Travellers' surveillance:

The role of the UN Countering Terrorist Travel Programme

December 2024

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

TABLE OF CONTENTS

List of abbreviations

API	Advance Passenger Information
CJEU	Court of Justice of the European Union
CTED	Counter-Terrorism Committee Executive Directorate
CTTP	United Nations Countering Terrorist Travel Programme
EC	European Commission
EDPB	European Data Protection Board
EU GDPR	European Union General Data Protection Regulation
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
INTERPOL	International Criminal Police Organization
IOM	International Organization for Migration
MIDAS	IOM Border Management Information System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
OCT	United Nations Office of Counter-Terrorism
ODC	United Nations Office on Drugs and Crime
OHCHR	Office of the United Nations High Commissioner for Human Rights
OICT	United Nations Office of Information and Communication Technology
PNR	Passenger Name Records

Executive Summary

Since 9/11 securitisation of international borders has shifted gear, and every new major geopolitical development (such as the Syrian conflict and the emergence of the foreign fighters' phenomenon) is further strengthening the hand of those advocating for the expansion of surveillance of travellers and at borders.

In this context, the collection, analysis and sharing of passengers' data is ramping up in scope, purposes and technical capabilities. Processing travellers' data is seen by many governments and industry as necessary to respond to perceived threats of terrorism, investigate serious crimes and more broadly secure borders against illegal entries.

PI has long been concerned by the largely unregulated introduction of surveillance technologies at borders, resulting in mass surveillance and unfettered powers. Specifically, the systematic, untargeted collection, analysis and sharing of travellers' personal data constitutes a form of mass surveillance and does not meet the requirements of necessity and proportionality under international human rights law.

Together with states and companies, the United Nations (UN) is becoming an increasingly influential actor in providing surveillance assistance to states. Within the complex and opaque UN counter-terrorism architecture, the UN Countering Terrorist Travel Programme (CTTP) plays a key role in promoting the surveillance of travellers. In particular, it offers UN Member States a purpose-made software, goTravel, that enables government authorities to process travellers' data such as Advance Passenger Information (API) and Passenger Name Records (PNR) data.

As such the UN has a key responsibility to ensure that their surveillance assistance to states complies with human rights due diligence and mitigates

risks of unlawful surveillance and other abuses. In this briefing, PI outlines the purposes and activities of the UN CTTP, identifies the most significant concerns, and puts forward a range of recommendations to mitigate some of the human rights risks associated with the surveillance of travellers.

1. Introduction

Since 9/11 securitisation of international borders has shifted gear, and every new major geopolitical development (such as the Syrian conflict and the emergence of the foreign fighters' phenomenon) is further strengthening the hand of those advocating for the expansion of surveillance of travellers and at borders.

In this context, the collection, analysis and sharing of passengers' data is ramping up in scope, purposes and technical capabilities. Processing travellers' data (in the form of Advance Passenger Information (API) and increasingly Passenger Name Records (PNR), see explanation below) is seen by many governments and industry as necessary to respond to perceived threats of terrorism, investigate serious crime and more broadly secure borders against illegal entries.

While recognising states' legitimate aim of preventing and investigating acts of terrorism and other serious crimes, PI has long been concerned by the largely unregulated introduction of surveillance technologies at borders, resulting in mass surveillance and unfettered powers. PI believes that the systematic, untargeted collection, analysis and sharing of travellers' personal data constitutes a form of mass surveillance and does not meet the requirements of necessity and proportionality under international human rights law.[1]

As a growing number of governments require travellers' data from airlines,

[1] Recently PI has been exposing the significant role that international and regional organisations, such as the EU and INTERPOL, play in supporting states developing their surveillance capabilities. See PI, "When Spiders Share Webs": Unveiling privacy threats of EU-funded INTERPOL policing programme in West Africa, September 2024, https://privacyinternational.org/long-read/5346/when-spiders-share-webs-unveiling-privacy-threats-eu-funded-interpol-policing

several states and private actors are providing support to process API and PNR data. Together with states and companies, the United Nations (UN) is becoming an increasingly influential actor in providing surveillance assistance. In a context where many states and private actors offer governments products and services to enable governments to process travellers' data, the UN Countering Terrorist Travel Programme (CTTP) offers UN Member States a range of assistance, including a purpose-made software, goTravel, that enables government authorities to process API and PNR data.

