Position Paper of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism on the United Nations Countering Terrorist Travel ('CT Travel') Programme and the goTravel Software Solution*

Professor Fionnuala Ní Aoláin

Introduction

1. In the past ten years, the international community has placed ever-greater trust in technical solutions to the threat of terrorism. The Special Rapporteur recognizes the valuable role that new technologies can play in society generally and in response to serious crime, including terrorism.[1] All too often, however, a blinkered focus on security has prompted a rush to implement 'fixes' without first taking the requisite time and investment to carry out detailed analysis of how such measures can be undertaken in compliance with international law, including international human rights law, international humanitarian law, and international refugee law. The Special Rapporteur maintains that respect for and promotion of international law and human rights may demand fundamental changes to how technology is designed, used, and promulgated, as well as difficult decisions to abstain from, or delay, the adoption of such technology at all, or at least until its lawful compliance has been fully investigated and secured.[2]

2. One field in which the rapid development and deployment of technological solutions for purposes of counter-terrorism has had both positive and negative impacts, affecting the rights and freedoms of individuals worldwide, is that of air travel. The emergence of mass global air travel since the Second World War has been transformative for economic growth and prosperity, cultural exchange and migration, leisure and family life. But with the ubiquity of air travel has come its use as a target of hijacking and terrorism, its co-option for criminal purposes of trafficking in persons and illegal goods, and its transport of criminal and terrorist suspects and fugitives.

3. While protocols for border and passenger manifest checks have a long history as mechanisms for responding to, and preventing, crime and terrorism, past decades have seen the growth of technological responses in the field. One such development which now affects the lives of each of the billions of passengers each year[3] is the ubiquitous collection and processing of personal data (either in the form of Advance Passenger Information

---

* This position paper builds on the portfolio of work carried out by the Special Rapporteur Fionnuala Ní Aoláin addressing the interface of counter-terrorism, new technologies and human rights. Research and writing was led by Senior Legal Advisor Adriana Edmeades Jones, and support was provided by the Office of the High Commissioner for Human Rights (Geneva).

1 A/HRC/52/39, [7].

2 For an overview, see the Special Rapporteur's March 2023 report to the Human Rights Council, 'Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism,' A/HRC/52/39.

3 According to the International Civil Aviation Organization Annual Report 2021, the total number of passengers carried on scheduled services increased to 2.3 billion in 2021. See: https://www.icao.int/sustainability/WorldofAirTransport/Pages/the-world-of-air-transport-in-2021.aspx

('API') or Passenger Name Record ('PNR') data) via commercial carriers, and its sharing between States. This development is normatively linked to the expanded role of the United Nations Security Council in its counter-terrorism regulation after 2001, including directly requiring Member States to regulate travel of persons named as 'Foreign Terrorist Fighters.'[4] The utility of API and PNR as standard-form means of establishing passenger identity accurately and efficiently is clear, and the legitimate uses of such datasets for various purposes with respect to criminal investigation and border management are self-evident. But that does not mean that all uses of such datasets, or proposals for further expansion of current uses ought necessarily to be approved as inevitable or acceptable in the absence of rigorous investigation of their legal and human rights implications.

4. The United Nations Office of Counter-Terrorism ('UNOCT') is currently implementing a programme known as the United Nations Countering Terrorist Travel Programme ('CT Travel Programme') together with six UN implementing partners (the Counter-Terrorism Committee Executive Directorate ('CTED'), the UN Office on Drugs and Crime ('UNODC'), the International Civil Aviation Organization ('ICAO'), the UN Office of Information and Communication Technology ('UNOICT'), the International Criminal Police Organization ('Interpol'), and the International Organization for Migration ('IOM'). The purpose of the CT Travel Programme is to support and build States' capacities in this field, including by way of a UN-owned software program known as goTravel. The stated objective of these efforts is to support States in preventing, detecting, and investigating terrorist offences and related travel, all aiming towards the reduction in the risk of terrorist violence and the preservation of greater safety worldwide.

5. The Special Rapporteur recognizes that the international co-ordination of the approach to API and PNR collection and transmission in the inherently global industry of air transport has traditionally been, and remains, properly a subject for the agencies of the United Nations. Further, the Special Rapporteur underscores that the promotion and protection of human rights and fundamental freedoms, particularly in respect of victims of serious crime and terrorism, necessitates concerted action at the international level aimed at preventing air travel from being used itself as a means of terrorism and crime, or a conduit for carrying out crime, or facilitating the travel or escape of perpetrators and suspects. Nevertheless, the Special Rapporteur is very concerned that, at least so far as it currently appears to be operating, the CT Travel Programme and the promulgation of the goTravel software solution demonstrates a troubling lack of investment and commitment in counter-terrorism policy-making to prioritize the promotion and protection of human rights. The design, implementation, and spread of the global API/PNR data collection and sharing regime poses substantial potential risks to human rights which cannot be addressed by inadequate mitigation strategies at the back end. The implication of the UN's engagement in this scale and scope of international data sharing is deeply concerning and may undermine the UN's efforts to lead on international respect for human rights in the fight against terrorism. The scale and scope of data engagement well as expose the United Nations to potential responsibility for human rights abuses stemming ultimately from the CT Travel Programme and goTravel.

[4] See e.g. UNSCR 2178 requiring Member States to prevent the entry or transit of individuals believed to be traveling for terrorism-related purposes.

6. This position paper carries out an in-depth analysis of human rights implications and concerns associated with the CT Travel Programme and its promulgation of goTravel. The position paper demonstrates how UNOCT and its UN implementing partners appear to be failing to adequately mainstream human rights in the development of the underlying system for collection, use, and sharing of API/PNR data, and how the system which is now being rolled out internationally at pace, risks squarely contravening international law, particularly international human rights law, in multiple respects.

7. This position paper proceeds in four parts. Part I provides a brief factual overview of how API and PNR systems work. Part II sets out the normative and legal framework applying to API and PNR collection and transfer at the international level. Part III explains how UNOCT and its UN implementing partners promote such systems through the CT Travel Programme and the provision of the goTravel software program. Part IV considers the clear human rights concerns arising from the CT Travel Programme and goTravel. The Special Rapporteur concludes by recommending that the roll-out of CT Travel Programme and goTravel be paused, and reiterating the urgent need, especially whenever United Nations organs seek to collaborate and support State agencies, to ensure compliance with international human rights law through the rigorous analysis of human rights impacts from the outset and at the design stage rather than, as is all too often the case, as a cursory – and ineffective – afterthought.

Part I: API and PNR

8. API and PNR are, broadly speaking, both types of datasets originally developed by commercial air carriers to streamline their operations and border management at airports.

a) API

9. **API data are the more basic of the two forms, consisting of data which identifies the individual traveller themselves**. This information comprises the traveller's name, date of birth, gender, citizenship or nationality, the country of issue of the traveller's identity document(s), and the specific flight details. API is typically captured from the Machine Readable Zone ('MRZ') of the traveller's passport, and is typically required by airlines to be provided well in advance of travel via the carrier's online platform. API is typically transmitted to the authorities of the arrival country either by way of batch notification (whereby a single manifest for an entire flight is transmitted shortly before departure) or by interactive API system ('iAPI'), which provides each individual traveller's API data separately upon their individual check-in.

10. The primary function of API data in the counter-terrorism context is to allow for the matching of travellers against international or domestic watchlists, allowing for identification of suspects and/or refusal of travel.

b) PNR

11. **PNR data are significantly more expansive in scope than API.** 'PNR' is an umbrella term to cover a wide array of information about air passengers far beyond the mere identity. Originally developed by the International Air Transit Association ('IATA') – the trade association of the world's airlines – as a means to exchange information between carriers regarding passengers needing to be transferred throughout different legs of a multi-stage journey, PNR data are the data which have been entered into the computer system of the carrier or booking operator. PNR typically includes not only identity information, but also a full suite of information relating to the circumstances of the particular trip, including the date of reservation, the passenger's billing address and contact details, travel agency details, baggage information, itinerary information (including co-travellers and journey), and flight-specific information (ticket and seat numbers, dietary preferences, frequent flyer details). In respect of each category, too, there may be multiple specific details. For instance, 'baggage information' may entail details on the total number of pieces of checked and/or carry-on baggage, the weight of those items, the pooled baggage indicator (that is, identification of any other baggage checked at the same time), baggage tag number and any linked tagged numbers.[5]

12. In addition to wider scope, the key difference between API and PNR data is that PNR data mainly depends upon that which the person making the booking has directly provided either online or at a travel agent,[6] whereas API data are automatically harvested from the traveller's official travel document(s). PNR data are typically transmitted twice, at two different time intervals, prior to departure to the authorities of the arrival State.

13. **As compared with API data, the potential use of PNR data in counter-terrorism contexts is much more complex.** Assessment of PNR data has been claimed by the European Union, for instance, to *'allow identification of persons who are unsuspected of involvement in terrorist offences or serious crime prior to such an assessment and who should be subject to further examination by the competent authorities*.'[7]

14. Accordingly, while the collection and use of API (that is, basic identity) data is chiefly about matching individuals to pre-existing watchlists at the point of travel, the collection and use of PNR data is more about using the expansive data harvesting opportunity which international travel affords (which leaves a trail of data about identity, contacts, individuals' sources of funds, etc) to feed that data into counter-terrorism prediction, prevention, and investigation.

Part II: The Legal Framework for API and PNR Collection and Transfer

15. Given its necessarily international nature, the need for global co-operation and regulation of air travel was recognized early, with the Convention on International Civil Aviation (the 'Chicago Convention') signed in 1944 to establish a global regulatory framework,

5 As noted in A Priestley and M Beauvais, 'International Experience and Good Practices in API/PNR,' OSCE (2021), p6.

6 Ibid., p5.

7 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offence and Serious Crime, OJ L 119, 4 May 2016 ('PNR Directive'), pp132-149, Recital (7).

including the foundation of the ICAO. The ICAO, subsequently incorporated as an agency of the UN in 1947, has since had a leading role in coordinating international law-making via robust multi-lateral negotiations on important topics in civil aviation. The international community agreed landmark treaties to deal with criminal offences committed on board aircraft[8] and, following the growth in aircraft hijackings in the late 1960s, the Montreal Convention of 1971.[9] Under these models, standards agreed following consideration at the international level were then implemented via national legal and regulatory frameworks.

