### ***Check against delivery***



***Statement by Ms. Fionnuala Ní Aoláin***

***SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS WHILE COUNTERING TERRORISM***

*Upholding human rights and promoting gender responsiveness while countering terrorism in the age of transformative technologies*

*29 June, 2021*

*New York*

**Technology, Counterterrorism and Human Rights**

**An Overview from the Special Rapporteur**

**Excellencies, Distinguished Delegates, Ladies and Gentlemen**

Thank you for the invitation to speak to today’s Global Outlook on technology, counterterrorism and human rights. The focus of the High-Level Conference is timely and of critical importance to our collective efforts to counterterrorism while promoting and protecting human rights. Through my mandate, I have continued to **affirm** thevalue of a focus on technology and its use in counterterrorism. I have also cautioned of its greatest risks. In my reflections today, I seek to reorient *us all to* the premise that the United Nations and Member States’ use of existing and new technology in counterterrorism and P/CVE must be indispensably connected to human rights and rule of law. This rooting in human rights not only applies to the development of such technologies but also their use and transfer. Only in firmly grounding counterterrorism technology use in human rights will there be meaningful compliance with international and national law. As the new Global Counter-terrorism strategy affirms – failure to comply human rights and rule of law principles and obligations (including in the use of technology), will only exacerbate the phenomena that drive radicalization to violence and terrorism.

**The Value of New Technologies**

To be successful in this context, we must hold several things to be true at once. We must recognize the value of existing, new and emerging technologies. In parallel, we must recognize the detriment to which they have been used in the past and the great risk they may (without proper controls) pose to fundamental human rights and the rule of law.

I have continued to acknowledge, that there is an expanding arena where the advancement and adaptation of new technologies can support the dignity and protection of the human person, including for example the use of biometric data to enable and support refugee or IDP family reunification,[[1]](#footnote-1) or food transfer to vulnerable populations in conflict affected settings.[[2]](#footnote-2) Other example of positive use include the use of human rights complaint cross-border e-evidence to prosecute serious crimes of international law including genocide, crimes against humanity and war crimes.

Through these ventures, we can see that promoting and protecting human rights while achieving development and security aims are not only possible, but in the best circumstances – mutually reinforcing. However, we have seen significant resistance to such balance in the counter-terrorism arena. To achieve success, we must press towards a broader recognition of the risks, bounds, and legal limits to the use of technology within a human rights and rule of law framework. In particular, the UN, and its counter-terrorism entities must consider and act upon the risks and abuses that arise in a service-oriented model of counter-terrorism technical assistance and capacity building; avoid being complicit in the transfer and support of use of new, or emerging technologies in States with clear and evidenced practices of human rights abuses and discriminatory patterns of use. We must ensure the UN itself enforces and affirms in a **uniform manner** the relevant human rights standards. We cannot have the UN human rights entities speaking in one voice on human rights, and the counterterrorism entities reinterpreting human rights and humanitarian law to the detriment of agreed State standards, and the values of the United Nations Charter as a whole.

**Broader Human Rights Challenges of Technology Developments in the context of Counterterrorism**

Let me now turn to address the risks. The negative effect of overly broad use, application and transfer of technology for counterterrorism has made international headlines over the last 20 years. It has been observed through growing surveillance with little legal limits, arbitrary and prolonged detention enabled by technology infringements, infringements on the right to speech, assembly, and more, exceptionality in criminal law, and the misuse of such measures to the detriment of civic space and civil society. We have seen border profiling and denial of refugee and asylum claims, the use and transfer of technologies to rights denying States where there is evidence of systematic human rights violations.

There are equally nefarious, but less visible *discriminatory* impacts recently elaborated on by my colleague the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance.[[3]](#footnote-3) Here I affirm her prescient warnings that what is needed is equality-based approach to human rights governance of emerging digital technologies in particular. This requires moving beyond “colour-blind” or “race neutral” strategies. What is required in the context of emerging digital technologies is careful attention to their racialized and ethnic impact, from government officials, the United Nations and other multilateral organizations, and the private sector.

I underscore that the discriminatory impacts of new technologies use in counterterrorism are both direct and indirect. And, SR Achiume has found “even where discrimination is not intended, indirect discrimination can result from *using innocuous and genuinely relevant criteria that also operate as proxies for race and ethnicity*.” This is particularly true for the underlying algorithmic functions of technologies, as well is in their standards for design and development that so often use and rely “on predictive models that incorporate historical data – data often reflecting discriminatory biases and inaccurate profiling – including in contexts such as law enforcement, national security and immigration,” AND fail to engage stakeholders subjected to such technologies.

I urge Member States and the United Nations to consider that promoting and protecting the right to privacy in a digital age requires new initiatives and methods.

* It requires keeping human rights safeguards development at an equivalent pace to the rapid development of new technologies.
* It requires human rights due diligence in the use, transfer and implementation of technologies for counterterrorism, including the use of mutual legal assistance frameworks that integrate safeguards.
* Enhancing the capacity of Governments, companies and individuals to use new technologies is not a risk free or rights free space. It is precisely here where such capacity building can pose the greatest threat if it is undertaken without required safeguards.

