosmos Targeted by the Judiciary: Is There a New Law on the Horizon?', 18 June 2013, available at https://www.fidh.org/en/region/europe-central-asia/france/amesys-and-qosmos-targeted-by-the-judiciary-is-there-a-new-law-on-the-13966 (visited 20 February 2020); Cora Currier, Morgan Marquis-Boire, 'A Detailed Look at Hacking Team's Emails About Its Repressive Clients', The Intercept, 7 July 2015, available at https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/ (visited 20 February 2020).

242 As also highlighted in the guidance of the European Commission on implementing the Guiding Principles in the information and communications technology sector, European Commission, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights (Luxembourg, 2013).

243 The government of the United Kingdom, in partnership with a technology industry association, produced a set of guidelines for the cybersecurity industry in which they stress the importance of preventing and mitigating human rights risks "through appropriate design modification" at the earliest stages of product development.

244 *See*, for example, Brad A. Greenberg, 'Rethinking Technology Neutrality', 100 Minnesota Law Review 1495 (2016); Lance Strate, 'If It's Neutral, It's Not Technology', Educational Technology 52, no. 1 (2012), at 6-9; Ritse Erumi, 'Technology Is Not Neutral – It's Political', Ford Foundation, 3 November 2017, available at https://www.fordfoundation.org/ideas/equals-change-blog/posts/technology-is-not-neutral-it-s-political/ (visited 20 February 2020); Melissa Gregg and Jason Wilson, 'The Myth of Neutral Technology', The Atlantic, 13 January 2015, available at https://www.theatlantic.com/technology/archive/2015/01/the-myth-of-neutral-technology/384330/ (visited 20 February 2020).

However, it needs reiterating that States, as the primary duty-bearers under human rights law, bear obligations in this respect as well. This means that States must set up and effectively implement a framework that guarantees that businesses comply with the above-described responsibilities. These considerations must guide State action with respect to conduct by public authorities as well as companies within the State's jurisdiction. The mandate of the Special Rapporteur highlights that the scope of due diligence obligations extends to post-sale or post-transfer human rights impact even in case where biometric tools are used by a third country's government. While it is left up to States to decide on the most effective way to operationalize this duty, considering the particular domestic context and relevant challenges, some positive practices can be delineated in this regard.

One such practice of particular relevance is to subject high human rights risk technologies to licensing requirements, including in the context of exports. In this respect, relevant international and regional initiatives, such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies[245] (hereinafter "Wassenaar Arrangement") and Council [of the European Union] Regulation setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items[246] constitute notable examples. Although their effectiveness in practice has been limited for a number of reasons, both frameworks provide useful models and tools, with the most pertinent aspects set out below.

The Wassenaar Arrangement, bringing together 42 States, has been established with the aim "to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies," including "to prevent the acquisition of these items by terrorists."[247] A limited list of surveillance technologies have been added to the list of dual-use goods after the Arab Spring;[248] however, as the Arrangement is not a binding instrument, "practical implementation varies from country to country in accordance with national procedures."[249] The founding documents of the Wassenaar Arrangement contain no references to international law, international human rights law, or international humanitarian law norms and standards,[250] a significant shortcoming leading to a lack of human-rights-based approach to surveillance technology (or any technology covered by the Arrangement).[251] Nevertheless, some participating countries have reportedly sought limiting the transfer of such technology to States with poor human rights records, as a consequence of their participation in the Arrangement.[252]

The European Union has, for a while now, been in the process of updating the EU-wide regulation focused on control of exports, transfer, brokering, technical assistance and transit of dual-use items.[253] The 2009 Regulation has been subject to criticism by human rights stakeholders, among others, due to surveillance technologies originally falling outside of its scope.[254] These actors viewed the review process as an opportunity to strengthen the human rights protections in the European Union export regime through an expansion of categories cov-

245 *See* Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 'Founding Documents' (Public Documents. Volume I) and 'List of Dual-Use Goods and Technologies and Munitions List', (Public Documents. Volume II).

