

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

I write in my capacity as the United Nations (UN) Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to Human Rights Council resolution 31/3, in response to the [Call for inputs](#) published by the Office of the United Nations High Commissioner for Human Rights (OHCHR).

The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism is an independent expert appointed by the UN Human Rights Council. As per my mandate, I have been invited to gather, request, receive and exchange information on alleged violations of human rights and fundamental freedoms while countering and preventing terrorism and violent extremism, and to report regularly and publicly to the Human Rights Council and General Assembly about *inter alia* identified good policies and practices, as well as existing and emerging challenges and present recommendations on ways and means to overcome them.

The Special Rapporteur welcomes OHCHR's work aimed at "identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business enterprises in this regard", pursuant to Human Rights Council resolution 34/7 adopted on 23 March 2017 and appreciates the opportunity to contribute to the upcoming report.

The present submission focuses on information-sharing in the framework of preventing and countering terrorism and the concerns such measures present in relation to the protection and promotion of human rights, with particular focus on the right to privacy. It outlines common shortcomings relating to the legality and oversight of cross-border data-sharing, particularly in an intelligence cooperation context and highlights the human rights risks posed by the over-expanding scope of related Security Council-mandated information-sharing measures, whether in the form of soft law or binding obligations. In light of the absence in protective parity of privacy frameworks in different jurisdictions, it draws attention to the risk that intelligence-sharing measures advocated by the Security Council contribute to greater privacy intrusions, which in turn lead to enhanced risk to the protection of a broad range of rights. In this vein, it recommends that relevant measures be interpreted and implemented in line with international human rights obligations, including good practices identified by the Special Rapporteur's mandate.

The promotion and protection of human rights in the context of the challenges posed by terrorism is at the heart of the mandate of the Special Rapporteur. Terrorism poses a serious challenge to very tenets of the rule of law, the protection of human rights and their effective

implementation. Effectively combatting terrorism and ensuring respect for human rights are not competing but complementary and mutually reinforcing goals, as also recognized by the UN General Assembly in the Global Counter-Terrorism Strategy.¹ Moreover, relevant provisions of Security Council resolutions 1373 (2001), 1456 (2003), 1566 (2004), 1624 (2005), 2178 (2014), 2341 (2017), 2354 (2017), 2368 (2017), 2370 (2017), 2395 (2017) and 2396 (2017); as well as Human Rights Council resolution 35/34 and General Assembly resolutions 49/60, 51/210, 72/123 and 72/180 require that any measures taken to combat terrorism and violent extremism, including incitement of and support for terrorist acts, comply with States' obligations under international law, in particular international human rights law, refugee law, and international humanitarian law.

In recent years, the General Assembly and the Security Council, together with a number of governments, have called for enhanced cooperation between the public and private sectors, especially with information and communications technology (ICT) companies to aid efforts to counter terrorism and violent extremism, "while respecting human rights and fundamental freedoms and complying with international law and the purposes and principles of the Charter."²

The expanding reliance by States on the private sector to conduct and facilitate digital surveillance is well-established.³ As observed by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the capacity of States to conduct surveillance may even "depend on the extent to which business enterprises cooperate with or resist such surveillance".⁴ In many jurisdictions, companies that provide access to online services are under statutory obligation to facilitate access by State authorities to their networks as well as to communications and content data generated by users. Such companies are frequently subject to data retention laws. They also face requests from judicial or law enforcement authorities to hand over information, including about persons not physically within the requesting State's jurisdiction as well as information held on servers abroad. In such cases, companies, in particular those operating in more than one jurisdiction, may need to accommodate diverging obligations under different legal systems that may not be easy or even possible to reconcile.

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 2011,⁵ they are not formally legally binding. They represent however an important step towards matching the impact of businesses on human rights with corresponding levels of corporate responsibility. Moreover, they denote the direction of legal obligations, as soft law norms that may crystalize to hard law obligation over time and use.

The General Assembly has already 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

¹ A/HRC/60/288.

² See, for example A/RES/72/284 and S/RES/2396 (2017).

³ A/HRC/27/37, para. 3ff.

⁴ A/HRC/32/38, para. 57.

⁵ A/HRC/17/4.

abuse human rights, in particular the right to privacy”.⁶ The increased use of the Internet and ICTs, together with related technological developments have made interferences with the right to privacy both less noticeable to society and the individual subjects affected by them and, at the same time, more intrusive, with potentially far-reaching consequences that frequently include implications beyond the right to privacy.