16. Following the September 11 terrorist attacks, however, international law-making with respect to criminal conduct relating to aviation has tended to be promoted via the law-making frameworks employed for counter-terrorism, but internationally and domestically. Various States,[10] regional entities,[11] and the United Nations Security Council have taken a range of steps aimed at intercepting would-be terrorists and other criminal actors during attempted transit.

17. Security Council Resolution 2178 (2014) drew attention to individuals who *'travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.*'[12] That Resolution called upon States, in an attempt to address this phenomenon, to require[13] the provision by airlines of API data of air passengers generally *'in order to detect*' travel or attempted travel by individuals designated by the Security Council Committee overseeing the sanctions against Al-Qaida (and, later, ISIL).[14] In doing so, the Security Council made clear that the collection of API and its sharing between States must occur *'in accordance with domestic law and international obligations*.'[15]

18. The Security Council repeated that commitment in Resolution 2309 (2016),[16] and at the same time reaffirmed the need for measures taken to combat terrorism to comply with international law *'in particular international human rights law, international refugee law, and international humanitarian law*.'[17]

19. Thereafter, the ICAO Council adopted amendments to the Standards and Recommended Practices ('SARPs') under Annex 9 of the Chicago Convention urging States to establish

8 ICAO, Convention on Offences and Certain Other Acts Committed on Board Aircraft, (1969) UNTS 219 (opened for signature, 14 September 1963, entry into force, 4 December 1969).
9 ICAO, Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, (1975) 974 UNTS 177 (opened for signature, 23 September 1971, entry into force, 26 January 1973).
10 An early mandatory requirement in relation to API data, albeit at the domestic level only, was introduced in the United States: 49 United States Code §44909(c)(3), and the implementing regulations at 19 Code of Federal Regulations §122.49d.
11 The European Union adopted its first API legislation in 2004: Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6 August 2004, pp24-27 ('API Directive').
12 S/RES/2178 (2014), p2.
13 S/RES/2178 (2014), [9].
14 The Committee having been established pursuant to Resolutions S/RES/1267 (1999) and S/RES/1989 (2011).
15 S/RES/2178 (2014), [9].
16 S/RES/2309 (2016), [6].
17 S/RES/2309 (2016), p2.

API systems in line with internationally-recognized standards and to consider the introduction of iAPI.[18]

20. In the following updated Resolution 2396 (2017),[19] the Security Council decided that, as envisaged by the ICAO Council, Member States should require that airlines operating in their territories to provide API to national authorities as a means to detect and monitor terrorists and sanctioned individuals.[20] Resolution 2396 (2017) went further, deciding also that Member States *'shall develop the capacity 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, will full respect for human rights and fundamental freedoms, for the purpose of preventing, detecting and investigating terrorist offenses and related travel*.'[21] In doing so, the Security Council specifically called upon *'Member States, the UN, and other international, regional, and subregional entities to provide technical assistance, resources and capacity building to Member States in order to implement capabilities, and, where appropriate, encourages Member States to share PNR data with relevant or concerned Member States*…'[22] At the same time, the Resolution underscored *'that respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures, and are an essential part of a successful counter-terrorism effort*…'[23]

21. Finally, in 2019 Security Council Resolution 2482 (2019) moved from urging the *development* of API and PNR capabilities, to calling upon Member States to *'implement obligations to collect and analyse*' API and further '*develop the ability to collect, process and analyse*' PNR data in line with ICAO technical standards.[24] In addition, Resolution 2482 greatly liberalized the purposes for the data collection and analysis effort. Instead of the identification of designated terrorists on UN sanctions lists, the wider rationale deployed by the Security Council was to *'help security officials make connections between individuals associated to organized crime, whether domestic or transnational, and terrorists, to stop terrorist travel and prosecute terrorism and organized crime, whether domestic or transnational*…'[25] The Security Council made clear that the efforts of Member States in relation to API and PNR must *'comply with all their obligations under international law, in particular international human rights law, international refugee law, and international humanitarian law*'[26] and must occur *'with full respect for human rights and fundamental freedoms*.'[27]

22. These developments at the level of the UN Security Council have been augmented by a range of further international and regional commitments. The European Union introduced

---

18 Via Amendment 26 to Annex 9 of the Chicago Convention, effective in October 2017 and applicable from 23 February 2018.
19 S/RES/2396 (2017).
20 S/RES/2396 (2017), [11].
21 S/RES/2396 (2017), [12].
22 S/RES/2396 (2017), [12].
23 S/RES/2396 (2017), p1.
24 S/RES/2482 (2019), [15(c)].
25 S/RES/2482 (2019), [15(c)].
26 S/RES/2482 (2019), p2.
27 S/RES/2482 (2019), [15(c)].

mandatory obligations on air carriers to collect and provide PNR data to State agencies in 2016,[28] and the ICAO adopted revised standards governing systems for collection, processing, and transfer of API and then PNR which became binding in 2018[29] and 2021 respectively.[30]

23. The key features of normative framework laid down by the Security Council therefore include that Member States should require air carriers to collect and provide API and PNR data from travellers prior to check-in, which may then be passed to State agencies known as Passenger Information Units ('PIUs') for the specific purposes of identifying and preventing the travel of known and suspected terrorists and/or serious criminals. The Security Council's broad guidance does not stipulate specific methods of giving effect to these obligations, other than by way of cross-reference to the ICAO's largely technical standards, **but does make very clear that all steps taken in furtherance of the Security Council's objectives must comply with international law, including in particular international human rights law, international refugee law, and international humanitarian law.**

24. The collection of personal information contained in API and PNR datasets and its use and transmission with respect to decision-making at international borders clearly entails various established international legal obligations of States including their obligations to respect individuals' right to privacy,[31] other civil rights (particularly to free expression,[32] political participation,[33] freedom of assembly,[34] association,[35] and religion),[36] and the free movement rights of persons to leave any country,[37] to return to their country of nationality,[38] and to seek asylum.[39]

25. The human rights risks raised by the collection and processing of PNR data, and the transfer of PNR data internationally, have already been specifically considered at the regional level by the Court of Justice of the European Union ('CJEU'). The Special Rapporteur considers that this jurisprudence is a useful resource for identifying how systems for the collection, analysis, and transfer of personal data like API and PNR may be operated in a rights-

---

28 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offence and Serious Crime, OJ L 119, 4 May 2016 ('PNR Directive'), pp132-149.

29 Via Amendment 26 to ICAO Annex 9, applicable from 23 February 2018.

30 Via Amendment 28 to ICAO Annex 9, applicable from 28 February 2021.

31 United Nations General Assembly, International Covenant on Civil and Political Rights, (1966) 999 UNTS 171 (opened for signature, 16 December 1966, entry into force, 23 March 1976) ('ICCPR'), Article 17; and Universal Declaration of Human Rights ('UDHR'), Article 12.

32 ICCPR, Article 19; UDHR, Article 19.

33 See: UDHR, Article 21; and Human Rights Committee ('HRC'), *Gauthier v Canada,* UN Doc. CCPR/C/65/D/633/1995, [13.4]; and *Aduayom, Diasso and Dobou v Togo,* UN Doc. CCPR/57/D/422-4/1990, [7.4]

34 ICCPR, Article 21; UDHR, Article 20.

35 ICCPR, Article 22; UDHR, Article 20.

36 ICCPR, Article 18; UDHR, Article 18.

37 ICCPR, Article 12(2).

38 ICCPR, Article 12(4); and A/RES/76/172 (10 January 2022).

39 UDHR, Article 14.

respecting fashion, and the key limitations and safeguards to which such systems should be subject.

26. The CJEU struck down the initial design of arrangements for sharing PNR data between the EU and the United States[40] and Canada,[41] the former for constitutional reasons that sharing arrangements had been adopted under the Union's commercial and trade competence, rather than security, competence,[42] and the latter because of non-compliance with EU fundamental rights to privacy and the protection of personal data.[43] Agreements compliant with EU have subsequently been struck with the United States (in revised form)[44] and Australia.[45]

27. The scope of the EU PNR regime itself was further called into question via references for preliminary ruling from the Belgian[46] and German courts[47] regarding national implementing legislation for the EU system. Those cases pointed to the indiscriminate nature of mandatory PNR data collection – and its compulsory storage for years – without any distinction, differentiation, or limitation by reference to the level of significance of any particular individual's data to the legitimate objective of protecting national security. The decision in the Belgian case was delivered in June 2022,[48] with the German references brought to an end without determination after the Belgian decision.[49]

28. In the Belgian case, the CJEU set out strict limitations which must apply in transposing and applying the PNR Directive in domestic law throughout the EU, significantly narrowing the ways in which EU Member States may lawfully process PNR data. The European Data Protection Board has concluded that as a result it is likely that the current processing of PNR data *'in many, if not most Member States'* does not comply. As a consequence, *'PNR*

40 Joined Cases C-317/04 and 318/04 *Parliament v Council* ECLI:EU:C:2006:346 (*'Parliament v Council*').

41 Advisory Opinion 1/15 *Opinion on Draft Agreement between Canada and the European Union on the Transfer and Processing of Passenger Name Record Data* ECLI:EU:C:2016:656 (*'Canada-EU Advisory Opinion*'). For a response to the Canada-EU Advisory Opinion, see A Vedaschi, 'Privacy and Data Protection Versus National Security in Transnational Flights: The EU-Canada PNR Agreement' (2018) 8(2) *International Data Privacy Law* 124.

42 *Parliament v Council*, [54]-[61] and [67]-[70].

43 *Canada-EU Advisory Opinion*, [328(3)].

44 'Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security,' OJ L 215, 11 August 2012, pp5-14.

45 'Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service,' OJ L 186, 14 July 2012, pp4-16.

46 Case C-817/19 *Ligue des Droits Humains v Conseil des Ministres*, OJ C 36, 3 Feburary 2020, pp16-17.

47 Joined Cases C-148/20, C-149/20, C-150/20 *AC v Deutsche Lufthansa AG*, OJ C 279, 24 August 2020; and Joined Cases C-215/20 and C-222/20 *JV and OC v Bundesrepublik Deutschland*, 19 May 2020.