246 Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. The regulation is currently under review, with a new Commission proposal having been published in 2016.

247 For more information, *see* https://www.wassenaar.org/.

248 Certain technologies, such as mobile telecommunication interception equipment, intrusion software and Internet protocol network surveillance software have been added to the control list, in light of concerns related to some participating countries providing surveillance equipment to governments from the Middle East and North Africa region, some of which were used to crack down on protesters and opposition in the context of the Arab Spring and as such used to aid serious human rights violations, including torture, crimes against humanity and likely also war crimes. *See, e.g.*, Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies', Access Now, available at https://www.accessnow.org/cms/assets/uploads/archive/Access%20Wassenaar%20Surveillance%20Export%20Controls%202015.pdf (visited 20 February 2020).

249 For more information, *see* https://www.wassenaar.org/about-us/#faq.

250 *See* Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 'Founding Documents' (Public Documents. Volume I).

251 *See* 'Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', A/HRC/41/35, para. 34.

252 Justin Sherman and Robert Morgus, 'As Exports of Surveillance Tech Rise, Freer Countries Face a Choice', Defense One, 10 December 2018, available at https://www.defenseone.com/threats/2018/12/exports-surveillance-tech-rise-freer-countries-face-choice/153416/ (visited 20 February 2020).

253 *See* European Commission, "Proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)", 28 September 2016, 2016/0295 (COD). *See also*, Electronic Privacy Information Center, 'Submission of the Electronic Privacy Information Center to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. The Surveillance Industry and Human Rights', 13 February 2019, available at https://epic.org/privacy/intl/EPICUNSurveillanceIndustry20190213.pdf (visited 20 February 2020); Lucie Krahulcova, 'The European Parliament Is Fighting to Strengthen the Rules for Surveillance Trade', Access Now, 8 December 2017, available at https://www.accessnow.org/european-parliament-fighting-strengthen-rules-surveillance-trade/ (visited 20 February 2020).

254 As the EU list is based on the control list of the Wassenaar Arrangement as well as that of other multilateral export control regimes (such as the Nuclear Suppliers Group (NSG); the Australia Group (AG); and the Missile Technology Control Regime (MTCR)), the additions to the Wassenaar list in terms of surveillance technology also came to be reflected in the EU's dual use list.

ered and establishment of mechanisms to ensure "respect for human rights in the country of final destination."[255] The proposal put forward by the European Commission advanced the creation of an "autonomous" EU control list that would include a set of surveillance technologies not currently covered under the Wassenaar Arrangement, such as digital forensics and data retention systems.[256] Such endeavors however met with considerable push-back on part of some EU Member States as well as lobby organizations, led by concerns that tighter export controls "could seriously undermine the competitiveness of EU-based industry."[257] While there seems to be agreement among the Commission, the European Parliament, and the Council of the European Union that certain surveillance technologies should come within the scope of the EU's dual-use regulation, opinions seem to differ as to the scope of amendments to be made to the control list.[258] The mandate of the Special Rapporteur reiterates that surveillance technologies are, from a human rights point of view, high risk technologies and considers that bringing them within the remit of the Regulation would improve human rights protection.

Despite all the shortcomings outlined above, export control mechanisms can provide for powerful tools to further the responsible sale and transfer of relevant technology, including biometric tools. Such mechanisms have the potential to provide for a comprehensive framework governing all relevant transactions and thus present a clear added value to relevant restrictions implemented in the context of sanctions regimes. These mechanisms should be built on the existing frameworks outlined above and based on human rights obligations incumbent upon States and corporate responsibilities established under frameworks such as the UNGPs. In this respect, **the mandate of the Special Rapporteur makes the following recommendations:**