Both the General Assembly and the Human Rights Council have, in this respect, 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.⁷ The effects of violations or abuses of the right to privacy may however point even further, and have adverse impact on the whole range of human rights, including the rights to life, to liberty and security of person, to health, to work, to social security, etc. The Special Rapporteur stresses in this regard that any responses must duly consider the universal, indivisible, interdependent and interrelated nature of all human rights.

In her 2014 report, then-High Commissioner Navi Pillay has highlighted that while the international legal framework provided for clear and sufficient protective standards for the right to privacy, the practice of many States revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards and ineffective oversight, all of which had contributed to a lack of accountability for arbitrary or unlawful interference with the right to privacy.⁸ These shortcomings are markedly noticeable in the context of countering terrorism and violent extremism, resulting in the right to privacy being one of the human rights most at risk to be unduly affected by such measures. Risks of abuse are particularly high in relation to measures involving the sharing of information, including information that contains or may disclose personal or sensitive data, and in particular when such information-sharing has a trans-border character.

Efforts to counter terrorism are evolving to encompassing broader transnational dimensions as terrorism-related incidents frequently comprise trans-border elements, either due to the involvement of terrorist entities whose activities are not restricted to the territory of one state, so-called ‘lone wolf’ perpetrators inspired by the methods of terrorist groups active abroad or simply due to the need for intelligence or judicial evidence located in another jurisdiction.

Against this background, Security Council resolutions have emphasized the need for international cooperation in information-sharing, both for the purposes of collecting intelligence and judicial assistance. As the High-level Conference of Heads of Counter-Terrorism Agencies of Member States (June 2018) illustrated, inter-institutional collaboration is also a priority for States.

The Council has underscored the importance of judicial cooperation in resolution 1373 (2001), requiring Member States to provide assistance “in connection with criminal investigations or proceedings” relating to the prosecution of terrorist acts⁹ and has in recent years emphasized that such obligation extended to assistance with respect to investigations or proceedings involving foreign terrorist fighters.¹⁰ It further highlighted the significance of cooperation with

⁶ A/RES/68/167; A/RES/69/166; A/RES/71/199.

⁷ A/RES/71/199; A/HRC/RES/34/7.

⁸ A/HRC/27/37, para. 47.

⁹ S/RES/1373 (2001), para. 2(f).

¹⁰ S/RES/2178 (2014), para. 12; S/RES/2322 (2016), paras. 8-9; S/RES/2396 (2017), para. 23.

respect to gathering “digital data and evidence from the Internet”¹¹ and the “importance of considering the re-evaluation of methods and best practices (...) related to investigative techniques and electronic evidence.”¹² In this respect, the Council also called for enhancing the effectiveness of mutual legal assistance agreements in criminal matters related to counterterrorism and “in the absence of applicable conventions or provisions, to cooperate when possible on the basis of reciprocity or on a case by case basis”.¹³

Moreover, the Council has repeatedly emphasized the need for States to ensure that domestic law enforcement, intelligence, counterterrorism, special services agencies and military entities¹⁴ have access to information necessary for the purpose of identifying and determining the risk posed by foreign terrorist fighters¹⁵, and other individual terrorists and terrorist organizations,¹⁶ and to intensify and accelerate the exchange of operational information regarding actions or movements of terrorists or terrorist networks “to prevent them from planning, directing, conducting, or recruiting for or inspiring others to commit terrorist attacks, and from exploiting technology, communications and resources to support terrorist acts”.¹⁷ The obligation to share information covers not only persons who can be qualified as foreign terrorist fighters in accordance with Security Council resolution 2178 (2014) but also their families “travelling back to their countries of origin or nationality, or to third countries, from conflict zones”.¹⁸

The Council labelled such individuals as threats¹⁹ and explicitly calls on Member States to address the risk posed “by foreign terrorist fighter returnees and relocators and their accompanying family members”²⁰ and to “assess and investigate suspected individuals whom they have reasonable grounds to believe are terrorists, including suspected foreign terrorist fighters and their accompanying family members, including spouses and children”²¹. The Council’s focus on family members accompanying foreign fighters represents a significant normative and procedural move, particularly in light of the Council having already broadened the scope of its engagement to encompass inchoate offences and showing more preoccupation for regulating the “pre-criminal space”. The Special Rapporteur stresses the importance that governments and other relevant stakeholders monitor the human rights impact of such measures, including on the long term.

Building on the above, Security Council resolution 2396 (2017) called on States to strengthen efforts in a number of key areas in ways that may have serious implications for domestic legal regimes, including by setting up new obligations in accordance with the powers vested in the Security Council under Chapter VII of the United Nations Charter.