This briefing, based on publicly available information and PI's own research, outlines the purposes and activities of the CTTP, identifies the most significant concerns, and puts forward a range of recommendations to mitigate some of the human rights risks associated with the surveillance of travellers.

PI shared a draft of this briefing with the United Nations Office of Counter-Terrorism (OCT), which coordinates and implements the CTTP in partnership with other UN entities. PI continues to engage with OCT and other UN partners of the CTTP.

2. Background

2.1 What are API and PNR data?

Advance Passenger Information (API) refers to a passenger's identity and includes full name, date of birth, gender, citizenship and travel document data. API is typically obtained from travel documents and available from the machine-readable area of passports.[2]

Passenger Name Records (PNR) are collected by airlines solely for their business purposes. PNR data may contain the names of the passengers, information necessary for the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers, such as meal preferences. PNR contain information about bookings made which can include sensitive personal data.[3] Indeed, PNR data provides very detailed information on individuals which, especially when taken as a whole, reveals intimate details of people's lives.[4]

[2] See IATA, API-PNR Toolkit, https://www.iata.org/en/publications/api-pnr-toolkit/#tab-2

[3] See IATA, API-PNR Toolkit, https://www.iata.org/en/publications/api-pnr-toolkit/#tab-3

[4] As noted in the Opinion 1/15 of the Court of Justice of the European Union, 26 July 2017, paragraph 128: "even if some of the PNR data, taken in isolation, does not appear to be liable to reveal important information about the private life of the persons concerned, the fact remains that, taken as a whole, the data may, inter alia, reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health…", https://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2836259). Similarly, para 100 of Case C-817/19 Ligue des Droits Humains v Conseil des Ministres ECLI:EU:C:2022:491: "the fact remains that, taken as a whole, the data may, inter alia, reveal a complete travel itinerary, travel habits, relationships existing between one or more persons and the financial situation of air passengers, their dietary habits or state of health, and may even reveal sensitive information about those passengers", https://curia.europa.eu/juris/document/document.jsf;jsessionid=AB7512C2D94F06AD226B884E431210B1?text=&docid=261282&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=143815

Unlike API, PNR data mainly depends on the information provided when booking. ICAO has developed Standards and Recommended Practices for the collection, use, processing and protection of PNR data (contained Chapter 9 of Annex 9 to the Convention on International Civil Aviation).[5] However, as noted by the International Air Transport Association (IATA), "accuracy is not guaranteed".[6]

2.2 What is the UN Countering Terrorist Travel Programme?

The CTTP's stated aim is to assist "beneficiary Member States in building their capabilities to detect and counter-terrorists and serious crimes by using Advance Passenger Information (API) and Passenger Name Record (PNR) data to improve the use of international databases with known and suspected terrorists and criminals, and enhance international information exchange", in accordance with relevant UN Security Council resolutions.[7]

The UN Secretary-General officially launched the Programme on 7 May 2019. The CTTP is being implemented by the United Nations Office of Counter-Terrorism (OCT) in partnership with 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). It is co-funded by strategic investments and in-kind support from the European Union, the Netherlands, Qatar, Germany, Australia, the United States of America, India, Japan, Hungary, and the Republic of Korea.[8]

[5] See ICAO, API Guidelines and PNR Reporting Standards, https://www.icao.int/security/fal/sitepages/api%20guidelines%20and%20pnr%20reporting%20standards.aspx

[6] See IATA, API-PNR Toolkit, https://www.iata.org/en/publications/api-pnr-toolkit/#tab-3

[7] Publicly available documents about the CTTP are found at: https://www.un.org/cttravel/

[8] See CTTP webpage, https://www.un.org/cttravel/

2.3 What is the goTravel software solution?

The goTravel software is a UN-owned software derived from the Travel Information Portal (TRIP), developed by The Netherlands and transferred to the UN in 2019. It supports compliance with UN Security Council resolutions 2178, 2396, and 2482, which require UN Member States to:

- Receive and analyse advance passenger information (API);
- Develop capabilities to receive and analyse passenger name records (PNR);
- Make full use of relevant watchlists;
- Share information about Foreign Terrorist Fighters (FTF) and terrorists using commercial air transports within their jurisdiction and across jurisdictions.