- **Relevant frameworks must contain binding obligations with respect to both government and business conduct (noting that this latter aspect would have to be enforced at the domestic level, through the action of government authorities).**
- **Export control frameworks must cover all tools the use of which presents a high risk to the enjoyment of human rights. Tools driven by or used to extract biometric data are to be presumed high-risk, due to the high sensitivity of such data and the far-reaching implications of its use.**
- **These frameworks must be developed through a human rights-conscious process[259] with due consideration to all human rights obligations of the State and ensuring adequate protection for all affected human rights, including the rights to privacy and data protection. The human rights-based approach must also be reflected in relevant benchmarks developed in this context.[260]**
- **The scope of certification and monitoring must cover all relevant stages, including post-sale and post-transfer.**
- **Processes set up under such frameworks must contain inbuilt safeguards that protect against abuse, including independent oversight[261] and transparency requirements covering export control decisions and relevant benchmarks used, as well as information on follow-up and monitoring processes.[262] Such trans-**

255 Coalition Against Unlawful Surveillance Exports (CAUSE), 'A Critical Opportunity: Bringing Surveillance Technologies Within the EU Dual-Use Regulation' (2015). The report advanced a series of recommendations: the EU should include cyber-surveillance tools in the dual-use list; strengthen protection of privacy, data protection, and freedom of assembly; emphasize that the exporters of high human rights risk products not listed in the regulation have to make sure that their goods don't fall into the wrong hands; increase the transparency of national authorities' export control decisions as well as baseline statistics on where the export is going; strengthen role of civil society in relation to monitoring control regimes.

256 Mark Bromley and Paul Gerharz, 'Revising the EU Dual-use Regulation: Challenges and Opportunities for the Trilogue Process', Stockholm International Peace Research Institute (SIPRI), 7 October 2019, available at https://www.sipri.org/commentary/topical-backgrounder/2019/revising-eu-dual-use-regulation-challenges-and-opportunities-trilogue-process (visited 20 February 2020).

257 Delegations of Cyprus, Czechia, Estonia, Finland, Ireland, Italy, Poland, Sweden and the United Kingdom, 'For adoption of an improved EU Export Control Regulation 428/2009 and for cyber-surveillance controls promoting human rights and international humanitarian law globally', WK 5755/2018 INIT (15 May 2018); Catherine Stupp, 'Nine Countries Unite Against EU Export Controls on Surveillance Software', EURACTIV, 8 June 2018, available at https://www.euractiv.com/section/cybersecurity/news/nine-countries-unite-against-eu-export-controls-on-surveillance-software/ (visited 20 February 2020); Reporters Without Borders, 'International Regulations: Broken or Blocked by Lobbies', 14 March 2017, available at https://rsf.org/en/reports/international-regulations-broken-or-blocked-lobbies (visited 20 February 2020); Daniel Moßbrucker, 'Surveillance Exports: How EU Member States Are Compromising New Human Rights Standards', Netzpolitik.org, 29 October 2018, available at https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/#spendenleiste (visited 20 February 2020). *See also* A/HRC/41/35, para. 19.

258 Some stakeholders have expressed unease about the EU's list going beyond those of other multilaterally agreed control regimes.

259 Such processes must be conducted in full respect for the right to participate in public affairs, as guaranteed in article 25 of the International Covenant on Civil and Political Rights. This includes consultation with relevant stakeholders, including civil society actors.

260 Participating States, as well as other exporting Governments, should deny licensing "where there is a substantial risk that those exports could be used to violate human rights, where there is no legal framework in place in a destination governing the use of a surveillance item, or where the legal framework for its use falls short of international human rights law or standards." *See* Privacy International, 'The Surveillance Industry and Human Rights. Privacy International submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (February 2019), available at https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReporttoHRC.aspx (visited 20 February 2020).

261 *See also* A/HRC/41/35, para. 49.

262 Monitoring should extend to licensing standards, decisions to authorize, modify or reject licenses, incidents or patterns of misuse of surveillance technologies and related human rights violations. In this sense *see also* A/HRC/41/35.

parency requirements also serve as a prerequisite for allowing the public and civil society to efficiently monitor the implementation of relevant frameworks.

b. Sharing of biometric data

In the context of the use of biometric tools, there are frequent examples of data-sharing between government and corporate actors. In instances of governments sharing data with corporate actors, they have the obligation to ensure that such data-sharing does not result in any unwarranted interferences with human rights. Data-sharing must pursue a legitimate public interest goal and incorporate necessary and efficient safeguards ensuring that corporations uphold the same standards that states have an obligation under human rights law to maintain. The considerations outlined above (Section C) are fully relevant in this respect.

