QUNO
Quaker United Nations Office

September 2020

The collection and use of biometric data in the context of children of parents suspected, accused or convicted of association with designated terrorist groups: a child rights-based briefing note for Civil Society, States and UN entities

Lucy Halton

Human Rights and Refugees

For over 15 years, QUNO has worked to draw attention to the impact on children of parental incarceration and clarify the existing human rights protection in international law.

This paper is a supplement to QUNO's Briefing Paper: Key Human Rights Considerations for Children of Parents Suspected, Accused or Convicted of Association with Designated Terrorist Groups, which is available here.

For more info, contact:

ltownhead@quno.ch

Context

There is growing international concern regarding the many children associated with designated terrorist organisations, one specific group of whom are children of parents suspected, accused or convicted of association with a designated terrorist group. Upholding the rights of these children is both a legal requirement and a moral imperative, yet they remain exposed to numerous, systemic violations of their rights.[1]

The use of biometric data[2], which raises a range of general human rights concerns, is an area of particular concern in relation to these children and raises a number of specific rights issues.[3] While the collection and use of biometric data can, in some circumstances, be in the best interests of a child, including when it facilitates family reunification, it must in all circumstances be subject to strict, thorough, child rights-based safeguards.

This briefing note provides a short overview of the key considerations for the rights of these children, and is intended for use by civil society, States, and UN entities working on the use of biometrics in countering terrorism, including in the implementation of UN Security Council resolution 2396. This information may be useful for those working directly with affected children, as well as to enhance advocacy strategies on topics including the use of biometrics in countering terrorism, and the rights of children associated with terrorist groups.

1 The Convention on the Rights of the Child does not allow for derogation in times of conflict or emergency, and only three of the substantive rights it includes may be restricted in the interests of national security (Article 10.2 on the child's right to leave any country and to enter their own country for the purposes of maintaining contact with their parents, Article 13 on the child's right to freedom of expression, and Article 15 on the child's right to freedom of association and peaceful assembly).

2 'Biometric data is defined as "unique markers that identify or verify the identity of people using intrinsic physical or behavioral characteristics", and has been noted to include DNA.' [United Nations Counter-Terrorism Centre, *Handbook on Children Affected by the Foreign Fighter Phenomenon* (2019), footnote 193].

3 For a broader analysis of the human rights implications of the use of biometric data in the context of counter-terrorism, see Privacy International, 'Responsible use and sharing of biometric data in counter-terrorism', (July 2020).

Key considerations:

The biometric data of children whose parents are suspected, accused or convicted of association with designated terrorist groups is typically collected in the form of DNA or iris scans for the purpose of identifying the child's parentage and therefore determining eligibility for nationality where there is doubt.[4] This practice raises several rights concerns, notably because it opens up the potential for harms which cannot be fixed or adjusted.[5]

The use of DNA testing of children of parents suspected, accused or convicted of association with designated terrorist groups **should only ever be an exceptional measure**, given how highly invasive it is, its rights implications, its inaccuracies, the risks of security breaches, and how little is known about its long-term consequences.[6]

First and foremost, the collection, retention, processing and sharing of the biometric data of all children, including this group, must comply with the provisions of the Convention on the Rights of the Child. The 2018 Addendum to the 2015 Madrid Guiding Principles specifically requires that States,

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).[7]

In particular, this means that the **best interests** of the child must be taken as a primary consideration in all decisions which affect them.[8] If the collection or use of a child's biometric data is not in their best interests, it should not be implemented. The best interests of the child must be established on a case-by-case basis: in the context of the use of biometric data of children of parents suspected, accused or convicted of association with designated terrorist groups, blanket policy approaches are therefore in contravention of the Convention on the Rights of the Child.

The collection and use of the biometric data of these children raises clear **privacy** concerns. The protection of the right to privacy under Article 16 of the Convention on the Rights of the Child affords all children a strong protection of their right to privacy, and any interference with this right must comply with the principles of **legality, necessity, and proportionality**. While for adults, an assessment of the legality, necessity and proportionality of an interference with the right to privacy may rely on a threat level assessment, in the case of children it should primarily constitute an assessment to establish whether the breach of that specific child's right to privacy is, in this circumstance, in their best interests. The least intrusive measure should always be taken to achieve a legitimate aim: this means using DNA testing or other biometric data collection as a measure of last resort in the identification of these children and their family ties.