48 Case C-817/19 *Ligue des Droits Humains v Conseil des Ministres* ECLI:EU:C:2022:491 (*'Ligue des Droits Humains*').

49 Joined Cases C-148/20, C-149/20, C-150/20 *AC v Deutsche Lufthansa AG*, Order of 9 August 2022; and Joined Cases C-215 and C-222/20 *JV and OC v Bundesrepublik Deutschland*, Order of 22 August 2022.

systems across the EU may continue to interfere disproportionality with the fundamental rights of data subjects every day.'[50]

29. The conclusions of the CJEU, as a competent Court interpreting modern ICAO-compliant PNR systems against the requirements of the right to privacy,[51] are instructive:

    29.1. First the CJEU recognized that the collection and processing of PNR data was *prima facie* an interference with privacy rights;[52]

    29.2. The consequence of that is that, for such collection and processing to qualify as lawful, it must *only be carried out* for the purposes of *preventing and investigating terrorism and serious criminal offences*[53] (which accords with the stated bounds of API and PNR use as set down by the Security Council);[54]

    29.3. Those lawful purposes for processing of PNR must be given effect by reference to pre-determined non-discriminatory criteria which are reviewed regularly so as to minimize false positives;[55]

    29.4. If a Member State indiscriminately uses PNR data for other purposes, including investigating less serious crime, or applies insufficiently restrictive criteria, that would be unlawful by virtue of going beyond what is strictly necessary;[56]

    29.5. The processing and analysis of PNR data may not employ artificial intelligence or self-learning systems since, *'given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match*;'[57] and

    29.6. Any transfer and use of PNR data for investigative purposes subsequent to persons' actual travel should be subject to prior judicial review and may only be permitted on the basis of new circumstances or objective evidence suggesting a reasonable suspicion of the data subject's involvement in serious crime.[58]

30. **It is against this legal backdrop, then, including the legitimate objectives for API and PNR use set down by the Security Council, and the substantive restrictions upon the collection, analysis, and transfer of such data implied by international law,**

---

50 Statement 5/2022 on the implications of judgment C-817/19 regarding the implementation of the Directive (EU) 2016/ on the use of PNR in MS, adopted 13 December 2022: https://edpb.europa.eu/system/files/2022-12/edpb_statement_20221213_on_the_pnr_judgement_en.pdf

51 European Union, Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012, pp391-407, Article 7.

52 *Ligue des Droits Humains*, [111].

53 *Ligue des Droits Humains*, [141]ff.

54 See: S/RES/2178 (2014), [9]; S/RES/2309 (2016), [6]; S/RES/2396 (2017), [12]; and S/RES/2482 (2019), [15(c)].

55 *Ligue des Droits Humains*, [193]-[201].

56 *Ligue des Droits Humains*, [173].

57 *Ligue des Droits Humains*, [194].

58 *Ligue des Droits Humains*, [218]-[220].

particularly human rights law, that the CT Travel Programme and the goTravel software solution fall to be considered.

Part III: The CT Travel Programme and goTravel

31. The worldwide implementation of systems to collect and share API and PNR data is far from uniform. A limited number of countries (including the United States, the UK, France, Germany, Turkey, Japan, Saudi Arabia, Brazil, and Indonesia) have operational API and PNR systems in place, but a number of large countries (including Russia, China, India, South Africa, Spain, Italy, Colombia, and Argentina) only have an API system. Further, substantial parts of the world (Central Asia, much of the Middle East, and almost every African nation) have neither system in place as yet.

32. In that context, the United Nations, led by UNOCT, sought to address inconsistent international adopt of API/PNR systems via the CT Travel Programme, launched in 2019 with assistance from the UN Global Counter-Terrorism Compact Partners.[59] While UNOCT has repeatedly described the CT Travel Programme as an 'All-of-UN' partnership, two of the agencies most directly concerned with the rights of individuals in the border management context, namely the United Nations High Commissioner for Refugees ('UNHCR') and the Office of the High Commissioner for Human Rights ('OHCHR'), were not identified as partners in the programme at its launch, and the Special Rapporteur understands that those agencies were not substantively involved in the programme's development or initial roll-out.

33. In this regard, and despite the Special Rapporteur having been provided by UNOCT with certain documents (not publicly available) relating to the implementation of the CT Travel Programme, the Special Rapporteur is concerned that it also remains unclear the degree to which UN entities with a lead role in human rights protection have subsequently been involved in the further development and expansion of the programme. The Special Rapporteur notes, for instance, that a March 2023 evaluation of the CT Travel Programme – which endorsed the programme without reservation – was carried out by three consultants jointly engaged by UNODC and UNOCT.[60] Given the clear impact of the programme on human rights protection, the Special Rapporteur would have expected that any review should have been fully independent – not conducted via consultants engaged by two of the implementing partners responsible for the project itself – and should have involved OHCHR, UNHCR, UN Special Procedures, and/or a panel of experts well-known in the field of technology, counter-terrorism, and human rights.[61]

34. The CT Travel Programme is designed to support States, *inter alia*, to draft relatively uniform legislation on the collection, transmission, use, retention, and sharing of API/PNR,

---

59 See: https://www.un.org/cttravel/

60 UNOCT and UNODC, 'Mid-Term Independent Joint Evaluation: United Nations Countering Terrorist Travel Programme' (March 2023) ('Joint Evaluation'), available at: https://www.unodc.org/documents/evaluation/indepth-evaluations/2023/Midterm_Joint_Evaluation_Report_UN_Countering_Terrrorist_Travel_Programme.pdf

61 The Special Rapporteur notes with regret that her mandate was not consulted in respect of this March 2023 evaluation.

and to establish national PIUs (including through the provision of training and ongoing mentorship). The centrepiece of the CT Travel Programme is the provision of the goTravel software program which, by virtue of the favourable terms (free provision for a two-year trial period, followed by a means-tested licence fee)[62] and the infancy of many countries' capacity, is likely to become the international default technical system for the collection and transfer of API and PNR datasets.

35. The goTravel software program itself was first developed by the Netherlands[63] and donated to the UNOCT in September 2018. It is intended to operate as a uniform, interoperable, secure system which allows for the seamless input of API (currently only in batch form)[64] and PNR data from air carriers, and the efficient provision of those datasets to departure and arrival State PIUs and law enforcement agencies for analysis.

36. As of October 2023, two States – Norway and Botswana – have fully implemented the goTravel software program as the means by which carrier-collected API and PNR data are communicated to those States' PIUs.[65] A further 65 Member States are in negotiation for future implementation.[66] Remarkably, this list includes Sudan,[67] which has long been subject to sanctions imposed by the UN Security Council preventing the provision of arms to entities including the government due to serious concerns regarding violations of international humanitarian law and human rights law.[68]

a) Uses of API and PNR

37. The stated purpose of the data processing which goTravel facilitates is two-fold. First, to identify persons who have already been recognized in connection with terrorist offences or serious crimes,[69] including by way of international watchlists or equivalent systems like the Interpol Red Notice system.[70] Second, to identify persons who *may* foreseeably be of interest in relation to such crimes. To that end, the software facilitates the direct transfer of API/PNR data from airlines and other commercial operators to the relevant PIU, where it is stored centrally (but accessible to various national agencies according to each State's domestic arrangements).[71] **After data records are received, national PIUs (and national**

62 See: https://www.un.org/cttravel/faq
63 As a system then known as the Travel Information Portal. The Special Rapporteur recognizes that the Netherlands has a strong record of active engagement with efforts to protect and promote human rights while countering terrorism, including its support to the active participation of civil society in counter-terrorism decision making particular in the New York security arena.
64 As opposed to interactive API ('iAPI'), which provides each individual traveller's API data separately upon their individual check-in.
65 See: https://www.un.org/cttravel/goTravel
66 See: https://www.un.org/cttravel/goTravel
67 S/RES/1591 (2005).
68 Two further Member States in negotiation with UNOCT for future implementation of goTravel (the Democratic Republic of Congo ('DRC') and Mali) are subject to Security Council sanctions regimes, but the chief provisions of those regimes apply to non-State actors and individuals. See, in respect of the DRC, S/RES/1533 (2004) as modified by S/RES/2293 (2016), and, in respect of Mali, S/RES/2374 (2019) and S/RES/2649 (2022).
69 See: 'goTravel FAQ, 3.2 and 3.4,' available at: https://www.un.org/cttravel/faq
70 See: 'goTravel FAQ, 3.10,' available at: https://www.un.org/cttravel/faq
71 See: 'goTravel FAQ, 3.3,' available at: https://www.un.org/cttravel/faq

agencies accessing PIU-held data) can profile the data against nominated 'risk indicators.'[72] This allows for identification of persons who are not existing persons of interest or subject to watchlisting/Red Notices, but whose travel behaviour corresponds to markers flagged via nationally-operated pattern- or link-analysis systems. Such pattern- or link-analysis is typically carried out automatically, covering all provided passenger data. Because the risk categories are applied by each State's PIUs (or national agencies accessing PIU data) rather than pre-coded in the API/PNR data collected, UNOCT can impose no prior fetter on the type of analysis carried out. **As a consequence, domestic authorities undertake these analyses in the manner of their choosing.** Further, they are under no obligation to report to UNOCT the criteria or methodology applied. While the goTravel platform provided by the UN will underpin Member States' use of API/PNR data for their own purposes, no current system is in place to address how the UN observes or controls that use by Member States.