However, a particular issue that needs addressing relates to government requests for biometric data addressed at companies. Companies must only share biometric data with governments:

- **With the informed, free, and unambiguous consent of the data subject; or**
- **To the extent such data-sharing is in the legitimate public interest and subject to a procedure set out in domestic law, with sufficient safeguards against unlawful or arbitrary use.**

However, many companies operate in environments or maintain business relationships with governments where domestic legislation and policies fall short of requirements under international human rights law. This phenomenon is distinctly noticeable in the national security context, particularly with respect to measures aimed at preventing and countering terrorism-related offences. In the following, this subsection sets out some recommended steps companies should follow when faced with State requests to share biometric data.

Compliance with domestic law

Business enterprises should ensure that they **only act upon State requests for biometric data that are made in compliance with domestic law.**[263] In particular, they should determine the existence of a substantive basis in domestic law for the particular request and that all relevant procedural requirements have been complied with. Should this not be the case, companies should refuse to comply with the request and explore available legal means to challenge it.

Companies should forego collaborating with States in a manner that may interfere with human rights of individuals on an informal basis as this removes the relevant transactions from the regular safeguards and oversight as well as remedial mechanisms established under the law.

Compliance with international human rights law

State requests received by companies should also be assessed for compliance with international human rights norms and standards to the extent such assessment is feasible. In this vein, **companies should examine the compliance of the domestic legal framework with international human rights law.**[264] This means that the legal framework in question must be must be sufficiently accessible[265] and foreseeable as to its effects.[266] The law must also provide sufficient guidance to those charged with their execution and indicate the scope of any discretion conferred on the competent authorities.[267] Finally, it must provide for sufficient and adequate safeguards against abuse[268] and must not violate the prohibition against discrimination entailed in international human rights law.[269] Having clear and detailed rules govern interference through digital technology is of particular importance especially when the technology that enables such interference is continually becoming more and more sophisticated.[270]

---

263 As relevant measures may restrict human rights, such measures must be provided by law. *See* European Court of Human Rights, *Malone v. The United Kingdom*, Application no. 8691/79, 2 August 1984, §§ 66-68.
See also, European Court of Human Rights, *Roman Zakharov v. Russia* [GC], Application no. 47143/06, 4 December 2015, § 230; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, § 35.

264 This requirement has first been voiced by the European Court of Human Rights in Sunday Times v. The United Kingdom, specifying that national law must conform to a certain standard of quality. See European Court of Human Rights, *Sunday Times v. The United Kingdom (no. 1)*, Application no. 6538/74, 26 April 1979, § 49. That mere compliance with domestic law is not sufficient for compliance with Convention standards has further been underlined in Malone v. The United Kingdom where the Court stated that lawfulness "does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law." See European Court of Human Rights, *Malone v. The United Kingdom*, Application no. 8691/79, 2 August 1984, § 67.

265 Accessibility implies that individuals that are to be affected by the respective legislation must have the possibility to become aware of its content. See European Court of Human Rights, *Groppera Radio AG and Others v. Switzerland*, Application no. 10890/84, Series A no. 173, 28 March 1990, §§ 65-68.

266 *Sunday Times v. The United Kingdom (no. 1)*, § 49. This requirement does not call for absolute foreseeability but rather that the law give individuals an "adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to interfere with their rights." *See Malone v. The United Kingdom*, §§ 66-68.

267 *Malone v. the United Kingdom*, §§ 67-68.

268 European Court of Human Rights, *Kruslin v. France*, Application no. 11801/85, 24 April 1990, §§ 33 and 35; and European Court of Human Rights, *Huvig v. France*, Application no. 11105/84, 24 April 1990, §§ 32 and 34. *See also Zakharov v Russia*, § 269.