These measures include requiring 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, and “to ensure API is analysed by all relevant authorities, with

¹¹ S/RES/2322 (2016)

¹² *Ibid.*

¹³ S/RES/2396 (2017), para. 24.

¹⁴ S/RES/2396 (2017), para. 7; S/RES/2322 (2016), para. 5.

¹⁵ S/RES/2178 (2014), para. 11, S/RES/2396 (2017), para. 6.

¹⁶ S/RES/2322 (2016), para. 3.

¹⁷ S/RES/2178 (2014), para. 3; S/RES/2322 (2016); S/RES/2396 (2017), paras. 3 and 22.

¹⁸ S/RES/2396 (2017), para. 5.

¹⁹ *Ibid.*, para. 44.

²⁰ *Ibid.*, para. 25.

²¹ *Ibid.*, para. 29.

full respect for human rights and fundamental freedoms for the purpose of preventing, detecting, and investigating terrorist offenses and travel”.²² States shall further “develop the capability to collect, process and analyse (...) passenger name record (PNR) data and to ensure PNR data is used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offenses and related travel.”²³

The Council further imposed an obligation 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 travellers and conduct risk assessments and investigations”²⁴ and 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”.²⁵ Both obligations are to be implemented in compliance with international human rights law.

With respect to all the above-mentioned databases and information systems, States are encouraged to share relevant information with Member States and international bodies, as appropriate.

The Special Rapporteur recognizes the utility of efficient international and regional cooperation for successfully countering terrorism and ensuring that perpetrators of terrorist offenses are brought to justice. She nonetheless emphasizes that such cooperation, whether in the area of judicial assistance or intelligence-sharing, is not a rights-free zone. Notwithstanding the context, States are bound by international human rights law, including relevant obligations under article 17 of the International Covenant on Civil and Political Rights (ICCPR). A number of governments have however resorted to measures that substantially encroach on human rights, including the right to privacy, under both emergency and ordinary legislation or practice. While international human rights law provides for accommodation mechanisms in the form of limitations and derogations, any permissible restrictions must be in genuine response to a threat, with due regard for the principles of necessity, proportionality and non-discrimination.²⁶ 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 as well as the Security Council.²⁷

The Special Rapporteur notes the challenges in implementing some of the above-addressed measures in a human rights compliant manner. In the context of international cooperation, governments will be faced with dilemmas flowing from state sovereignty considerations, jurisdictional complexities, and complications caused by the diverging legal and policy frameworks and standards applicable in different jurisdictions. The Special Rapporteur acknowledges that the quality of privacy protection in law and in practice shows divergence between States. In the absence of protective parity, the implementation of measures advocated

²² *Ibid.*, para. 11.

²³ *Ibid.*, para. 12.

²⁴ *Ibid.*, para. 13.

²⁵ *Ibid.*, para. 15, S/RES/2322 (2016), para. 3.

²⁶ A/HRC/37/52.

²⁷ See S/RES/1373 (2001), 1456 (2003), 1566 (2004), 1624 (2005), 2178 (2014), 2341 (2017), 2354 (2017), 2368 (2017), 2370 (2017), 2395 (2017) and 2396 (2017); A/RES/68/167; A/RES/69/166; A/RES/71/199; A/RES/49/60; A/RES 51/210; A/RES/72/123; A/RES/72/180; A/HRC/RES/28/16; A/HRC/RES/34/7.

for States by the Security Council is likely to contribute to greater privacy intrusions, which in turn leads to enhanced risk to the protection of interlinked rights.

She in particular warns about the potential negative human rights impact of cooperation with States who display a poor human rights record. The Special Rapporteur and other relevant stakeholders, among them OHCHR, have repeatedly warned about vague and overbroad definitions of terrorism and terrorism-related offenses adopted by a number of States as these grant undefined and therefore potentially arbitrary discretion on implementing authorities, in violation of core human rights principles and the fundamentals of the rule of law. Such laws lead to critical consequences on the protection and promotion of human rights, with particularly serious implications on marginalized groups, human rights defenders, journalists, political opposition and dissidents. The lack of an internationally accepted definition of terrorism means that individual States implement the above addressed measures in accordance to with their own definitions of terrorism and terrorist entities. For this reason, the Special Rapporteur warns against any form of cooperation, whether in the area of mutual legal assistance or intelligence-sharing, that may facilitate human rights violations or abuses and notes that State responsibility may be triggered through the sharing of information that contributes to the commission of gross human rights violations.

