ODIHR Expert consultation meetings on human rights challenges related to information gathering and sharing and new technologies in border management in the counter-terrorism and freedom of movement context

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

15 June 2020

The mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism acknowledges and thanks ODIHR and OSCE for convening this important discussion on collecting and sharing information and the use of new technologies in the counter-terrorism and freedom of movement context. The mandate of the Special Rapporteur has been particularly concerned about the interface of new technologies and counter-terrorism.[1] Most specifically I have been uneasy about the ways in which counter-terrorism has become the 'early adoption' or experimental arena for new, highly-intrusive and under-regulated technologies. Let me note a couple of framing reference points:

1) The lack of an agreed multi-lateral treaty definition of terrorism means that in practice there is a wide and apparently unlimited latitude to States to defined 'terrorism' as they please domestically. This means that globally we see wide, vague, imprecise and highly problematic definition of terrorism in multiple national legal systems. The mandate's starting point is that the collection, sharing and use of data collected at borders under the rubric of 'terrorism' is attached to domestic definitions of terrorism that are often wholly problematic from a human rights perspective.

2) The nature and form of the global counter-terrorism architecture and its hardwired regulatory incentives that produce UNSCRs, including UNSCR 2396 that have

[1] I acknowledge my thanks to Dr. Krisztina Huszti-Orban mandate legal advisor who leads the SRCT & HR's work on the interface of technology and counter-terrorism.

limited human rights substance, fail to 'think-through' the human rights dimensions and deficits of what I have termed 'super-legislative' Security Council Resolutions.[2]

3) The lack of specific human rights guidance on many of the 'technology' solutions, including API and PNR, but also stretching beyond to biometric data use, AI +. There is also a lack of sustained integration of human rights specifics in the authorization for their application by Security Council Resolutions as well as in national legislation. Thus, while Security Council Resolutions can be highly specific on counter-terrorism demands and requirements from actors, to process, to mechanisms, this capacity for specificity, benchmarking and guidance has a human rights blind spot.[3]

4) The lack of civil society engagement and human rights expert engagement by the Counter-Terrorism Committee / Security Council in the CT regulatory space.[4]

A reminder of what is at stake from a human rights perspective. Data collection, retention, processing and sharing have become an essential tool for many States in the fight against terrorism. While affirming the importance and value of information gathering and analysis in the prevention, investigation and prosecution of terrorism, I remain deeply concerned about the control and management of data and related oversight in a human rights-compliant manner.[5] I

[2] A/73/361
[3] UNSCR 2396 mentions human rights four times generically in the preamble "*Reaffirming* that Member States must ensure that any measures taken to counter terrorism comply with all their obligations under international law, in particular international human rights law, international refugee law, and international humanitarian law, *underscoring* that respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures" and "*Noting with concern* that terrorists and terrorist groups continue to use the Internet for terrorist purposes, and *stressing* the need for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology and communications for terrorist acts, as well as to continue voluntary cooperation with private sector and civil society to develop and implement more effective means to counter the use of the Internet for terrorist purposes, including by developing counter-terrorist narratives and through innovative technological solutions, all while respecting human rights and fundamental freedoms and in compliance with domestic and international law …" and a reference to the Nelson Mandela Rules. In the text of the resolution, human rights is mentioned in OP4, OP7, OP12, OP13 (x2), OP15, OP18, OP19, OP22, and OP23.
[4] A/HRC/40/52
[5] *See* https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunication File?gId=24238.

underscore the importance of privacy, due process and remedial rights for persons' subject to such measures. I highlight that privacy facilitates the exercise of a wide range of human rights and that consequently, privacy violations may have an intersectional adverse impact not only on civil and political but also economic, social and cultural rights.

In a number of my country reports,[6] I have been critical of the use of databases generally including addressing the definitional basis that creates the basis for individual inclusion. For example, I have noted that while inclusion in a database might not constitute a criminal law measure, it nonetheless comes with potentially far-reaching negative consequences on the affected individuals' human rights, including restrictions on liberty that may engage article 5 of the European Convention on Human Rights. I have also been troubled by the inability of individuals in multiple countries to be notified of their inclusion on a database, to challenge and/or exist (find an off-ramp).[7] I continue to voice my concern about the oversight of data collection, the lack of independent oversight in most countries, specifically the need for independent oversight covering all states of data collection and processing given the implications of the rights limitations concerned.

In the context of API/PNR, let me raise some very specific concerns for this audience.

Issue of defining 'known' and 'suspected' terrorists as referred to in OP4, UNSCR 2396 – definitions need to be broader than relevant criminal law definitions (as watchlists/ no fly lists are broader than e.g. arrest lists). A key question for States and human rights actors is how these terms are they defined in domestic law? The UNSCR provided no specific guidance on this issue, and there is the expectation that we will "know it when we see it" in practice. The Special Rapporteur is clear that precise and defined terminology is needed for these terms. Threshold needs to be clearly set out in domestic law, but many jurisdictions only seem to have policy definitions (if any). The Special Rapporteur expresses profound concern about the establishment of passenger

[6] *See* country visit reports to Belgium, France and Kazakhstan, https://www.ohchr.org/EN/Issues/Terrorism/Pages/Visits.aspx
[7] *See generally*, Gavin Sullivan, The Law of the List (Cambridge University Press, 2020)

data exchange systems across countries, in particular whether the countries being set up to share and receive data have extremely poor human rights records, and have a demonstrated record of applying CT/PVE against HRDs, civil society and political opposition.