269 Human Rights Committee, General Comment no. 34, CCPR/C/GC/34, para. 26.

270 In the cases of Kruslin v. France and Huvig v. France, the European Court of Human Rights emphasized the need for clear, detailed rules, especially as the technology available for use was continually becoming more sophisticated.

Evaluating the human rights compliance of State requests may, however, pose serious challenges to companies. Such requests are rarely accompanied with sufficient information that would make it possible to meaningfully assess whether a State measure would be in line with international human rights law.

If, on the basis of the information available to the company and the assessment conducted, the company has reason to believe that the request may not be in full compliance with international human rights law, it should seek clarifications from the government with regard to the aspects of concern. If necessary, clarification on the scope of the request should be sought, in particular regarding the legal basis of the order and the way in which the law has been applied to the case at hand.

In case the government's replies do not settle the doubts expressed, **the company should use available legal means at its disposal to challenge the request**, wherever feasible. In case judicial or other independent review is not available, companies must make sure they use their leverage to influence the outcome in the particular case as well as advocate for change in the legal framework and policy that would guarantee improved respect for human rights. Companies should use such leverage with the government involved as well as with other stakeholders that could influence government conduct and policies, such as international organizations or, in case of companies operating abroad, the diplomatic representation of their own government.

In situations in which the company "lacks the leverage to prevent or mitigate adverse impacts and is unable to increase its leverage," **it should give due consideration to ending the business relationship**.[271] In this sense the business must consider the severity of the adverse human rights impact that it contributes to through its activities.[272] In case it decides to continue its business relationship, it must demonstrate continuous engagement with the authorities and other relevant stakeholders aimed at mitigating negative human rights effects. Moreover, in such situations the business should be prepared to accept financial, legal or reputational consequences linked to its continued operations in this context and its connections to human rights violations and abuses.[273]

Recommendations:

- **Companies should forego informal collaboration with States that may interfere with human rights of individuals, as this removes the relevant transactions from the regular safeguards and oversight as well as remedial mechanisms established under the law.**
- **Should companies have doubts about the human rights compliance of State requests for biometrics data, they must use any legal avenues at their disposal to avoid contributing to State practices that run afoul of human rights protections.**
- **In this regard, business enterprises should keep in mind that corporate responsibility under the UNGPs is independent of State obligations and as such "exists over and above compliance with national laws" and irrespective of States' abilities and/or willingness to fulfil their own duties under human rights law.**

c. Furthering rights compliance through interest groups and public-private partnerships

In certain areas, efforts aimed at improving international law and human rights compliance of corporate conduct, including in the context of state-business cooperation, have been strengthened and supported through the formation of interest groups and implementation of public-private partnerships.

For example, with respect to addressing challenges posed by the activities of private security and military companies, the Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict[274] (hereinafter "Montreux Docu-

271 See UNGPs, Principle 19.
In accordance with the Interpretive Guide, ending the relationship may be particularly challenging in case it can be qualified as "crucial" relationship for the company. In order for a relationship to qualify as "crucial," it must provide "a product or service that *is essential to the enterprise's business, and for which no reasonable alternative source exists'. See The Corporate Responsibility to Respect Human Rights. An Interpretive Guide*, p. 22.

272 *Ibid.* The Interpretive Guide warns that "the more severe the abuse, the more quickly the enterprise will need to see change before it takes a decision on whether it should end the relationship."

