HUMAN RIGHTS CENTER
UNIVERSITY OF MINNESOTA

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

Summary of findings and recommendations

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

Knowledge Management Fund | Knowledge Platform Security & Rule of Law

The report is available at: z.umn.edu/HRC-BiometricDataReport

Background

Biometric tools are increasingly 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. While biometric tools come with great potential to contribute towards positive change in many societal areas, their use may also lead to abuses and violations of human rights. At times, such tools have become weapons in the hands of authoritarian or oppressive governments enabling gross infringements on human rights.

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 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."

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 substantively address the ways in which these 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 under domestic law, the need for detailed and granular human rights guidance is overwhelming.

AIM:

Identifying the human rights gaps in the use of biometric tools and data, with particular focus on the prevention and countering of terrorism and violent extremism.

Main findings:

- The use of biometric tools and data affect a broad range of civil, political, economic, social, and cultural rights.
- Focus on the impact of biometrics on the right to privacy and data protection is necessary but insufficient to identify the overall effect on human 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.

- The existing international human rights framework governing state obligations regarding collection, retention, processing and sharing of biometric data offers adequate protections. However, implementation on the part of duty-bearers is often patchy and inadequate.
- There is an identifiable protection gap relating 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 this shortcoming, both State and business stakeholders must reevaluate 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.

Common human rights shortcomings include the lack of comprehensive human rights impact assessments, 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.

NEXT STEPS:

Strengthen compliance with international human rights obligations, including through legal and policy developments, 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.

How:

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 must also 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.

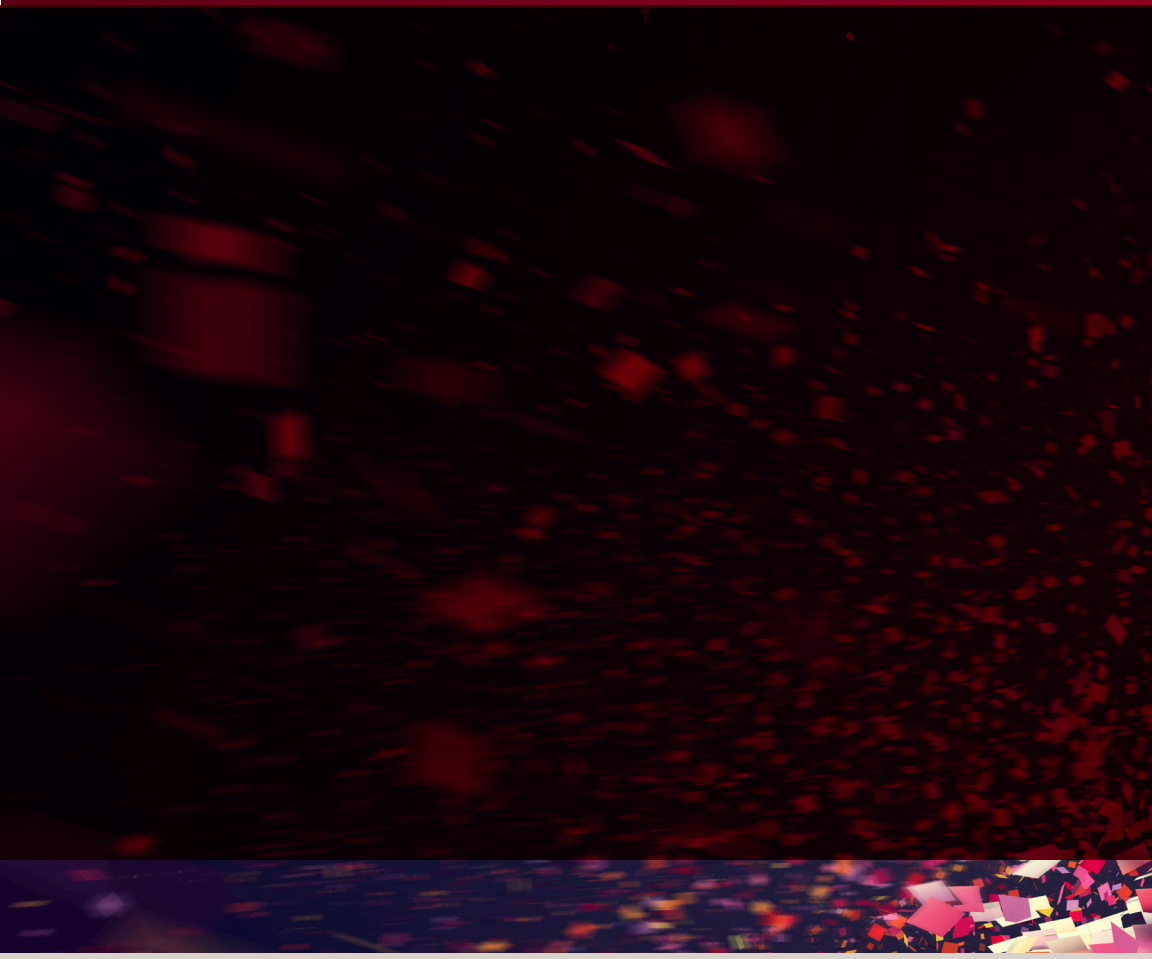
- A human-rights-minded approach should govern State conduct in relation to all phases of development and deployment of biometric tools. This includes integrating "human rights by design" in the development of relevant technology from the earliest stages.
- When sharing biometric data with State or other 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.



HUMAN RIGHTS CENTER

UNIVERSITY OF MINNESOTA