Its stated aim is to support "the end-to-end process for law enforcement to obtain passenger data from (airline) carriers and conduct targeted analysis as well as share the findings of their data assessment. Member States may opt to adopt the UN-owned goTravel solution to enable the automated analysis of large data volumes on passengers on all inbound and outbound traffic. goTravel currently supports air travel data collection/analysis/dissemination."[9]

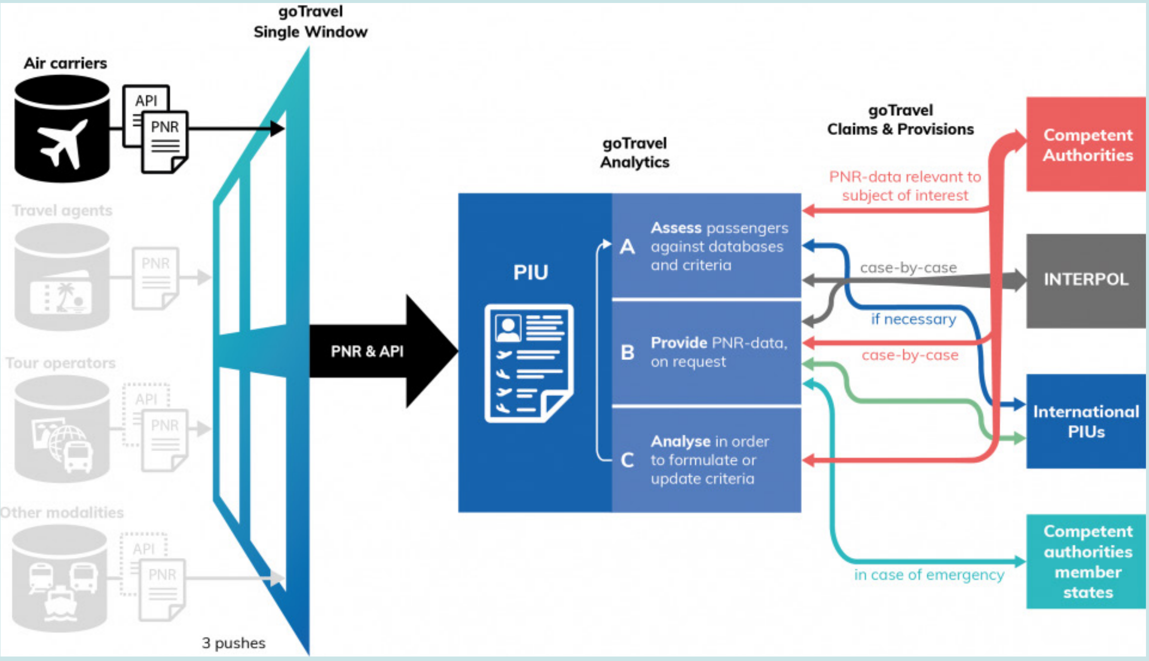
Its main functionalities include (but are not limited to):

- configuration of rule-based risk indicators and watchlists, and lists the records that match against those rules;
- performing an assessment of passengers prior to their scheduled

[9] See CTTP goTravel Software Solution, https://www.un.org/cttravel/goTravel

arrival/departure (matching with risk indicators, watchlists, and Interpol databases);

- Automatically notify competent authorities when goTravel identifies passenger data requiring further examination;
- Enable verification of API and PNR data retrieval and data quality of connected air carriers;
- Enable analysts to reveal relationships between objects in the PNR data (such as passengers' phone numbers, credit cards, etc.) and visualize connections on graphs;
- Use network analysis to identify formally unknown relationships.[10]