Advance Passenger Information (API)

This category may be considered less problematic from a human rights point of view because it is information that is contained in identification documents —it is verified information and can be used to check against watchlists and databases. [8] Nonetheless, this data is biographic information so both privacy and data protection are engaged (potentially other rights as well). Abuses tend to mostly be linked to

1) Abusive/ overbroad inclusions on different terrorism-related watchlists (and no fly lists etc. are in many countries reportedly riddled with errors, with information and resulting nominations being inaccurate or outdated);

2) API being combined with PNR, biometric data, etc. for the purposes of profiling (including predictive profiling).

Passenger Name Record (PNR)

PNR= information collected by airlines/ travel companies related to data provided by individuals in relation to bookings.[9] It may include travel dates, itineraries, travel companions, financial information related to the booking, address and phone numbers of individuals, dietary preferences (kosher, halal); disability-related needs; travel companions, IP address and other information about the operating system used when booking a ticket or checking in for flights or travel.

[8] The same as what can be read when passport machine readable strip is run at the airport. Note that in principle, API/ PNR do not contain/ focus on biometric data (as you need to be able to collect the data remotely) but are frequently linked to biometric data (watchlists/ databases will contain it, profiles built using PNR, etc. will likely have it/ be linked to it as well).

[9] Including check-in, etc.

- It can contain extensive datasets and may include sensitive data or data that may be used for profiling and predictive risk assessments.
- Inconsistencies as to number of data points 1) collected by airlines/ travel companies; 2) required by governments from these companies. Notably, there is no general industry standard regarding either for the layout and content of a PNR. There is a clear risk that this will result in states/ regional/ international standards going for the highest common denominator which, from a human rights point of view will be the lowest common denominator.

Purpose of PNR:

Unlike API, it focuses on patterns and connections: PNR can help to identify suspicious travel patterns and hidden connections between known threats and their unknown associates by examining specific data elements.

- Includes potentially sensitive data that may allow for profiling, etc.:
  - **Financial data**. Reminder that financial data was not included as sensitive data in the GDPR (despite controversy) and will enjoy even less protection in a law enforcement/ national security context.
  - **Information that makes it possible to deduce information on health (disability accommodation); religion (kosher meal);** etc. This information may be able to indicate to governments if the person uses VPN (if they used it when booking/ checking in), which is a problem when shared with governments that prohibit its use. Phone number allows for additional surveillance, and other challenges that relate both to privacy and connected rights.
- There are a range of issues engaged by **data mining and profiling** in quite a few jurisdictions seeking 'bulk' access to PNR records, on all travelers. Many of these states allow for PNR data to be combined with other data and use the additional data for data mining and profiling purposes (declared security rationale: to identify probable/ potential terrorists).

- **Pattern recognition** may have different levels of intrusiveness, depending on its use (predictive or not). Some systems reportedly rates passengers based on the supposed risk they pose. The rating is based on algorithms, powered by machine learning and may present the same issues as other predictive policing tools. + Makes it next to impossible to challenge.
- **Individuals are not aware** what data is collected in this context or how it is used.
- **This brings us back to the importance for such data collection to be restricted to known or suspected terrorists and that these terms are narrowly defined.** We also need systems that minimize data collection, retention, and use by authorities (along the principles of necessity and proportionality). The UN travel system formally does not transmit sensitive data to Member States which, if correct, would be a start to a more robust human rights complaint approach.

What do we need?

1) Clear definitions and precision, currently entirely lacking in the international norms
2) Robust international and domestic oversight of the application, use, storage and sharing of API and PNR, currently entirely lacking in the international norms
3) Consequences for Abuse, currently entirely lacking in the international norms

To that end, the Special Rapporteur has set out a set of Principles that should guide any regulatory action in this arena, based on the applicable international law obligations of States.

Human Rights Principles Applicable to Watchlisting

1. Any placement of individuals or groups on watch lists should be as a result of a fair and accountable legal process.

2. Placement of individuals or groups on a watch list should be a necessary and proportionate response to an actual, distinct and measurable terrorism threat, and consistent with the definitions of terrorism found in the terrorism suppression conventions and United Nations Security Council resolution 1566.

3. Placement of individuals or groups on a watch list should not be discriminatory nor based on attributes of race, ethnicity, national or social origin, religious belief, age, sex or gender, minority status or any protected attribute under international human rights law.

4. Placement of individuals or groups on a watch list implicates a range of human rights including freedom of movement, association, expression, the rights to privacy, property, health, due process, family life, and social and economic rights including the right to work. Any such human rights impact must be adequately considered and taken into account in watchlisting procedures.

5. Human rights protections deriving from both customary international law and treaty law apply to every stage of the watchlisting process including collection, processing, storage and sharing of data.

6. States engaged with or supporting watchlisting must comply with internationally recognized data protection standards including the principles of lawfulness and fairness; transparency in collection and processing; purpose limitation; data minimization; accuracy; storage limitation; security of data; and accountability for data handling.

7. Individuals subject to watchlisting must have a reasonable and legally-based opportunity to judicially and administratively challenge the basis of their inclusion on a list. Adequate legal representation, reasonable access to information and promptness in proceedings must be ensured in this respect.

8. If an individual is removed from a list by the listing country, other States must endeavor to ensure that delisting occurs in all jurisdictions or provide an adequate legal process to challenge continued listing.

9. The inclusion of children (persons under 18) in any listing process must generally be avoided.

10. If children are included in watchlists, any data collection, processing, storage and sharing must always comply with the safeguards contained in the Convention on the Rights of the Child.