273 *Ibid.*

274 Swiss Federal Department of Foreign Affairs/FDFA and International Committee of the Red Cross, *Montreux Document on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict* (Montreux, 17 September 2008), available at https://www.icrc.org/en/doc/assets/files/other/icrc_002_0996.pdf (visited 20 February 2020).

ment") has been developed as a result of a joint initiative by the Swiss government and the ICRC. Almost twelve years after its adoption, there are currently 56 States supporting the Document.[275] As non-State actors such as companies cannot join the Montreux Document, a non-binding International Code of Conduct for Private Security Service Providers[276] has been developed aimed at articulating human rights responsibilities of companies active in the space. The implementation of the Code is facilitated and overseen by the multi-stakeholder International Code of Conduct Association (ICOCA).[277] A comparable initiative would have the potential to considerably boost international law and human rights compliant approaches to the development and use of biometric tools and data.[278]

275 Swiss Federal Department of Foreign Affairs/FDFA, 'Participating States of the Montreux Document', available at https://www.eda.admin.ch/eda/en/home/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies/participating-states.html (visited 20 February 2020).
276 *The International Code of Conduct for Private Security Service Providers*, available at https://www.icoca.ch/en/the_icoc (visited 20 February 2020).
277 For information on the International Code of Conduct Association, see https://icoca.ch/en/association (visited 20 February 2020).
278 Other notable initiatives of relevance include the Global Network Initiative (https://globalnetworkinitiative.org), Tech Against Terrorism (https://globalnetworkinitiative.org) and the Global Internet Forum to Counter Terrorism (https://gifct.org). Furthermore, Ranking Digital Rights produces a Corporate Accountability Index that evaluates the publicly disclosed policies and practices of major tech companies for effects on users' freedom of expression and privacy. See https://rankingdigitalrights.org.

Conclusions and recommendations

Biometric tools are becoming ubiquitous. They are employed by a multitude of stakeholders, both public authorities and private actors, corporations and individuals. They are used in law enforcement, criminal justice, smart city initiatives, in identification and registration systems aimed at preventing identity fraud and theft, or to authenticate beneficiaries of humanitarian aid. Biometric tools come with great potential to contribute towards positive change in many societal areas. However, their use may also lead to abuses and violations of human rights and have at times become weapons in the hands of authoritarian or oppressive governments enabling gross infringements on human rights.

As such, biometric tools and data can constitute a powerful instrument in the prevention and countering of terrorism and violent extremism by facilitating efficient and targeted responses to threats. This is also reflected in the regulatory efforts by the United Nations Security Council with its resolution 2396 requiring that States "develop and implement systems to collect biometric data" in order to "responsibly and properly identify terrorists, including foreign terrorist fighters" and to do so "in compliance with domestic and international law, including human rights law."

Indeed, compliance with internationally recognized human rights norms is an essential precondition for effective and sustainable counter-terrorism action. However, the Security Council resolution and relevant subsequent technical guidance do not develop on ways in which such obligations can be implemented in a manner that safeguards human rights. Given the universally binding nature of the Security Council's resolution, requiring all 193 UN Member States to implement biometric data systems, many of which do not have adequate privacy and data protection frameworks set up under domestic law, the need for detailed and granular human rights guidance is evident.

It is against this background, that this report embarked upon identifying the salient human rights gaps in connection to the use of biometric tools and data, with particular focus on the prevention and countering of terrorism and violent extremism.

In outlining the human rights implications linked to the use of biometric tools and technology, the report highlights ways in which the use of biometrics affect the right to privacy and data protection, but also stresses that pertinent ramifications point beyond, engaging a broad range of civil, political, economic, social, and cultural rights. Efficiently tackling the rights impact of biometrics requires that relevant stakeholders adopt a comprehensive approach that considers the indivisible and interdependent character of all human rights.

In the view of the mandate of the Special Rapporteur, the existing international human rights framework governing State obligations regarding collection, retention, processing and sharing of biometric data, as set out in the report, offers an adequate structure to ensure that human rights are duly safeguarded. However, implementation on part of duty-bearers is often inadequate, patchy,

and insufficiently resourced. Common shortcomings include the lack of comprehensive human rights impact assessments as well as meaningful monitoring and evaluation of ways in which human rights are affected by relevant laws, policies, and practices, and, in particular, the lack of effective independent oversight.