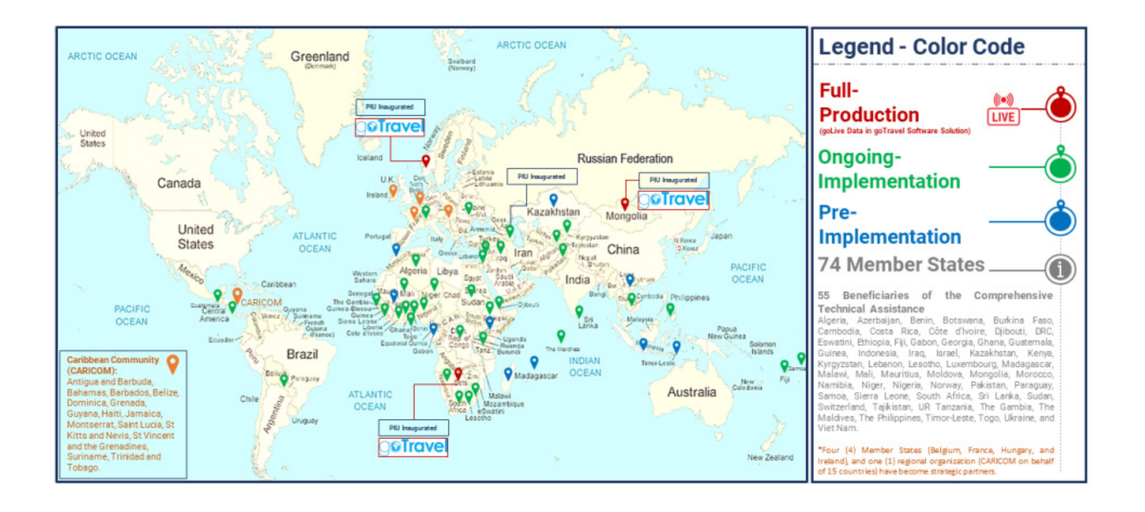
Source: https://www.un.org/cttravel/goTravel

[10] See UN CTTP goTravel Software Solution, https://www.un.org/cttravel/goTravel

2.4 Which countries are receiving UN CTTP support?

According to publicly available information, over 70 UN Member States (including CARICOM on behalf of 15 countries) are engaging with CTTP.[11] 57 UN Member States have received technical assistance from CTTP.[12]

This map shows the states beneficiaries of the CTTP support:



Caribbean Community (CARICOM): Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Haiti, Jamaica, Montserrat, Saint Lucia, St Kitts and Nevis, St Vincent and the Grenadines, Suriname, Trinidad and Tobago.

55 Beneficiaries of the Comprehensive Technical Assistance

Algeria, Azerbaijan, Benin, Botswana, Burkina Faso, Cambodia, Costa Rica, Côte d'Ivoire, Djibouti, DRC, Eswatini, Ethiopia, Fiji, Gabon, Georgia, Ghana, Guatemala, Guinea, Indonesia, Iraq, Israel, Kazakhstan, Kenya, Kyrgyzstan, Lebanon, Lesotho, Luxembourg, Madagascar, Malawi, Mali, Mauritius, Moldova, Mongolia, Morocco, Namibia, Niger, Nigeria, Norway, Pakistan, Paraguay, Samoa, Sierra Leone, South Africa, Sri Lanka, Sudan, Switzerland, Tajikistan, UR Tanzania, The Gambia, The Maldives, The Philippines, Timor-Leste, Togo, Ukraine, and Viet Nam.

*Four (4) Member States (Belgium, France, Hungary, and Ireland), and one (1) regional organization (CARICOM on behalf of 15 countries) have become strategic partners.

Source: image downloaded from CTTP website (https://www.un.org/cttravel/goTravel) on 25 April 2024.

[11] See UN CTTP webpage, https://www.un.org/cttravel/ The latest figures available as of October 2024 is from CTTP Newsletter, 1 January – 31 March 2024, https://www.un.org/cttravel/sites/www.un.org.cttravel/files/un_ct_travel_programme_quarterly_newsletter_-_2024_q1.pdf. According to this September 2023 press release reporting the opening remarks by Mr. Vladimir Voronkov, Under-Secretary-General of the United Nations Office of Counter-Terrorism, the UN CTTP "is currently assisting 68 beneficiary countries to meet their obligations under UN Security Council resolutions to adapt and use advance passenger information (API) and passenger name record (PNR) data systems in combination with biometrics and national, INTERPOL and other relevant watchlists.", Opening Remarks by Mr. Vladimir Voronkov Under-Secretary-General of the United Nations Office of Counter-Terrorism, Eighteenth Symposium and Exhibition on ICAO Traveller Identification Programme (TRIP) 12 September 2023, Montréal, Canada, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/230912_oct_usg_video_remarks_icao_trip_symposium.pdf