All considerations, including best interests assessments and establishing whether a breach of the child's right to privacy is legal, necessary and proportionate, must include consideration of the reduced stability of children's biometric markers, given that children are still developing.[9]

The uniqueness[10] and permanence of biometrics, which in some ways make them so useful, also make their processing and storage particularly concerning:[11] once stored, individuals – in this case children – are not the sole possessor

4 United Nations Counter-Terrorism Centre, *Handbook on Children Affected by the Foreign Fighter Phenomenon* (2019), para 99. See also Louisa Loveluck, 'In Syrian camp for women and children who left ISIS caliphate, a struggle even to register names' (Washington Post, June 28 2020); Stewart Bell, 'Canadians at camp for ISIS families fingerprinted, questioned as part of drive to support repatriation' (Global News, 15 June 2020).

5 UNICEF, 'Faces, Fingerprints and Feet: *Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes'* (July 2019), page 16.

6 United Nations Counter-Terrorism Centre, *Handbook on Children Affected by the Foreign Fighter Phenomenon* (2019), para 99.

7 Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council , 2018 Addendum to the 2015 Madrid Guiding Principles (S/2018/1177).

8 Dr. Krisztina Huszti-Orbán and Prof. Fionnuala Ní Aoláin, '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], (July 2019), page 22.

9 UNICEF, 'Faces, Fingerprints and Feet: *Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes'* (July 2019), page 19.

10 Biometric data is a special, sensitive category within data protection law, such as the European Union's General Data Protection Regulation (under Article 9).

11 Privacy International, 'Responsible use and sharing of biometric data in counter-terrorism', (July 2020); UN High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age', A/HRC/39/29 (August 2018) para. 14.

of their biometric data, and when biometric data is lost, abused or misused the consequences can be far greater.[12] In the context of the collection and use of children's biometric data, all such processes much be strictly regulated by a rights-based legal framework, and thorough proportionality assessments must be in place. The storage and use of the data collected is a matter of key concern. States which collect the biometric data of these children in the form of DNA must not retain that information for any other use, including the development of biometric databases.[13] The development of these databases does not, on its own, constitute a legitimate aim.[14] Robust regulation, higher standards and additional safeguards are necessary to protect the rights of children, because children's biometric data requires special protection both because it is children's data, and because it is biometric data. Regulations should ensure that data is deleted after a certain period of time, and access to children's data, along with the sharing of that data, must be strictly regulated.

It is well attested that errors in some biometric systems are much more common among children: iris scanning, for example, is extremely inaccurate in young children.[15] In the case of children of parents suspected, accused or convicted of association with designated terrorist groups, this fact is often compounded by the inherent racial biases of certain technologies.[16] Too often, DNA testing processes to determine a child's identity or parentage rely on historical gene pools in a given area, making them highly prone to inaccuracies and racial biases.

The use of biometric data, particularly DNA, in the case of these children is further unreliable as it will not confirm a genetic link if a child was adopted or in situations where the child's biological parents were different from those who raised them.[17] This presents a significant possibility for children to be deprived of their right to family life, particularly in cases involving very young children who were unaware of their biological relationship to their parent(s). Additionally, the absolute reliance on DNA, and narrow definition of family on this basis, risks discriminatory practice by failing to take into account different cultural conceptions of familial connections.[18]

Article 2 of the Convention on the Rights of the Child protects children from **discrimination**, in law or in practice, including on the basis of the status or activities of their parent(s).[19] This protection applies when States are considering collecting or using the biometric data of children of parents suspected, accused or convicted of association with designated terrorist groups. This means that States or other actors must not retain the data of a child whose parent is suspected, accused or convicted of association with a designated terrorist group for the purpose other than that for which is was obtained if the same would not be done for all children. The only exception to this principle is in circumstances in which individualised assessment of that child demonstrates that doing so is in the best interests of the child, or provides other sufficient reason to do so.

