UNITED NATIONS
HUMAN RIGHTS
SPECIAL PROCEDURES
SPECIAL RAPPORTEURS, INDEPENDENT EXPERTS & WORKING GROUPS

PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9543 / +41 22 917 9738 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

As delivered

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,

I do want to underscore the importance of this timely discussion. It is important discussion for our collective efforts to counter terrorism while promoting and protecting human rights. Through my mandate, I have continued to affirm the value of a focus on technology and its use in counterterrorism. But, I have also cautioned of its greatest risks. In my reflections today, I want to reorient *us all to* the premise that the United Nations and Member States' use of existing and new technology in counterterrorism and preventing and countering violent extremism must be indispensably connected to human rights and rule of law. The rooting in human rights not only applies to the development of these technologies but also their use and transfer. Only when we firmly ground counterterrorism technology use in human rights practice will there be meaningful compliance with international law. As the new Global Counter-terrorism strategy affirms – failure to comply human rights and rule of law principles and obligations, including specifically 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 a number of almost contradictory things to be true at once. We have to recognize the value of existing, new and emerging technologies, absolutely so. 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 in the present and the future.

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. So, for example, if we think about use of biometric data to enable and support refugee or IDP family reunification,[1] or we think about food transfer to vulnerable populations in conflict affected settings.[2] Or another positive example can be 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. All of these are positive uses, affirming and supporting human rights.

Through these ventures, what we can see is that promoting and protecting human rights while achieving development and security aims are not just possible, but in the best circumstances – they are mutually reinforcing. However, what we have also seen regrettably is significant resistance to this kind of balance in the counter-terrorism arena.

If we are going to achieve success, and success means really preventing terrorism, we must press towards a broader recognition of the risks, bounds, and the legal limits to the use of technology within a human rights and rule of law framework.

In particular, the UN itself and its counter-terrorism entities, those members of the Global Counter-Terrorism Coordination Compat, we have to consider and act upon the risks and abuses that arise in a service-oriented model of counter-terrorism, particularly when we are engaged in technical assistance and capacity building. Because what we have to avoid is being complicit in the transfer and support of new, or emerging technologies in States with clear and evidenced practices of human rights abuses and discriminatory patterns of use.

We must ensure that the UN itself enforces and affirms in a uniform manner – and it's the uniformity that is really important here – the relevant human rights standards. We cannot have, as we sometimes do, the United Nations human rights entities like my mandate or the Human Rights Commissioner who spoke earlier speaking in one voice on human rights, and the counterterrorism entities reinterpreting human rights and humanitarian law to the

[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.

[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.

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

So let me talk now about the broader human rights challenges of technology developments and some of those risks in a really practical way. It is the negative us of overly broad use, application and transfer of technology for counterterrorism has made international headlines over the last 20 years. Where have we seen this overreach, this abuse? We have seen it through growing mass surveillance with few meaningful legal limits. We have seen it in arbitrary and prolonged detention enabled by technology. We have seen it in infringements on the right to speech, assembly, and exceptionality in criminal law, and the misuse of such measures to squeeze and choke civil society and civic space. We have seen border profiling and denial of refugee and asylum claims through the use these technologies and we have seen the wholesale transfer of highly problematic and high risk technologies to rights denying States where there is evidence of systematic human rights violations being incurred by the use of those technologies.

As well as that, and the High Commissioner has already eluded to this – there are equally nefarious, but less visible *discriminatory* impacts, which have been succinctly elaborated on by my colleague the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance.[3] Today, I affirm her prescient warnings on what is needed for in equality-based approach to human rights governance of emerging digital technologies, in particular. This requires us to move beyond a "colour-blind" or "race neutral" strategies. What is required, as we have heard in the High Commissioner

Statement today, in the context of emerging digital technologies is careful attention to their racialized and ethnic impact. That attention needs to come from government officials, the United Nations and other multilateral organizations, as well as the private sector.

[3] A/HRC/44/57.

I want to underscore here that the discriminatory impacts of new technologies use in counterterrorism are both direct and indirect. That is the case precisely because "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*."[4] This is particularly true for the underlying algorithmic functions of technologies, as well as the standards for design and development that so often use and rely on as Tendayi Achiume says, "predictive models that incorporate historical data" and that historical data reflects discriminatory biases and inaccurate profiling, including in law enforcement, national security and immigration contexts.

I urge Member States and the United Nations to consider that promoting and protecting the right to privacy as a gatekeeper right for other rights in a digital age needs new initiatives and methods.