38. **Future updates of the goTravel software are anticipated to support artificial intelligence ('AI') and machine and deep learning algorithms to analyse behavioural patterns to highlight previously unidentified individuals of interest,**[73] to integrate iAPI data, as well as to widen the net of data collection to include maritime, international high-speed rail, and coach travel.[74]

b) Data Handling and Retention

39. The goTravel program operates a default storage period of 5 years for API and PNR data, albeit that personal details are described as 'masked out' of the dataset after 6 months.[75] That means that each national PIU is entrusted with the task of removing names, address, and contact information, payer information, and frequent flyer information capable of directly identifying individual travellers. That depersonalization process (even assuming it is completed uniformly by PIUs) is not equivalent to full anonymization,[76] since depersonalized datasets may still be re-identified by comparison with other datasets held at the national level. Further, domestic law may provide exemptions, as contemplated by the EU PNR Directive, which would allow for disclosure of full API/PNR data outside the initial 6-month retention period at the order of judicial or other competent national authorities as defined by domestic legislation.[77]

---

72 See: 'goTravel FAQ, 3.1,' available at: https://www.un.org/cttravel/faq
73 See: 'goTravel FAQ, 3.8,' available at: https://www.un.org/cttravel/faq
74 See: 'goTravel FAQ, 2.3 and 3.11,' available at: https://www.un.org/cttravel/faq
75 See: 'goTravel FAQ, 2.4,' available at: https://www.un.org/cttravel/faq
76 In IT security practice, there is a different between full 'anonymisation' of data and 'pseudonymisation,' with the latter subject to a heightened residual risk of re-identification of the dataset. As datasets become more ubiquitous, however, re-identification of individuals even from anonymised data (by way of matching with non-anonymous datasets sharing correlations) is an increasing risk such that even typical anonymisation processes cannot be guaranteed to be effective for the long term. For a discussion, see: European Data Protection Supervisor, '10 Misunderstandings Related to Anonymisation,' available at: https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf. For a technical explanation, see: A Farzanehfar et al., 'The risk of re-identification remains high even in country-scale location datasets,' (2021) 2 *Patterns*, 100204.
77 EU PNR Directive, Recital (25) and Articles 12(3) and 12(5).

40. Just as retention periods are governed by domestic rules (subject to a backstop capacity of the software), the mechanics of data handling and security depend upon the domestic infrastructure managed by individual State PIUs. While UNOCT has described transmission from carriers to PIUs as *'via secure connection and B2B protocol*' and the goTravel program as *'hosted in the secure network of a Member State country*,'[78] and while technical assistance is provided to States via the UN OICT, **the reality is that the security or otherwise of the API and PNR data collected by, and transferred between, States remains vulnerable to any security weaknesses at the domestic level, since the system is decentralized between States.** Accordingly, the integrity of the system and the data accessed through is only as secure as its weakest link. Security vulnerabilities at the level of Member States – such as vulnerabilities to cyberattacks or overthrow of governments[79] – place personal identifying information at real risk.

c) Unknown Reliability

41. **The goTravel software is an experimental software program which, to the Special Rapporteur's knowledge, has never been subject to formal review in respect of its accuracy rate in identifying named individuals, much less the accuracy of its use in any risk-based profiling system**. With billions of air travellers every year, even a miniscule error rate of a tenth of one percent would mean millions of false positives/negatives.

42. Of course, with respect to risk-based profiling, experience suggests that PIU systems using data provided via the goTravel program will involve much more substantial inaccuracy. In Germany, for instance, the government has estimated a success rate of only 0.1% of identifying potential terrorists through algorithmic profiling of incoming passengers, which means that 99.9% of all air travellers (about 170 million people a year) are unnecessarily subject to enhanced border screening.[80] Analysts have proposed that a fundamental limitation upon the accuracy of algorithmic profiling of terrorist suspects is that terrorism is an extremely rare event, however narrowly-defined the population identified as displaying relevant correlated variables may be.[81] **In short, methodological generalization is unlikely to be dependable, as the amount of data is too small,[82] meaning that the algorithm cannot be sufficiently trained for accuracy, with the result of its attempts at pattern recognition being over-identification and/or under-identification.**

---

78 See: https://www.un.org/cttravel/goTravel

79 The Special Rapporteur notes with concern that the government of one of the 63 Member State applicants for goTravel – Mali – has recently been deposed by way of a military coup. The vulnerability of government systems worldwide to such events is a factor which those designing and supplying systems to share data internationally are obliged reasonably to anticipate.

80 B Moini, 'Against Mass Surveillance of Air Passengers,' *Digital Freedom Fund Blog* (26 March 2020), available at: https://digitalfreedomfund.org/against-mass-surveillance-of-air-passengers/

81 B Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (2007).

82 A Mackenzie, 'The Production of Prediction: What Does Machine Learning Want?' (2015) 18(4-5) *European Journal of Cultural Studies* 429.

43. As one researcher has put it: *'While there appear to be some discernible trends in characteristics common to terrorists, the tiny number of terrorists within the general population renders broad characteristics based on profiling of no predictive value*.'[83] In other words, while hindsight is capable of discerning some generally common data points shared by terrorists, the degree to which those data points are shared by non-terrorists alike means that profiling based on such data points provides no meaningful predictive worth – inconveniencing (at least) hundreds of millions of innocent people while identifying only some potential terrorists (only until, of course, such potential terrorists change their behaviour to minimize even that marginal statistical risk), and potentially opening up a much more sizeable group of persons to government intrusion and intervention.

Part IV: Human Rights Concerns

a) Overview

44. The provision of API and PNR data capacities to dozens of governments worldwide via the CT Travel Programme and its goTravel software platform provides national authorities with access to the personal data of vast numbers of travellers which those authorities may use for their own purposes purportedly in pursuit of counter-terrorism and national security objectives. **But the data collection and sharing system being promoted by the UN implementing partners does not build in or guarantee the sort of clear limitations on the purpose and function for which API and PNR data may be used which international human rights law demands**.

45. **As a result, malign or unaccountable use by State agencies cannot be excluded**. Further, even *bona fide* use for counter-terrorism or national security purposes entails obvious risks to human rights of privacy, free expression and associated rights, and rights of movement and asylum, chiefly through disproportionate application and inadequacy of individual remedies. Granting such a powerful tool to governments requires careful human rights planning and rigorous structures which ensure that control over the API and PNR data and its use is retained, foreseeable misuse can be prevented, and instances of unavoidable misuse can be readily sanctioned. **The Special Rapporteur has been unable to verify that the CT Travel Programme and the roll-out of the goTravel software program currently display such features.** On the contrary, the Special Rapporteur is concerned that the effort appears a rushed attempt by the UN to promulgate new technology for counter-terrorist purposes without sufficient human rights analysis, in direct breach of UN due diligence requirements and apparent defiance of contemporaneous human rights jurisprudence from international courts.

b) No Inherent Value in the Status Quo

46. The ubiquity of API and PNR collection processes as part of modern commercial air travel, their clear theoretical utility for law enforcement and border control, and the enthusiasm with which States have received offers of cooperation and assistance under the CT Travel

[83] K McKendrick, 'Artificial Intelligence Prediction and Counterterrorism,' Chatham House Research Paper (August 2019), p18.

Programme ought not to displace the need to interrogate the status quo. It is important to recognize from the outset that the CT Travel Programme and its centrepiece —the goTravel software—are not the product of considered inter-State and multi-agency negotiation on agreed requirements and safeguards, but rather entail the opportunistic co-opting of air carrier API and PNR protocols to serve counter-terrorism and security purposes for which those commercial passenger datasets were never originally devised.

47. Prior to, and aside from, the UN Security Council's Resolutions, API and PNR datasets were creations of convenience by air carriers, and the guidance recommending their adoption is in the nature of 'soft law' – that is, non-binding guidance which became normalized in State patterns of behaviour. **The Security Council Resolutions calling upon States to implement obligations regarding API and PNR collection and analysis do not explicitly necessitate an open-ended worldwide framework for data collection and sharing such as that envisaged by the UN implementing partners and promoted via the CT Travel Programme and goTravel software program**. On the contrary, the purposive limits placed on data collection by the most recent Security Council Resolution 2482 (2019) – collection and use to *'help security officials make connections between individuals associated to organized crime … and terrorists, to stop terrorist travel and prosecute terrorism and organized crime*' – could certainly be satisfied by more targeted data collection. That said, definitions of *'organized crime*' and *'terrorism*' and associated terms differ among Member States. While the Security Council itself has previously promoted a limited definition of terrorism,[84] the Special Rapporteur has consistently expressed the concern that, in the absence of any international consistency in the manner in which Member States define of terrorism, there remains extraordinary leeway for arbitrary and unjustified action by State authorities using purported counter-terrorism as a pretext.[85] While the Special Rapporteur has advocated a precise and tightly-defined model definition of terrorism, few States have adopted the same.[86]

48. **The current worldwide API and PNR collection and sharing system envisaged and facilitated by the CT Travel Programme is therefore not a system which has been developed at the international level with multi-agency input as part of a through-composed strategy balancing legitimate counter-terrorism aims against necessary and proportionate restrictions on human rights.** The implementation of the Security Council's imperative to address travel of foreign fighters and support API/PNR use must involve a proper working-through of how such systems can be implemented consistent with the UN Charter and international law, rather than an assumption on the part of Member States and others that the current technical systems used by commercial airlines are inarguably fit for legal purpose. If the use of API and PNR cannot fully be operated in a human rights compliant manner, it should be reformed, rather than adopted simply because doing so would represent the path of least resistance.