The inclusion of these children in watchlists must not be a blanket policy. Where children are included on watchlists, their inclusion must be **reviewed periodically**. To ensure full compliance with the rights of these children, data should be automatically **destroyed** after a certain period of time, and only retained if deemed absolutely necessary. A child's right to privacy must not be infringed upon solely on the basis of the acts or alleged acts of their parents. The collection of this data must only be undertaken when strictly necessary, as a measure of last resort, and when in the best interests of the child.

There are no recommendations of good practices on the use and sharing of biometrics in relation to any affected group of children in the 2018 'United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism'. Further work is needed in this area given the significant numbers of children and human rights impacts in question.

There are also serious concerns about children and families' ability to **consent** to the collection of biometric data, heightened by the uncertainty and trauma that children whose parents are suspected, accused or convicted of association with designated terrorist groups often encounter.

12 UNICEF, 'Faces, Fingerprints and Feet: *Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes'* (July 2019) page 17; Privacy International, 'Responsible use and sharing of biometric data in counter-terrorism', (July 2020).
13 United Nations Counter-Terrorism Centre, *Handbook on Children Affected by the Foreign Fighter Phenomenon* (2019), para 99.
14 Privacy International, 'Responsible use and sharing of biometric data in counter-terrorism', (July 2020), page 10.
15 Ibid, page 19.
16 Ibid, page 16.
17 United Nations Counter-Terrorism Centre, *Handbook on Children Affected by the Foreign Fighter Phenomenon* (2019), para 99.
18 United Nations Counter-Terrorism Centre, *Handbook on Children Affected by the Foreign Fighter Phenomenon* (2019), para 99.
19 UN Convention on the Rights of the Child (1989), Article 2.

Children, especially those in this situation, often lack the knowledge or agency to be able to consent to the collection and storage of their biometric data. Furthermore, it is almost impossible for children, or their parents or guardians, to predict how technology may develop in the course of the child's lifetime and the range of possible uses for the data collected. This is often compounded by the unequal power balances between humanitarian actors, State authorities, and military actors all of whom may come into contact with, and seek to collect data from, these children.[20]

20 UNICEF, 'Faces, Fingerprints and Feet: *Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes'* (July 2019), page 17.

Recommendations:

When deciding whether to allow a child whose parents are suspected, accused or convicted of association with designated terrorist groups the right to re-enter a State, or grant them nationality, **States should only use biometric data collection in the form of DNA testing of the children of parents suspected, accused or convicted of association with designated terrorist groups as measure of last resort**. States should consider the full range of information available to them in establishing familial links.[21]

All collection, retention, processing and sharing of the biometric data of children, including the children of parents who are suspected, accused or convicted of association with designated terrorist groups, must be subject to strict periodic review by a child rights expert, such as an ombudsperson or children's commissioner.[22]

National use of biometric data must be prescribed in specific law, and not assumed to be covered by general data protection legislation: such legislation must be publicly available and explicitly include child rights considerations.[23]

The UN Counter-Terrorism Executive Directorate should develop, in cooperation with the mandate of the UN Special Rapporteur on counter-terrorism and human rights, human rights guidelines on the requirement of Security Council resolution 2369 that states develop and implement systems to collect biometric data.[24] These guidelines must incorporate all relevant child rights considerations.

All national implementation of Security Council resolution 2396 should also be subject to review by a child rights expert. A central element of this is that the data of children of parents suspected, accused or convicted or association with designated terrorist groups should not be included in centralised biometric databases or Advanced Passenger Information (API) systems.

The dissemination of the 2018 'United Nations Compendium of recommended practices or the responsible use and sharing of biometrics in counter-terrorism' should be undertaken with an informed awareness of the child rights implications of the recommendations it contains. Any review or updating of the Compendium should be done in consultation with a range of relevant human rights experts, including a child rights specialist, and supplementary information should be published with good practice examples relating to this particular group of children.

21 United Nations Counter-Terrorism Centre, *Handbook on Children Affected by the Foreign Fighter Phenomenon* (2019), para 99, and recommendation 'g' p. 49.

22 Dr. Krisztina Huszti-Orbán and Prof. Fionnuala Ní Aoláin, '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], (July 2019), page 22.

23 Privacy International, 'Responsible use and sharing of biometric data in counter-terrorism', (July 2020), page 8.

24 Privacy International, 'Responsible use and sharing of biometric data in counter-terrorism', (July 2020), page 24.