**New Technologies in Counterterrorism and the Global Counter-Terrorism Strategy Review**

* As we take a global view to next two years, the newly concluded Global Counter-Terrorism Strategy presents both new opportunities and challenges.
* First, it has expanded the references made to new technologies, including social media, online content and its moderation, virtual assets and countering the financing of technology, biometrics, artificial intelligence, infrastructure and vulnerable targets, and more.
* Secondly, it presents a farther-reaching commitment to the promotion and protection of human rights and fundamental freedoms while countering terrorism increasing reference to international law compliance overall as well as in the specific use of technology.
* This indicates a common theme in the security and counter-terrorism arena where security is often the driving impetus for new technologies, with human rights considerations and rights enhancing goals either deemed irrelevant or a last step.
* Again, we must hold two things at once. We see a growing concern among Member States around the use of technology for terrorism purposes, as well as a growing willingness to expand the technological tools to counterterrorism.
* It is the equal commitment to use such technology in compliance with international human rights, humanitarian and refugee law that must be the outcome.
* It is the time to articulate precisely what such safeguards look like to develop a technology security nexus that is fit for purpose, effective, and sustainable.

**Biometrics**

I highlight the mandate particular focus on the deployment of biometrics in counterterrorism.[[4]](#footnote-4) I have observed accelerated use and affirmation of the use of biometrics in the counter-terrorism context both normatively and practically[[5]](#footnote-5) from ‘heart-prints’ to mass ‘iris scanning’ to scalar DNA sampling.

Biometric data collection is inherently high-risk, as it involves the collection of the most intimate human data both physiological characteristics and ‘behaviometrics’ making the costs of misuse of uniquely abhorrent. I am particularly concerned about the development of ‘‘behaviometrics’’ in detention and interrogation contexts, given its Kafkaesque implications for the most fundamental of due process and liberty rights. Precisely because biometric measurements and metrics relate to biological or behavioural human characteristics, that are commonly possessed by all human beings while also being highly representative of a person, thereby allowing for the identification of individuals with profound and often irreparable costs when misused. When scaled up and involving mass collection, use and transfer of intimate data on vulnerable and minority groups what we may be observing is systematic violations of the most fundamental of rights that might in certain cases reach the threshold of crimes against humanity under international law.

Against the background of obligations imposed by the United Nations Security Council requiring States to develop biometrics systems and collect relevant data, in line with international human rights law norms, I am concerned about salient human rights gaps in domestic and international legal and policy approaches. What do we need to address this?

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. At most basic, I call for granular and universally applied human rights assessments, benchmarking and oversight at every stage of biometric counter-terrorism data collection, retention, processing, and sharing. We must enhance human rights implementation, such as human rights impact assessments, meaningful monitoring and evaluation of ways in which human rights are affected by relevant laws, policies, and practices, and increasing effective independent oversight.

**Covid-19**

The world is still struggling with the devastating health, human rights, economic and social impact of Covid-19. We feel those harms acutely. I continue to highlight concerns about the deployment of security-created and regulated technologies to regulate a health pandemic, whose effects are most acutely felt by populations whose marginal and vulnerable status in national settings, have often corelated to their experience of human rights violations at the hands of the security sector. Any exceptional measures taken during the pandemic including the deployment of human rights intrusive technologies is subject to the triparted tests of proportionality, necessity, and non-discrimination. Moreover, lest we forget the nagging tendency of the exceptional to normalize in times of crisis, we have an obligation to prevent the securitization of health, by virtue of an insidious creep of counterterrorism practice as the ‘solution’ to a health crisis.

**Conclusion**

The mandate has articulated the impact of emerging and new technologies on human rights, including detailed reporting on one of the most ubiquitous forms of technology used in counter-terrorism – biometrics.

As the use of new, emerging, and even well-established technologies continues, it is imperative to ensure the promotion and protection of human rights is central to the discussion.

Placing human rights at the center of the analysis is not only what is required by international human rights law, but it also remains one of the only ways to ensure that counter-terrorism laws, policies, and practice are fit for purpose. As I have reiterated, and evidence continues to demonstrate, it is only through human rights and rule of law compliant responses to the challenges we face that counter-terrorism efforts will be successful in the long term.

Importantly, we must reflect on what is often a misstep in analysis in this discussion. Technology’s use for counterterrorism does not just affect the “right to privacy,” or implicate the need for data protection, but holds ramifications for a broad range of civil, political, economic, social, and cultural rights, noting the "indivisible and interdependent character of all human rights." Technology should be a friend and not a foe of human rights, but to do that we must affirm the centrality of human rights to the digital and technology age, to preserve not only human rights but our fundamental humanity.

1. For deeper discussion, GSMA Refugee and Identity: Consideration for mobile-enabled registration and aid delivery (2017) addressing the use of mobile data, forecasts and analysis to address the needs of refugee populations; IOM and Biometrics, Supporting the Responsible Use of Biometrics (2018) addressing the use of biometrics in the context of orderly and safe migration. [↑](#footnote-ref-1)
2. See e.g. GSMA Mobile for Humanitarian Innovation programme, which has been funded by the UK Department for International Development (DFID) since 2017, this three-year collaboration will primarily focus on the use of mobile money to deliver digital assistance through cash-based transfers to save lives in global emergencies, including pandemics and natural disasters. [↑](#footnote-ref-2)
3. A/HRC/44/57 [↑](#footnote-ref-3)
4. <https://www.law.umn.edu/sites/law.umn.edu/files/2020/07/21/hrc-biometrics-report-july2020.pdf> [↑](#footnote-ref-4)
5. The use of biometric data as a counter-terrorism tool was first referenced in Security Council resolution 2160 (2014). [↑](#footnote-ref-5)