[12] See Opening Remarks by Mr. Mauro Miedico, Officer-in-Charge, United Nations Office of Counter-Terrorism Forum Celebrating the 5th Anniversary of the Launch of the Countering Terrorist Travel Programme Budapest, Hungary, 19 July 2024, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/240719_opening_remarks_mauro_miedico_ct_travel_5th_anniversary_forum.pdf

Support includes: legislative assistance (assisting Member States when drafting regulatory/legal frameworks relating to the processing of travellers' data); operational support for the setting up of Passenger Information Units (including providing standard Operating Procedures or Terms of Reference' for PIUs); transport industry support through carrier engagement; technical support and expertise in goTravel software solution and interoperability with national and international databases and watchlists, including those of INTERPOL.[13]

Details on the level of support are hard to come by, particularly since the CTTP last published quarterly newsletter only covers up to 31 March 2024.[14]

[13] See UN CTTP Mid-term Joint Evaluation Report, UNCCT-2018-02-82, March 2023, https://www.unodc.org/documents/evaluation/indepth-evaluations/2023/Midterm_Joint_Evaluation_Report_UN_Countering_Terrrorist_Travel_Programme.pdf

[14] See UN CTTP Newsletter, 1 January – 31 March 2024, https://www.un.org/cttravel/sites/www.un.org.cttravel/files/un_ct_travel_programme_quarterly_newsletter_-_2024_q1.pdf

3. Supporting capacity to surveil travellers

A growing number of countries have fully operational capacity to process API and PNR data.[15] However, it is telling that the CTED's own assessment of fifteen states in Africa has identified significant lack of resources to set the most basic border management security, including the lack of electricity, basic infrastructure, and information and communications technology.[16] Beyond the resources and technical requirements necessary, the expansion of travellers' surveillance has raised significant data security and human rights concerns.[17]

Given the large, growing number of UN Member States it supports, the CTTP has a significant responsibility to ensure that its support in expanding the capacities of states to process API and PNR data does not lead to human rights violations associated with state surveillance. As the following sections describe, PI is concerned that the CTTP is failing in its responsibility in many ways.

[15] See ICAO Working Paper, UNOCT/ICAO Collaborative work on the implementation of API and PNR and proposals for additional capacity building, 23 December 2023, https://www.icao.int/Meetings/FALP/Documents/FALP13-2024/FALP13-WP6.EN.pdf

[16] The April 2024 trend alert on counter-terrorism and border management in Africa summarises CTED assessments of the following countries: Benin, Burkina Faso, Côte d'Ivoire, the Democratic Republic of the Congo, Equatorial Guinea, Ghana, Mali, Morocco, Mozambique, Niger, Nigeria, South Africa, Sudan, Togo, and Uganda. CTED, Counter-terrorism and border management in Africa, Technical and capacity-related gaps, April 2024, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ct_border_technical_and_capacity-related_gaps_-_april_2024.pdf

[17] D. Korff and M. Georges, 'Passenger Name Records, Data Mining and Data Protection: The Need for Strong Safeguards', report prepared for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe, June 2015, available at https://rm.coe.int/16806a601b

3.1 Mission creep

As with many other counter-terrorism surveillance policies, passengers' surveillance has expanded and is expanding in purpose and scope.

As for **purpose**, the UN Security Council resolution originally mandated the collection and analysis of API and PNR data 'for the purpose of preventing, detecting and investigation terrorist offences and related travel'.[18] Two years later it broadened the purpose to 'stop terrorist travel and prosecute terrorism and organized crime, whether domestic or transnational'.[19]

The CTTP stated objective is to "assist Member States in building their capacities to prevent, detect, investigate and prosecute terrorist offences and other serious crimes, including their related travel".[20]

Terrorist offences, organized crime, serious crimes: none of these terms are defined, with the associated risk of allowing governments to dictate the range of conducts which justify surveillance measures on travellers. The use of broad, vaguely defined terrorist offences and the criminalisation of legitimate exercise of human rights in the name of countering terrorism by governments around the world have long been a well-documented concern.[21] The human rights consequences of subjecting individuals

[18] UN Security Council Resolution 2396 (2017).

