GENEVA 10, SWITZERLAND
-MAIL: registry@ohchr.org

Technology, Counterterrorism and Human Rights

An Overview from the Special Rapporteur

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 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

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

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 h

the effects of the pandemic