An important protection gap highlighted by the report relates to the role of business enterprises in developing, deploying, selling, and transferring biometric tools. Businesses are not formally bound by international human rights law and States commonly fall short of setting up and implementing necessary frameworks to duly ensure corporate accountability. To address that shortcoming, the Special Rapporteur's mandate recommends that both State and business stakeholders re-evaluate the ways in which they tackle the development and deployment of biometric tools by adopting a human rights-based approach to all phases of development and use, including in relation to sales, transfers, and post-transfer monitoring and maintenance.

The report further explores areas where legal and policy development is needed or compliance with international human rights norms needs strengthening in order to ensure that ways in which biometric tools and data are developed and used reinforce human rights protections and the rule of law as opposed to undermining these fundamental values.

In this respect, the mandate of the Special Rapporteur advances the following recommendations:

States

- States must set up a comprehensive domestic legal framework that enables them to tackle the challenges and opportunities presented by the use of biometric tools and data in line with international human rights norms and standards. This also includes the development and effective implementation of adequate privacy and data protection safeguards.
- States must take necessary and adequate steps to bridge the gap between technological developments on the one hand and legal and policy responses on the other. This requires a future-proof approach to legislation and policy, ensuring that such frameworks meet the challenges brought by innovation, among others through incorporating human rights principles and safeguards. Human rights-sensitive regulatory impact assessments can meaningfully contribute towards such future-proofing efforts.
- Considering the high risk associated with the use of biometric tools, due to the sensitive character of biometric data and the potential for exploitation and abuse, States must conduct comprehensive human rights risk assessments. Such risk assessments must examine implications on the right to privacy of data subjects and incidental effects on third parties, and tackle compliance with recognized data protection principles. Risk assessments also must fully consider the broader human rights impact in light of the universal, indivisible, interdependent, and interrelated nature of all human rights.
- Any measures that interfere with human rights must be in line with conditions established under human rights law. Restrictions on rights must be provided by law and necessary to protect a legitimate aim (such as national security, public order, or the rights and freedoms of others). Any measures must also be governed by the principles of proportionality and non-discrimination and respect the need for consistency with other guaranteed human rights.
- States should only resort to derogations from their human rights obligations when the legitimate public interest pursued cannot be met through restrictions on limitable rights within the scope of the ordinary law of the State. Derogations should be strictly aimed at restoring a state of normalcy and thus limited in material scope and duration. Relevant measures must comply with the principle of proportionality and be consistent with the State's other obligations under international law.
- The use of biometric tools employed to address the threats and challenges posed by the COVID-19 pandemic should be subject to rigorous and independent monitoring and evaluation. States should further ensure that such tools are not unreflectively expanded to counter-terrorism, security, and other public policy spheres.
- When States collect, retain, process, and share biometric data, conditions governing restrictions of human rights must be met at every stage of data usage.
- States should 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 achieving a legitimate aim. Such considerations are particularly relevant when States choose to implement integrated and/ or centralized systems.

- States must take necessary and adequate measures to safeguard the security of biometric systems and databases.
- States must ensure that recognized data protection principles including the principles of lawfulness, fairness and transparency in collection and processing; purpose limitation; data minimization; accuracy; storage limitation; security of data; and accountability for data handling are complied with even when such data is gathered and processed in a national security or law enforcement context.
- A human-rights-minded approach should govern State conduct in relation to all phases of development and deployment of biometric tools. This includes integrating "human rights by design" in the development of relevant technology from the earliest stages.
- When sharing biometric data with State or other stakeholders across borders, States must ensure that such actions are governed by a sufficiently accessible and foreseeable domestic legal basis that provides adequate human rights safeguards against abuse. Data-sharing practices must be driven by the principle of accountability and subject to comprehensive independent oversight.
- States must ensure that relevant oversight bodies are duly mandated to review the compatibility of data-sharing agreements with domestic and international law. Furthermore, States must find solutions to guarantee that such bodies have the power to seek or verify information about the means and methods of collection, retention, and processing of information, including when such information has been acquired from another State.
- States should set up and implement authorization and licensing systems governing technology presenting a high human rights risk. Biometric tools are to be presumed high-risk due to the high sensitivity of such data and the far-reaching implications of its use. Such systems should cover development, sales, and transfer of high-risk technology, including for export purposes.
- Building on existing frameworks, such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, States should work towards establishing comprehensive export control systems with strong inbuilt human rights safeguards, governed by the principles of accountability and transparency.
- States must ensure that non-State actors, including business enterprises, comply with due diligence requirements, as set out in the "respect, protect, remedy" framework set up by the United Nations Guiding Principles on Business and Human Rights.
- States should only use biometric tools that have undergone a comprehensive human rights risk assessment and found human rights compliant. In case of technology that falls short of these standards, States must implement moratoria on their use until the tool can be brought in line with international human rights norms and standards.
- In the context of United Nations efforts aimed at capacity-building support and technical assistance to Member States with a view of facilitating the full implementation of Security Council resolution 2396, Member States should promote the meaningful participation of United Nations human rights entities, including the Office of the High Commissioner for Human Rights and the mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Meaningful participation would require that these entities are resourced commensurately with their role in the United Nations counter-terrorism architecture.