---

84 S/RES/1566 (2004), [3].

85 In response to the OHCHR Call for Inputs prior to the 'Right to Privacy in the Digital Age' report. See the Special Rapporteur's response at: https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf

86 A/HRC/16/51, [28].

c) Absence of Evidenced Due Diligence on goTravel Recipients

49. A central concern with respect to the roll-out of the CT Travel Programme and goTravel system is that it appears to the Special Rapporteur that insufficient human rights due diligence has been, or is being, conducted with respect to recipients of the goTravel software (and the access it provides to vast amounts of personal data). UNOCT has stated that, as part of its initial assessment of the needs of recipient States, *'human rights considerations are an integral part of the overall deep-dive assessment*' of such recipients.[87] UNOCT further states[88] that the CT Travel Programme *'follows the requirements*' contained in the UN Human Rights Due Diligence Policy ('the HRDDP').[89]

50. **The Special Rapporteur has not been a party to any such *'deep-dive assessments*.' The involvement of experts from OHCHR or UNHCR in these assessments is also unclear, as is the degree to which the *'deep-dive*' assessments comply with the HRDPP and adequately consider the various human rights implications of sharing API and PNR datasets by way of goTravel with recipient States.**

51. The HRDDP applies, *inter alia*, whenever UN agencies provide technical[90] or programmatic support[91] to national forces including border control or the civilian departments overseeing such forces,[92] **and is acknowledged by UNOCT to apply to the CT Travel Programme**. The HRDDP imposes stringent requirements to ensure that UN support for Member State agencies is not inadvertently complicit in adverse human rights outcomes. These requirements include the mandatory obligation to conduct a risk assessment considering, *inter alia*: the record of the recipients in terms of compliance or non-compliance with international humanitarian, human rights, and refugee law; (b) the record of the recipients in taking or failing to take effective steps to hold perpetrators of violations accountable; (c) whether corrective measures have been taken to prevent the recurrence of violations, and the adequacy of such measures; (d) an assessment of the degree to which providing or withholding support would affect the UN's ability to influence the behaviour of the recipient entity; (e) the feasibility of the UN putting in place effective mechanisms to monitor the use and impact of the support provided; and (f) an assessment on the basis of these factors and the overall context of the risk that the receiving entity might nevertheless commit grave violations of international humanitarian, human rights, or refugee law.[93] **A United Nations agency is only entitled to pursue support for a Member State agency if the risk assessment concludes that no substantial grounds exist for believing there to be a real risk of the intended recipient committing such violations.[94]**

87 See: https://www.un.org/cttravel/news/un-countering-terrorist-travel-programme-and-human-rights
88 Ibid.
89 General Assembly, 'Human Rights Due Diligence Policy on United Nations Support to Non-UN Security Forces,' UN Doc. A/67/775-S/2013/110 (5 March 2013) ('HRDDP').
90 HRDDP, [8(a)].
91 HRDDP, [8(b)].
92 HRDDP, [7(a)-(b)].
93 HRDDP, [14].
94 HRDDP, [17].

52. Aside from the HRDDP and more generally, it is a basic principle of the UN Global Counter-Terrorism Strategy that any measures taken by Member States (and those promoted by UN entities for Member State adoption) must fully comply with international law, in particular international human rights law, international refugee law, and international humanitarian law.[95] As the Special Rapporteur has previously observed, the expansion of UN technical assistance to Member States in the field of counter-terrorism must be matched by a comparable mainstreaming of human rights within such programmes, which is now, in her view, generally lacking.[96]

53. The information released to the Special Rapporteur regarding the *'deep-dive'* assessment undertaken prior to the initiation of cooperation with Member States, and the provision of CT Travel Programme support including the goTravel program, currently provides insufficient grounds for confidence that the risk assessment obligation has properly been discharged. The structure of these *'deep-dive*' assessments is that representatives from the recipient State agencies are invited to discuss (often by way of videoconference)[97] their system requirements with technical experts from UNOCT, UNODC, ICAO, OICT, and Interpol, rather than UN agencies being tasked with initiating investigations or obtaining information Member States do not wish to divulge. **It appears *prima facie* unlikely that searching examination of human rights risks posed by recipient States agencies' potential misuse of personal data in fact forms part of the exercise as it should**.

54. The Special Rapporteur is aware that, pursuant to the UN CT Travel Programme: Programme Action Plan, a three-step human rights due diligence process is contemplated, involving: (a) considering human rights concerns at the CTED-led assessment and selection stage of identifying potential recipient States; (b) provision of human rights advice to recipient States as they draft legislation, as well as institution-building support and training; and (c) receipt of assurances from recipient States prior to handing over the goTravel software. The Special Rapporteur is aware that, on an ad hoc basis, implementing partners may request a briefing from the OHCHR with respect to human rights concerns with potential recipient States. The Special Rapporteur understands that such briefings often involve analysis of the legislative and institutional capacity of the potential recipient State, as well as a review of the State's human rights record. The Special Rapporteur understands that that such analysis does not extend to involving human rights experts in direct negotiations or investigations of how potential recipient States intend practically to operate their API/PNR systems, or that human rights experts are granted any ongoing role to ensure compliance.

55. Further, the Special Rapporteur acknowledges that UNOCT has shared with the Mandate a technical questionnaire (not otherwise publicly available) which indicates that information

---

95 General Assembly, 'The United Nations Global Counter-Terrorism Strategy: Eighth Review,' A/RES/77/298 (3 July 2023), pp2-3.

96 See: A/76/261.

97 See, for instance, the virtual deep-dives in respect of Djibouti, Côte d'Ivoire, Botswana, Sierra Leone, and the Gambia: https://www.un.org/securitycouncil/ctc/news/cted-leads-virtual-deep-dive-assessment-mission-djibouti, https://www.un.org/securitycouncil/ctc/news/cted-leads-two-virtual-deep-dive-assessment-missions-côte-d'ivoire-and-botswana, and https://www.un.org/securitycouncil/ctc/news/cted-leads-virtual-deep-dive-assessment-missions-sierra-leone-and-gambia

is sought from prospective recipient States on a range of matters to gauge the States' institutional, legal, ICT, and operational readiness for the collection and receipt of API/PNR data. The structure of the questionnaire asks Member States to provide answers to enquiries about capabilities and the integrity of legal frameworks. The Special Rapporteur has been unable to verify the degree to which the reliability of those answers is further interrogated, and, specifically, to what extent UN agencies engaging with Member States have independent powers to investigate and assess matters. It does not appear that information is directly sought from other essential stakeholders including civil society or human rights experts in-country.

56. **The preliminary view that the *ex ante* assessments of recipient States' human rights records is insufficiently rigorous appears borne out by the fact that, of the current 65 beneficiary States – those participating in the CT Travel Programme and on the path to receipt of the goTravel system – there are a number of States with extremely concerning records of systematic human rights abuse, particularly in respect of the sort of surveillance and persecution of dissidents and journalists which API/PNR data systems facilitate**. One of these States is currently subject to the Security Council sanctions regime, namely Sudan.[98] Further, UN human rights treaty bodies have consistently expressed concerns in respect of a range of proposed beneficiary States such as Azerbaijan,[99] the DRC,[100] Ethiopia,[101] Guatemala,[102] Kazakhstan,[103] Mali,[104] Nigeria,[105] Sri Lanka,[106] Tajikistan,[107] and Vietnam[108] in respect of a wide spectrum of human rights violations ranging from torture, inhuman treatment and arbitrary detention to violations of the right to privacy, free expression, and political participation. Further, such States do not display sufficient judicial independence to prevent or remedy State excesses of power. The Special Rapporteur is profoundly concerned that the provision of powerful data monitoring tools to regimes with histories of such violations either indicates that rigorous analysis of human rights concerns cannot have been conducted, or, if conducted, cannot have been afforded sufficient weight.

57. The importance of conducting a rigorous assessment[109] of recipient States' records of human rights compliance when it comes to border management is heightened because of the width of the discretion which vague definitions of terrorism afford to States in this

98 S/RES/1591 (2005).
99 A/HRC/WG.6/30/AZE/2, [14]-[30].
100 A/HRC/WG.6/33/COD/2, [15]-[34].
101 A/HRC/WG.6/33/ETH/2, [18]-[42].
102 A/HRC/WG.6/42/GTM/2, [16]ff.
103 A/HRC/WG.6/34/KAZ/2, [14]-[33].
104 A/HRC/WG.6/43/MLI/2, [10]-[39].
105 A/HRC/WG.6/31/NGA/2, [22]-[48].
106 A/HRC/WG.6/42/LKA/2, [16]ff.
107 A/HRC/WG.6/39/TJK/2, [16]-[39].
108 A/HRC/WG.6/32/VNM/2, [22]-[43].
109 The Special Rapporteur recalls that the 8th Review of the Global Counter-Terrorism Strategy has, by way of Pillar IV, specifically called upon *'Member States and the United Nations entities involved in supporting counter-terrorism efforts to continue to facilitate the promotion and protection of human rights and fundamental freedoms…*' See: A/RES/77/298 (2023), [105].

context.[110] The abuse of spurious or overly flexible counter-terrorism justifications by regimes with a record of systemic and gross violations of human rights as a cover for surveillance, repression and grave misuse of security measures, harassment, targeting, and persecution of, among others, political leaders and activists, human rights defenders, lawyers, journalists, and minorities has been a well-documented focus of the work of the Special Rapporteur throughout this and previous Mandates.[111] The misuse of the Interpol Red Notice system (and its foundational principle of political neutrality with respect to the merits of Red Notices)[112] by States to leverage international cooperation to target dissidents has rightly been a key concern of civil society[113] and various international institutions in recent years.[114] The provision of bulk API and PNR data happens in real time so that State authorities in places of departure and arrival can more efficiently enforce controls against persons subjectively designated as suspects, as well as potentially their associates, family members, colleagues, and community raises just the same concerns.

d) Absence of Ex Post Control or Sanctions

58. The limitations in respect of human rights due diligence on CT Travel Programme recipient States is exacerbated by the way in which, once deployed, there is no ability to monitor a recipient State agency's use of the goTravel software or prevent or respond to serious human rights breaches facilitated by the goTravel program where they arise. The statements by the proponents of the CT Travel Programme and goTravel system that recipient Member States are supported to ensure that human rights-respecting frameworks are in place prior to provision of goTravel and that the goTravel software is *'compliant with human rights, privacy and data protection principles by design*' ring hollow and appears to have no concrete action or ongoing oversight point attached to it.[115] The Special Rapporteur notes that, even assuming full and rigorous compliance with the *ex ante* human rights due diligence contemplated by the CT Travel Programme: Programme Action Plan, the absence of follow-up renders prior actions of limited utility.

59. It would be one matter if, having supplied technical assistance to States opting into the free goTravel system, the UN implementing partners were entitled (contractually or otherwise)

---

110 The Special Rapporteur regularly conducts review of the adequacy and rigour of proposed Member State counter-terrorism legislative frameworks. See: https://www.ohchr.org/en/special-procedures/sr-terrorism/comments-legislation-and-policy

111 See, for example: A/HRC/31/65, [21]. [24], and [27]; A/HRC/37/52, [33], [36], and [66]; and A/HRC/40/52, [34]-[35].

112 Constitution of the ICPO-Interpol, I/CONS/GA/1956 (2021), Article 3: *'It is strictly forbidden for the Organization to undertake any intervention or activities of a political, military, religious or racial character*.'