- First, it requires keeping human rights safeguards development at an equivalent pace to the rapid development of new technologies.
- The second thing it requires is human rights due diligence in the use, transfer and implementation of technologies for counterterrorism. You cannot pick and choose which one of those you want, you have to have all of them in order to fully and effectively enforce human rights. This includes in the use of mutual legal assistance frameworks that integrate safeguards.
- Thirdly, we have to enhance the capacity of Governments, companies – and its great to Facebook with us today and I thank the dialogue that my mandate has had with Facebook on community standards in this area – but also individuals to use new technologies that are not risk free from human rights abuse. It is precisely here where we know that these technologies are not risk free and we have to build capacity to enforce these rights and safeguards.

[4] A/HRC/44/57.

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

Let me briefly say two or three words about the new technologies we have seen and attention to this issue in the new Global Counter-Terrorism Strategy.

What we do see in this two-year strategy is a number of both new opportunities and challenges. First, we see expanded reference 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.

The second thing we see, is really an extraordinary and far reaching commitment to the promotion and protection of human rights and fundamental freedoms while countering terrorism and an overall deepening of the necessity to comply with international law in the use of technology.

And what these two things do is indicate a common theme in the security and counter-terrorism sector and it is a hard one for us all, which is that security is often the impetus for driving new technologies and human rights often gets added in as either a last step or afterthought.

And so we have to do better. What we have to do is again go back to those two things we are going to hold at once. Recognize that there is a growing concern among Member States around the use of technology for terrorism purposes and a desire to use these tools. And at the same time, we have to have an equal commitment to compliance with international human rights law, not just as an abstract good, but as a practical and enforced set of tools to ensure that these technologies are not human rights abusive.

Biometrics

Let me say two more things I will focus on before I close.

The first is to underscore the attention my mandate has paid to biometrics and the deployment of biometrics in counterterrorism.[5] I have observed and seen as many of us

[5] https://www.law.umn.edu/sites/law.umn.edu/files/2020/07/21/hrc-biometrics-report-july2020.pdf

have, an accelerated use and affirmation of the use of biometrics in the counter-terrorism both normatively and practically[6] whether this is from ‘heart-prints’ to mass ‘iris scanning’ to scalar DNA sampling. I think we all know, but it needs to be said - biometric data collection is inherently high-risk. It involves the collection of the most intimate human data both physiological characteristics and ‘behaviometrics’ making the costs of misuse uniquely abhorrent. I am particularly concerned about the development of ‘‘behaviometrics’’ in detention and interrogation contexts, given its Kafkaesque implications for the most fundamental rights of due process and liberty. Precisely because biometric measurements and metrics relate to biological or behavioural human characteristics, they are commonly possessed by all human beings and are highly representative of a person, making individual identification so precarious and often come with irreparable costs when that data is misused.

When we scale up that kind of data collection – its use, its transfer – the impact on vulnerable and minority groups is extraordinary and what we see. in many contexts regrettably, is systematic violations of the most fundamental of rights that in certain cases may meet the threshold of crimes against humanity under international law.

It against this background of risk that we have to really think about our salient human rights obligations and the gaps we have. How can we do better? I think how we can do better as the UN is we can call for granular and universally applied human rights assessments, benchmarking and oversight at every stage of biometric counter-terrorism data collection, use and transfer. We need meaningful monitoring, we need evaluation and we need increasingly effective, as my mandate has continue to call for, independent oversight.

Closing: COVID-19 & Placing Human Rights at the Center of Our Responses

Two closing remarks, one is on COVID-19. The world is still struggling with the devastating health, human rights, economic and social impact of Covid-19. We all feel those harms acutely. I continue to highlight the concerns about the deployment of security-created and regulated technologies to engage a health pandemic. I want to underscore that

[6] The use of biometric data as a counter-terrorism tool was first referenced in Security Council resolution 2160 (2014).

the effects of the pandemic are most acutely felt by populations with marginal and vulnerable status in national settings. And equally, those populations are the ones who have frequently negative, difficult, discriminatory or exclusionary experience 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 a tripartite test of proportionality, necessity, and non-discrimination under international law. Lest we forget the nagging tendency of the exceptional to persist from the exception into normal times, we in particular in the Global Counter-Terrorism Coordination Compact have an obligation to prevent the securitization of health, particularly when that securitization will affect marginal and vulnerable communities most. And we have to stop the insidious creep of counterterrorism practice as the 'solution' to a health crisis.

In conclusion, placing human rights at the center not just our 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 are central to the challenges we face in addressing terrorism, will we be successful as well as consistent with our international law obligations in preventing and addressing terrorism.

Many thanks to you all.