Business enterprises

- Business enterprises must ensure that their operations are guided by international human rights law, including the "respect, protect, remedy" framework set up under the United Nations Guiding Principles on Business and Human Rights.
- Businesses should adopt an explicit and public policy commitment to meet their responsibility to respect human rights. This commitment should be reflected in operational policies and procedures governing the business's activities.

- Business enterprises must conduct human rights due diligence. This includes conducting risk assessments examining actual and potential human rights impacts, both direct and indirect, of the business's operations. Risk assessments must encompass all phases and aspects of the business's operations and monitor how the nature and scope of the risks may change over time. In relation to biometric tools, due diligence responsibilities cover all phases of technology development and deployment, including in relation to sales or transfers of the product as well as after-sales support and maintenance.
- Companies should set up internal accountability mechanisms for the implementation of human rights policies and have processes in place that enable the remediation of adverse human rights impacts that the company caused or contributed to. Companies should externally communicate the ways in which they address human rights impacts linked to their operations. In particular, companies should report on their business relationships with governments and public authorities, both in relation to sales and transfer of biometric technology as well as any relevant data-sharing arrangements.
- Companies should adopt a human-rights-minded approach towards development and deployment of biometric tools. This includes integrating "human rights by design" in the development of relevant technology from the earliest stages.
- Companies must take necessary steps towards ensuring that their data-sharing practices do not infringe on internationally recognized human rights. In case such data is requested by a State, companies should ensure that they only act upon State requests that are made in compliance with domestic law. Companies should forego informal collaboration with States in ways that may interfere with human rights of individuals as this removes the relevant transactions from regular legal safeguards and oversight as well as remedial mechanisms. Should they have doubts about the human rights compliance of requests, companies must use legal avenues at their disposal to avoid contributing to State practices that run afoul of human rights protections.
- Business enterprises should keep in mind that corporate responsibility under the United Nations Guiding Principles on Business and Human Rights is independent of State obligations and as such "exists over and above compliance with national laws" and irrespective of States' abilities and/or willingness to fulfil their own duties under human rights law.

United Nations entities and the global counter-terrorism architecture

- Ensure that international law, including international human rights law, international humanitarian law, and refugee law norms and standards are duly incorporated in technical assistance and capacity-building activities, at all relevant stages.
- Support the development of detailed United Nations-wide human rights guidance on the development and deployment of biometric tools and the collection, retention, processing, and sharing of biometric data.
- Facilitate the establishment of an international framework to govern the transfer, sale, and export of biometric technology while ensuring that such framework duly incorporates relevant international law, including human rights law safeguards, and is transparent and accountable.
- Support human-rights-based law and policy-making at the international, regional, and domestic level by ensuring that any efforts aimed at supporting States in the implementation of international obligations include comprehensive human rights mainstreaming.
- Step up efforts aimed at the consolidation and strengthening of the 4th Pillar of the Global Counter-Terrorism Strategy.