113 See, for instance: 'Civil Society Resolution on the Forthcoming 89th General Assembly of INTERPOL that will take place in Istanbul on 23-25 November 2021,' available at: https://arrestedlawyers.org/2021/11/16/8029/

114 See, for instance: Directorate-General for External Policies of the Union, 'Misuse of Interpol's Red Notices and impact on human rights – recent developments,' PE 603.472 (January 2019), available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU(2019)603472_EN.pdf; and Parliamentary Assembly of the Council of Europe, 'Abusive recourse to the Interpol system: the need for more stringent legal safeguards,' Resolution 2161 (2017), available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=23714&lang=en

115 See Joint Evaluation, p24.

to restrict the provision of API and PNR data (whether generally or subject to certain criteria) only to those circumstances in which recipient State authorities (PIUs and law enforcement) could demonstrate that collection and analysis would assist in the detection of terrorist risks properly so-called. **But the design of the system renders such oversight impossible.** Not only is no UN agency granted access to the API and PNR data transmitting from carriers to State authorities, but the immediacy and absence of case-by-case request is the entire virtue of the automated API/PNR system in the first place. Even if the Memorandum of Understanding and Memorandum of Agreement which recipient Member States sign contain undertakings as to human rights-compliant use (and the detail of existing MoU/MoA arrangements with Norway and Botswana has not yet been publicized), the reality is that such mechanisms are not legally binding or enforceable by the UN. As the recent UNOCT/UNODC evaluation of the CT Travel Programme admitted with disarming frankness: *'[n]aturally the [CT Travel Programme] cannot enforce [MoU commitments] on the M[ember] S[tate] and many external factors (e.g., political change, economic downturn) will impact upon the likelihood of the MS adhering to those commitments*.'[116] The notion that UNOCT can address the behaviour of recipient Member States through an unenforceable MoU/MoA process is singularly unrealistic.

60. As for human rights being 'designed into' the goTravel system, the Special Rapporteur is concerned this may be an illusionary position. This position paper has already identified that the supposed privacy dividend delivered by 'de-masking' of data after 6 months is not the guarantee it is promised to be given that: (a) such a process again relies upon the *bona fides* of national PIUs to comply; (b) in any event, different anonymisation or pseudonymisation protocols will produce inconsistent levels of privacy protection; and (c) new re-identification techniques will likely erase the privacy benefit of anonymisation in any event in the near future. Further, anonymisation in any event only seeks to address retention of personal information for an excessive period of time. There is no design element which prevents or mitigates the risks of current misuse by national authorities in real time.

61. The Special Rapporteur notes (with thanks for the positive engagement involved) that she has been provided by the UNOCT with documents (not publicly available) relating to the terms of reference for the operations of PIUs and the standards which UNOCT expects Member States to implement in domestic legislation with respect to the powers and functions of domestic PIUs. It is welcome that guidance documents refer in passing to the need for PIUs to be subject to domestic legal obligations to operate in a rights-respecting manner, and urge PIUs in practice to function within those boundaries. But aspirational language is clearly unlikely to be sufficient to restrain the operations and decision-making of national PIUs.

62. It would be one thing if, for instance, the goTravel software built in a **'kill switch'** capacity which enabled UN agencies or other third parties to identify where a particular request for API/PNR data from a national PIU raised red flags as to potential misuse and prevent the data transfer (for example, if the subject of the data request was, or was connected to, a dissident associated with the State in which the PIU was located). But the design of the

116 Joint Evaluation, p20.

system contains no such coding; unsurprisingly, since such a function would entail extremely complicated consideration of markers capable of flagging when a target might be at risk and the degree of risk required before a red flag might be raised.

63. **Indeed, once the goTravel software is implemented, no UN agency itself has access to any passenger data, which is transferred exclusively between carriers and State authorities via the program.** No UN agency is able to discern, for instance, what categories State PIUs are using to guide their pattern analysis, or whether State PIUs are in fact complying with data storage and retention standards.[117] Nor does the CT Travel Programme provide an obvious mechanism for the UN to revoke support once granted as a sanction for human rights non-compliance. Instead, the only barrier to retention of goTravel access contemplated by the CT Travel Programme is the recipient State's payment of its individualized fee after the initial two-year free trial period.[118]

64. **In circumstances where it can be reasonably foreseen that State authorities may use technology freely provided by the UN in ways which are unregulated and discretionary, and thus inconsistent with human rights protection, the risks for the UN are significant and deeply detrimental to its perceived neutrality and integrity.[119]** This requires the most searching and rigorous assessment of human rights risks posed by provision of unfettered API and PNR data access to a recipient State, and robust mechanisms for preventing or sanctioning abuse of the powers grants. Bare assertions of human rights compliance are deeply concerning and raise fundamental concerns about the consequences of a pattern of misuse or misuse that leads to the violation of both derogable, non-derogable and *jus cogens* norms.

e) Concerns for Right to Privacy

65. The substantive human rights risks of widespread access to personal information contained in API and PNR datasets are evident but nonetheless must be set out in detail, so as to identify lacunae and to advance better protections.

66. **First, with respect to the right to privacy (and the various rights of expression, religion, political participation, etc which depend upon privacy),[120] the sensitivity and risks represented by API and PNR data is difficult to overstate.** Both API and (to a greater extent) PNR data comprise rich datasets because they provide not only biographical information but also further data points (about movements and, in the case of PNR, financial transactions, companions, address etc) which hold the promise of more precise conclusions about each person's activities and connections. The existence of such datasets which combine location information, financial connections between people, and their physical travel histories means that those State authorities with access to the data can identify where a person has travelled, with whom, and at whose expense. This is clearly a

---

117 This is not to suggest that UN agencies ought to be fixed with permanent monitoring responsibilities: such responsibilities are not likely appropriate bearing in mind UN agencies' mix of expertise, size, and resources.

118 See: 'goTravel FAQ, 5.2,' available at: https://www.un.org/cttravel/faq

119 See, making a similar point: A/77/345, [24].

120 A/HRC/52/39, [45].

prima facie interference with the privacy not only of those travelling, but also of those tangentially connected with them (travelling companions, the individuals paying on their behalf).

67. **The interferences with privacy represented by government access to, and analysis of, personal data become even more pronounced if those data are subject to decision-making carried out by AI systems.** AI systems can be trained on personal data to make inferences and predictions about individuals based on correlations between certain personal characteristics and certain historic events experienced or carried out by persons sharing such characteristics. As the Office of the High Commissioner on Human Rights noted in its 2021 report, *'AI-made inferences and predictions, despite their probabilistic nature, can be the basis for decisions affecting people's rights, at times in a fully automated way*.'[121] Criminal justice agencies, for instance, may subject individuals to investigation on the basis of AI-generated prediction, of that individual's likelihood of future involvement in terrorism. But *'AI-based decisions are not free from error*' and indeed *'the scalability of AI solutions can dramatically increase negative effects of seemingly small error rates*.'[122]

68. The privacy concerns raised by the application of AI systems to personal datasets such as API and PNR data are substantial. First, AI analysis can only function properly when consuming vast quantities of personal data – by definition exposing the information of large numbers of people to analysis and the potential for data leakage or misuse. Second, AI-based decisions can trigger interventions by the State even though there is no evidence that probabilistic AI assessments constitute a reasonable suspicion of likelihood of the human target (man, woman or child) committing any future wrong. Third, the opacity of AI-based decisions creates substantial barriers for effective oversight or remedies, since the actual operation of the system is typically extremely complex and hidden even from technical experts. Fourth, since AI-based decision-making replicates and draws conclusions about correlations between historic data, it is unavoidably bound by the limitations, deficiencies, or biases in the historic data. Where racial or ethnic minorities have historically suffered disproportionate incarceration, the AI system will operate on the basis that such race or ethnic markers correlate with higher rates of criminal involvement, rather than seeing them as potentially irrelevant statistical noise created from a non-representative input. As a result, as the OHCHR notes, AI tools *'carry an inherent risk of perpetuating or even enhancing discrimination, reflecting embedded historic racial and ethnic bias in the data sets used, such as a disproportionate focus of policing of certain minorities*.'[123] This additional discrimination risk renders AI application of API and PNR data particularly problematic from the point of view of human rights compliance.

69. Under international human rights law, every person enjoys the right to private and family life without undue interference. Article 17 of the ICCPR requires that:

[121] A/HRC/48/31, [16].
[122] Ibid, [18].
[123] Ibid., [24].

> *'1. No one shall be subjected to arbitrary or unlawful interference with [their] privacy, family, home or correspondence, nor to unlawful attacks on [their] honour and reputation.*
> *2. Everyone has the right to the protection of the law against such interference or attacks*.'[124]

70. The boundaries of what the word *'privacy*' denotes have not been precisely established in international human rights law, but the jurisprudence of the HRC and regional human rights courts have demonstrated that the right certainly entails protection of individuals' correspondence, communications, and personal information. In this respect, the HRC has urged that the *'processing and gathering of [personal data] be subject to review and supervision by an independent body with the necessary guarantees of impartiality and effectiveness*,'[125] and has advised that:

> *'[i]n order to have the most effective protection of [their] private life, every individual should have the right to ascertain in an intelligible form, whether, and if so what, personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination*.'[126]

71. Those principles regarding personal data have been enshrined in a number of specific international instruments which set out, *inter alia*, that individuals should have the right to obtain information regarding the personal data others hold on them and, with respect to errors or data held unlawfully, should have the right to require amendment, rectification, or erasure.[127]

72. Specific data protection legislation gives effect to the balance between private rights regarding personal information and the powers of the State. But in addition to those specific standards, and in respect generally of any State policies and practices which affect the right

---

124 See also UDHR, Article 12.

125 HRC, Concluding Observations on Sweden, UN Doc. CCPR/C/SWE/CO/6 (2009), [18].

126 HRC, *General Comment 16*, UN Doc. HRI/GEN/1/Rev.9 at 142 (1988), [10].

127 See, for instance: OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, Annex; updated in 2013 by OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 11 July 2013, Annex; Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data (adopted 28 January 1981, entered into force 28 January 1981) ETS 108; European Union, Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012, pp391-407, Article 8; Regulation (EU) 2016/279 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Articles 4, 5, 14-17; Inter-American Juridical Committee, OAS Principles on Privacy and Personal Data Protection, OEA/Ser.O, CJI/doc. 474/15 rev.2 (26 March 2015); ECOWAS, Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 16 February 2010; and African Union, Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) (adopted 27 June 2014, not yet in force).

to privacy, international human rights law stipulates further conditions which must be satisfied for an interference to be lawful. First, the interference may only take place in accordance with established law[128] which specifies in detail the precise circumstances in which such interferences may be permitted.[129] Further, any interference with the right to privacy must be *'reasonable*,' which the HRC has clarified in the case of *Toonan v Australia* means that it *'must be proportional to the end sought and be necessary in the circumstances of any given case*.'[130]

73. The text of Article 17 of the ICCPR (unlike the text of various other rights) does not expressly set out what type of *end* might justify an interference with the right to privacy. But the consistent approach of the HRC[131] and regional courts interpreting equivalent protections under regional instruments such as the European Convention[132] is to require that a legitimate aim (such as the prevention of crime) is identified in furtherance of which the interference represents a necessary and proportionate measure.