Against this background, the Special Rapporteur emphasizes the importance of ensuring that State efforts aimed at increasing the efficiency of, at times lengthy and over-bureaucratized mutual legal assistance arrangements, do not lead to sidestepping existing mechanisms for accessing data held abroad and thereby undermine established human rights safeguards. She therefore stresses that any mutual legal assistance arrangements must be compliant with domestic and international, including human rights, standards and procedures governing such arrangements, and subject to democratic oversight.

The Special Rapporteur expresses particular concerns regarding cross-border intelligence-sharing arrangements. The mandate of the Special Rapporteur has already warned against such arrangements falling short of international human rights norms and standards, in particular the lack of a human rights-compliant legal basis and of adequate oversight.²⁸

While intelligence sharing practices may serve as an effective counter-terrorism tool, their use interferes with human rights, in particular the right to privacy, and as such must be implemented pursuant to a domestic legal basis that is sufficiently foreseeable, accessible and provides for adequate safeguards against abuse. 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.²⁹ 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 as well as their communications may be shared with foreign intelligence agencies without the protection of a publicly available legal framework and without proper safeguards,³⁰ making the operation of such regimes unforeseeable for those affected by it and thus incompatible with article 17 of the ICCPR.³¹ Moreover, in many jurisdictions intelligence and law enforcement agencies are excluded from provisions of data protection legislation that limit the sharing of personal data, meaning that information gathered for one purpose may be used for other unrelated

²⁸ See, for example A/69/397 and A/HRC/13/37.

²⁹ A/HRC/27/37. See also, Privacy International, 'Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards' (April 2018).

³⁰ A/HRC/27/37, para. 30.

³¹ A/69/397, para. 44.

governmental objectives. This “purpose creep” presents concerns not 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.³²

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.³³ 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.

The Special Rapporteur notes that interferences with human rights, including the right to privacy must be accompanied by adequate safeguards to protect against abuse. In the view of the mandate, these safeguards “generally include independent prior authorization and/or subsequent independent review.”³⁴ This is also in line with recommendations made by the General Assembly³⁵, the UN Human Rights Committee³⁶ and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.³⁷

The Special Rapporteur highlights the need for consistency of both soft law and of binding obligations imposed on UN Member States with international human rights norms and standards. In this respect, she recommends that States as well as relevant UN bodies be guided by the *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*³⁸, developed by the mandate, including in the implementation of relevant resolutions of the Security Council.

She underscores that intelligence-sharing should be based on publicly accessible and sufficiently foreseeable national law that outlines clear parameters for the intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.³⁹ States should further ensure that intelligence-sharing agreements and their implementation are subject to meaningful independent oversight and that oversight bodies have the power to consider all relevant aspects of activities related to such intelligence-sharing.⁴⁰ Finally, the Special Rapporteur emphasizes the due diligence obligations incurring on States sharing information as well as States accessing or receiving information to undertake an

³² A/HRC/13/37, para. 50; A/HRC/69/397, para. 56.

³³ A/HRC/13/37, A/69/397.

³⁴ A/69/397, para. 45.

³⁵ A/RES/68/ para. 4(d); A/RES/69/166, para. 4(d); A/RES/71/199 para. 5(d).

³⁶ UN Human Rights Committee, Concluding Observations on the Fifth Periodic Report of France, CCPR/C/FRA/CO/5, para. 12; UN Human Rights Committee, Seventh Periodic Report of the United Kingdom, CCPR/C/GBR/CO/7, para. 24.

³⁷ A/HRC/23/40, para. 93.

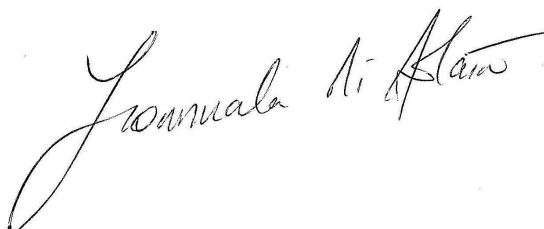
³⁸ See *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, A/HRC/14/46.

³⁹ *Ibid.*, Practices 31 and 32.

⁴⁰ *Ibid.*, Practices 6 and 7.

assessment of the counterpart's record on human rights, as well as the existing legal safeguards and institutional controls.⁴¹

Yours sincerely,

A handwritten signature in black ink, reading "Fionnuala Ní Aoláin". The signature is written in a cursive style with a large initial 'F'.

Fionnuala Ní Aoláin

Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism

⁴¹ *Ibid.*, Practice 33.