74. The legitimate aim of preventing terrorism and/or serious crime is clearly capable of justifying limited interference with the right to privacy. But the degree of interference must be considered in the light of the necessity of the measure to achieve the aim and the actual benefit it yields.[133] In another context (the right to freedom of movement), the HRC has clarified that such consideration requires that the infringement is the *'least intrusive instrument amongst those which might achieve their protective functions*,'[134] and has counselled that, *'[i]n adopting laws providing for restrictions permitted [for legitimate aims], States should always be guided by the principle that the restrictions must not impair the essence of the right … the relation between the right and restriction, between norm and exception, must not be reversed. The laws authorising the application of restrictions should use precise criteria and may not confer unfettered discretion on those charged with their execution*.'[135]

75. **Judged against States' obligations to respect the right to privacy, multiple aspects of the approach to collection, analysis, and transmission of API and PNR data facilitated by the CT Travel Programme and the goTravel program raise serious concerns.**

76. **First**, by definition and unavoidably, the API and PNR data collection procedures currently being required by PIUs of air carriers apply to all travellers without discrimination. The data of all passengers is subject to pattern analysis against opaque risk factors, which are themselves not subject to oversight or analysis. Individuals are subject to constant monitoring irrespective of the fact that they are not suspected of any criminal offence. This

128 HRC, *General Comment 16*, UN Doc. HRI/GEN/1/Rev.9 (Vol I) (8 April 1988), [3].
129 HRC, *General Comment 16*, [8].
130 HRC, *Toonan v Australia*, UN Doc. CCPR/C/50/D/488/1992 (1994), [8.3].
131 See, for instance: HRC, *Van Hulst v Netherlands*, UN Doc. CCPR/C/82/D/903/1999 (2004), [7.6]-[7.10].
132 See, for instance: *Weber and Saravia v Germany* (App No. 54934/00), Decision of 29 June 2006, [103]-[137].
133 As noted in OHCHR, Annual Report of the UN High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age,' UN Doc. A/HRC/27/37 (30 June 2014), [24].
134 HRC, *General Comment 27*, UN Doc. CCPR/C/21/Rev.1/Add/9 (1999), [14]; and HRC, *General Comment 34*, UN Doc. CCPR/C/GC/34 (2011), [34].
135 HRC, *General Comment 27*, [13].

raises clear questions of necessity and proportionality, and in effect reverses the presumption of innocence, contrary to the fundamental principles of legality and due process.

77. **Second**, once API and PNR data are transferred via goTravel to national PIUs, whatever the intentions of UN agencies may be, there is no binding guarantee that national processes will in fact conform with basic safeguards such as human oversight of artificial decision-making[136] or the requirement that data not be further disclosed and re-used by other State agencies.[137] The Special Rapporteur acknowledges that recipient States are provided with legislative guidance by UNOCT and terms of reference to domestic PIUs which proceed on the basis that PIUs will operate in a rights-respecting manner. Further, recipient States agree MoUs/MoAs with UNOCT with respect to the provision of the goTravel program under the CT Travel Programme which may seek to impose *ex ante* limitations upon PIU and national use of transferred API and PNR data. But in the absence of binding legal mechanisms or technological failsafes, the normative value of any undertakings cannot be assumed.

78. **Third,** the length of the retention period takes the use of such data beyond being merely an instantaneous check against a particular suspect profile. Instead, it allows the data to be used as a longer-term record of personal behaviour from which detailed knowledge may be drawn (including, in forthcoming generations of goTravel, via AI and algorithmic analysis). While the goTravel software builds in a default storage period of 5 years, with personal details masked after 6 months, those details are capable of being 'de-masked' by PIUs operating the goTravel system. Further, of course, all time limits and data management parameters are ultimately a matter controlled by recipient States' domestic law, rather than under UN oversight.

79. **Fourth,** the goTravel software facilitates potentially invasive follow-up measures however guidance provides no indications or standards as to when pattern analysis or follow-up measures based on it are lawful or necessary. PIUs and domestic authorities are free to determine next steps. In particular, those persons who are not suspected of any offence before the PNR data are processed may then be 'further investigated' by the security authorities within the framework of preventative police or security measures.

80. **Fifth**, there is nothing in the goTravel architecture to prevent national PIUs from onward transfer of API/PNR data records and the processing results to other countries or parties. In keeping with the laxity of legal frameworks across the entire regime, there is no guarantee that any such transfers will be limited only to circumstances where such onward information sharing is necessary and proportionate to a legitimate aim.

81. **Six,** given that the assessment of the lawfulness of necessity and proportionality concerning interferences with privacy is such a nuanced and fact-specific exercise, it is a matter of grave concern that the CT Travel Programme and the goTravel program are structured in such a way that State authorities' own decision-making and use of API and PNR data

136 Cf. *Ligue des Droits Humains*, [194].
137 Cf. *Ligue des Droits Humains*, [218]-[220].

received is opaque and largely shielded from external review. The structure of this project contains insufficient design rigour to ensure human rights compliance in this regard.

82. **The Special Rapporteur notes that the privacy deficiencies identified above are consistent with the conclusions of the CJEU with respect to the lawful bounds of PNR collection and processing in the European Union.** That the UN would actively promote a type of data collection and sharing regime internationally which has, in key respects, been held unlawful in the European Union raises deep concerns. Quite apart from human rights compliance, the practicality of pressing on with the promotion and roll-out of API and PNR capabilities via goTravel which are inconsistent with the requirements imposed by EU Member States would appear to create significant operational difficulties given the centrality of EU jurisdictions (and EU-based air carriers) to the global air transportation industry. **The Special Rapporteur is concerned that the implications of the limitations imposed by the CJEU on the operation, and inter-operation, of API and PNR systems worldwide may not fully have been considered by the CT Travel Programme's UN implementing partners.**

f) Concerns for Freedom of Expression

83. In circumstances where it can be reasonably foreseen that State authorities will deploy the knowledge obtained about individuals' movements from API and PNR data to target and persecute human rights defenders, political dissidents, journalists, etc, the protection of freedom of expression is clearly also engaged. Freedom of expression is protected worldwide as a fundamental human right.[138] Article 19 of the ICCPR provides that:

> *'1. Everyone shall have the right to hold opinions without interference.*
> *2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of [their] choice*.'

84. The right to freedom of expression is recognized in human rights law as particularly important, since it provides the mechanism by which other rights, such as political participation,[139] freedom of assembly[140] and association,[141] and freedom of religion,[142] may be exercised. As the HRC put it in its *General Comment 34*:

> *'Freedom of opinion and freedom of expression are indispensable conditions for the full development of the person. They are essential for any society. They constitute the foundation stone for every free and democratic society … Freedom of expression is a necessary condition for the realization of the principles of*

138 UDHR, Article 19.
139 See: UDHR, Article 21; HRC, *Gauthier v Canada*, UN Doc. CCPR/C/65/D/633/1995, [13.4]; and *Aduayom, Diasso and Dobou v Togo*, UN Doc. CCPRC/57/D/422-4/1990, [7.4].
140 ICCPR, Article 21; UDHR, Article 20.
141 ICCPR, Article 22; UDHR, Article 20.
142 ICCPR, Article 18; UDHR, Article 18.

transparency and accountability that are, in turn, essential for the promotion and protection of human rights.'[143]

85. The right applies broadly, and includes *'political discourse, commentary on one's own and public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching and religious discourse*.'[144] Further, as regional courts have made clear, opinion and expression does not lose its protection merely by virtue of being untrue, shocking, offensive, or disturbing, or indeed by challenging the democratic principles upon which its protection is justified.[145] As with the limited right of privacy set out above, the right to freedom of expression is similarly capable of lawful restriction subject to satisfaction of the three-part test that the restriction is prescribed by law, pursues one of a closed list of legitimate aims, and the effect of the restriction is no more than is necessary and proportionate to achieve that aim.[146]

86. The same risks which pertain in respect of the protection of privacy – namely the absence of any effective method to prevent or hold States accountable for unnecessary and disproportionate interferences with the right – similarly apply in respect of the risk posed by the international system of API/PNR data sharing to freedom of expression. As noted by the Special Rapporteur in her 2019 report to the Human Rights Council[147] and affirmed in her Global Study on the Impact of Counter-Terrorism on Civil Society,[148] there is a long history of misuse of purported counter-terrorism powers by Member States to target dissidents, political opponents, journalists, and human rights defenders in breach of rights of expression and associated rights. Against that backdrop, the provision of a powerful tool to States for the identification of individuals, and their family members and associates, and to track their movements internationally in real time, raises significant concerns which require robust safeguards greater those provided by the unenforceable undertakings currently contemplated as the high point of recipient State human rights compliance.

g) Concerns for Freedom of Movement Rights

87. Another unique human rights challenge presented by the use of API and PNR data in screening is that, because such data are provided well ahead of travel, it may lead to individual travellers not only being subject to screening on arrival, but to denial of boarding and departure altogether. Such an outcome is in tension with fundamental rights to freedom of movement and, crucially, the right to seek asylum overseas.

88. The UN General Assembly recently affirmed, in Resolution 76/172 on the Protection of Migrants, that *'everyone has the right to leave any country, including his or her own, and*

143 HRC, *General Comment 34*, UN Doc. CCPR/C/GC/34 (12 September 2011), [2].
144 *General Comment 34*, [11].
145 *Handyside v United Kingdom* [1975] ECHR 5; (1976) 1 EHRR 737, [49]; and *Gündüz v Turkey* [2003] ECHR 652, [51].
146 HRC, *General Comment 27*, [14]; and HRC, *General Comment 34*, [34].
147 A/HRC/40/52.
148 See: defendcivicspace.com; and A/78/520.

to return to his or her country.'[149] That right is well-attested in international law: Article 12 of the ICCPR provides, *inter alia*, that:

> *'2. Everyone shall be free to leave any country, including his own.*
> *3. The above-mentioned rights shall not be subject to any restrictions except those which are provided by law, are necessary to protect national security, public order (ordre public), public health or morals or the rights and freedoms of others, and are consistent with the other rights recognized in the present Covenant.*
> *4. No one shall be arbitrarily deprived of the right to enter his own country.*'

89. The right to seek asylum is enshrined in Article 14 of the Universal Declaration of Human Rights,[150] along with regional instruments.[151]

90. As the recent UN OCT Handbook on Human Rights and Screening in Border Security and Management notes, in border control situations States *'must have particular regard to the right of all persons to leave any country, including their own*' since *'[d]enial of boarding may put an individual at risk, and may deprive them of the opportunity to seek asylum*' upon arrival in another country.[152] The General Assembly has underscored that States must *'adopt concrete measures to prevent the violation of the human rights of migrants while in transit, including in ports and airports and at borders and migration checkpoints*.'[153]

91. It is crucial to emphasize that the right to leave a country is separate and independent from any question about eligibility to enter another country. While the rise of international API and PNR data sharing has allowed for efficient communication between States, it is important to resist the conflation of the concepts of exit, movement, and entry, and the legal regimes governing those concepts. As a matter of law, State A is not entitled, save in exceptional circumstances, including, for instance, the arrest of criminal suspects, to prevent persons from exiting State A. Nor is State B save in exceptional circumstances entitled to prevent persons from exiting State A, even if State B may be entitled to prevent persons from entering State B upon arrival (subject to its obligations to respect the right of would-be entrants to seek asylum). That is why Article 13 of the Chicago Convention provides that administrative requirements that a State party apply only *'upon entrance into or departure from, or while within the territory of that State*'[154] and not also upon departure from a third State for a journey to the State party.

92. This is not merely a point of academic interest. The reason why the asylum claims must be determined upon arrival rather than prior to departure is not because of purist adherence to legal technicality – it is because a prospective applicant for asylum may be free to disclose and explain their situation in full only once outside the jurisdiction of the State from which they seek to flee. Facts caught by API data and/or PNR data collection and analysis and

149 A/RES/76/172 (10 January 2022).
150 UNDHR, Article 14.
151 EU Charter of Fundamental Rights, Article 18.
152 UN OCT UN Counter-Terrorism Centre, 'Handbook on Human Rights and Screening in Border Security and Management' (July 2020) ('UNOCT CTC Handbook'), p16.
153 A/RES/76/172.
154 Chicago Convention, Article 13.

which might be flagged as worthy of concern in the abstract include: (a) apparent inconsistencies in official identification documents; (b) an unexplained source of funds for travel; (c) transfers of money from overseas being used to fund travel; and (d) disjunct between travel behaviour and family connections.

93. But such factors could very well be related to legitimate reasons for clandestine travel for the purposes of seeking asylum or fleeing domestic abuse or threats of violence. Unconventional behaviour regarding travel for such purposes, if presented and considered by border officials in person upon arrival, could form the basis for meritorious asylum applications or discretionary grants of entry on humanitarian grounds according to relevant national legislation in line with international standards. The blanket use of a system whereby automatic decisions are made as to eligibility to disembark prior to departure prevents any such discretionary apparatus functioning as it should. Accordingly, programming which supports the use of API and PNR data in pre-departure screening decisions poses a real risk of frustrating legitimate exercise of free movement and associated rights.

94. Of course, if would-be entrants are found, upon assessment, not to have good grounds for an asylum claim, the State of arrival is entitled, under international law, to deport them (subject to the prohibition on *refoulement* contained in the Refugee Convention).[155] But the possibility of future denial of admission is not a lawful basis for a prospective denial of the right to leave any other country.

h) Right to a Remedy

95. A further issue in the context of API and PNR data is that decisions taken in reliance on such data typically occur in the liminal context of the border and generally securitized spaces of national jurisdictions. Border decisions pose particular challenges for human rights compliance. The OHCHR has specifically urged Member States *'to provide effective remedies for violations of human rights at international borders, to provide reparation to victims and to bring State and private actors to account for such violations and abuses…*'[156]

96. The right to an effective remedy for any breaches of rights is a fundamental principle of international human rights law.[157] Human rights law imposes obligations to make available effective remedies to people whose rights have been violated. This right to a remedy has often been identified as one of the most fundamental aspects of an effective framework for human rights protection.[158] The HRC has emphasized that, even in times of emergency, States must comply with the *'fundamental obligation … to provide a remedy that is*

155 UN General Assembly, *Convention Relating to the Status of Refugees*, 189 UNTS 137, opened for signature 28 July 1951, entered into force 22 April 1954, Article 33.

156 UN Office of the High Commissioner for Human Rights, 'Principles and Guidelines on Human Rights at International Borders' (October 2014), p13.

157 ICCPR, Article 2(3).

158 See, for instance: Report of the Special Representative on Human Rights Defenders, UN Doc. A/56/341 (2001), [9]; and Report of the Special Rapporteur on Violence Against Women on Cultural Practices in the Family that are Violent Towards Women, UN Doc. E/CN.4/2002/83 (2002), [116].

effective.'[159] The jurisprudence of all international human rights bodies has consistently established that for remedies to be *effective*, they must satisfy the criteria of: being prompt;[160] being practical rather than theoretical;[161] being determined by an independent authority;[162] and being accessible (without undue practical or financial barriers).[163]

97. The need for remedies in respect of decisions at the border is self-evident: as with all administrative systems, mistakes are made, and with the particular complexities of border decisions (involving potential misunderstandings/miscommunications on the basis of language and culture), it is perhaps predictable that such mistakes may be more frequent when compared to typical administrative settings. Further, decision-making regarding permission to enter at international borders often involves broad discretions.

98. Technically speaking, individuals subject to border screening decisions prior to admission into a country are likely under the jurisdiction of the State responsible for the screening (regardless of its exact location).[164] Further, States typically have some formal mechanism for review and challenge of immigration/border decisions. But in practice, the reality is that individuals will commonly face considerable obstacles posed by, among other things: lack of legal representations (often exacerbated by ineligibility for legal aid due to foreign nationality), lack of awareness of the State's administrative or legal system, language barriers, etc. These represent considerable obstacles to accessing the right to a remedy for any breach of human rights associated with the processing of API and/or PNR data which leads to a border refusal decision.

Conclusion

99. **The CT Travel Programme's API and PNR collection and sharing system was never designed with human rights in mind.** It is marked by *ad hoc* thinking and the absence of rigorous analysis of how the technology and the international framework for data sharing it facilitates could be designed and operated in a manner which complies with relevant legal obligations, particularly international human rights law. The absence of that analysis has led to a situation in which the UN is now directly implicated in an approach to API and PNR data collection and sharing being rolled out globally which risks placing immensely powerful tools in the hands of States which may misuse them, intentionally or inadvertently, to jeopardize human rights, without any evidence of sufficient prior vetting, and without any practical or legal recourse to prevent or sanction such misuse.

100. At precisely the same time that the UN has promulgated the CT Travel Programme and goTravel software platform across Member States, the European Union has been forced to re-imagine its approach to API and PNR systems in light of the CJEU having found multiple

159 HRC, *General Comment 29*, UN Doc. CCPR/C/21/Rev.1/Add.11 (2001), [14].
160 HRC, *General Comment 31*, UN Doc. CCPR/C/21/Rev.1/Add.13 (2004), [15]; CEDAW Committee, *General Recommendation 33*, [11]; and Inter-American Court of Human Rights, *Judicial Guarantees in States of Emergency*, Advisory Opinion OC-9/87 (6 October 1987), Series A No. 9, [24].
161 CEDAW Committee, *General Recommendation 33*, [1] and [14].
162 HRC, *General Comment 31*, [15].
163 CEDAW Committee, *General Recommendation 33*, [36]-[37].
164 UNOCT CTC Handbook, p17.

features of its initial design (which the UN-backed system mirrors) to be unlawful and in violation of human rights protection. **The Special Rapporteur anticipates further legal challenges ahead which only serves to underscore the need for a fundamental rethink in this area of counter-terrorism practice**.

101. **The current UN approach to API and PNR data collection and sharing which is facilitated by the UNOCT and UN implementing partners in the CT Travel Programme and go Travel software platform represents a profound human rights risk and a serious reputational risk for the UN itself. The roll-out of the system must be paused and an urgent review initiated.**

102. As a result, the Special Rapporteur recommends that:

102.1. The UN implementing partners for the CT Travel Programme should pause the roll-out of the programme and goTravel software in light of its apparent potential human rights risks;

102.2. The implementing partners should engage with all relevant UN agencies, including the OHCHR, the mandate of the Special Rapporteur and other relevant Special Procedure mandates, UNICEF, UN WOMEN, and the UNHCR, to undertake a robust, meaningful, and independent human rights review of the CT Travel Programme and goTravel;

102.3. As part of that review, the implementing partners should consider in detail the implications for the CT Travel Programme and its intended operations of the recent decisions of the CJEU with respect to the limitations applicable to API and PNR systems in the European Union;

102.4. UN implementing partners should ensure that any future programme for the collection, analysis, and sharing of API and/or PNR data is subject to rigorous legal and practical/technical safeguards, including, so far as possible, re-design of the goTravel software platform, to minimize the risk that such data will be misused by recipient States in violation of human rights and to ensure that appropriate sanctions apply in instances of misuse; and

102.5. Finally, the eligibility for States to receive assistance from UNOCT and its UN implementing partners as part of the CT Travel Programme should be contingent on a robust human rights analysis, including compliance with the UN Human Rights Due Diligence Policy.