[19] UN Security Council Resolution 2482 (2019).

[20] CTTP, Building the Capacity of Member States to Prevent, Detect and Investigate Terrorist Offenses and Related Travel by Using Advance Passenger Information (API) and Passenger Name Record (PNR) Data, https://www.un.org/cttravel/content/summary. See also UNCCT ProDoc New API and PNR_10.09.2018 p.8, quoted in UN CTTP Mid-term Joint Evaluation Report, UNCCT-2018-02-82, March 2023, https://www.unodc.org/documents/evaluation/indepth-evaluations/2023/Midterm_Joint_Evaluation_Report_UN_Countering_Terrrorist_Travel_Programme.pdf

[21] Inter alia, UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Global Study on the impact of counter terrorism measures on civil society and civic space, UN doc. A/78/520, 10 October 2023, https://www.ohchr.org/en/documents/thematic-reports/a78520-report-special-rapporteur-promotion-and-protection-human-rights. See also Council of Europe's Commissioner for Human Rights, Misuse of anti-terror legislation threatens freedom of expression, https://www.coe.int/en/web/commissioner/-/misuse-of-anti-terror-legislation-threatens-freedom-of-expression

to travellers' data surveillance of the type supported by the CTTP can therefore be serious and wider-ranging, affecting the right to privacy and a range of other human rights, such as freedom of movement and the right to seek asylum, freedom from arbitrary arrest, and freedom of expression.[22]

One just needs to look at the current list of Member States beneficiaries of the CTTP to identify many whose counter-terrorist legislation and policies have been used to repress dissent and curtail human rights. The UN Special Rapporteur on Countering Terrorism and Human Rights noted Sudan, subject to UN Security Council sanctions, as well as Azerbaijan, the DRC, Ethiopia, Guatemala, Kazakhstan, Mali, Nigeria, Sri Lanka, Tajikistan and Vietnam as beneficiary States in respect of which a wide spectrum of human rights violations have been documented.[23] Other UN Member States beneficiaries have also been singled out by UN or other independent human rights monitoring mechanisms for significant human rights concerns related to their counter-terrorism legislation and practices.[24]

As for **scope**, some UN publicly available documents suggest that the CTTP is seeking to expand beyond air travel, notably into processing of API and PNR maritime data, as well as international high-speed rail and coach travel.[25]

[22] For an outline of main human rights concerns associated with the processing of API and PNR data, see 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, 30 October 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023-10-30-a-ct-travel-gotravel-position-paper.pdf

[23] 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, 30 October 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023-10-30-a-ct-travel-gotravel-position-paper.pdf

[24] See, for example, the Universal Periodic Review of the Philippines, Compilation of information prepared by the Office of the United Nations High Commissioner for Human Rights, 26 August 2022, UN doc. A/HRC/WG.6/41/PHL/2, https://www.ohchr.org/en/hr-bodies/upr/ph-index

[25] OCT, Annual Report 2022 for the government and the Shura Council of the State of Qatar, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/qatar_annual_report_2022_en.pdf

There is a concerning sense of inevitability in this expansion to support states to meet their obligations under relevant UN Security Council resolutions. As aptly described in the mid-term evaluation report of the CTTP: "The programme has understood a MS [Member State] need to address Serious Crime travel and collect maritime API/PNR data. With the programme being identified as utilising the 'One-UN' approach to its advantage, the movement of the programme into these areas is logical given the UN (and other) expertise upon which it can draw."[26]

More chillingly, CTTP priorities for 2023, as reported by OCT in its annual report to Qatar, one of the programme main donors, included to "expand its scope to support comprehensive border management that integrates API and PNR for air, maritime, rail and road/bus travel and will continue its technical development, including compatibility with external solutions, incorporation of biometrics, data analytics, artificial intelligence, and machine learning".[27]

3.2 Interoperability

Interoperability facilitates mission creep in so far as it enables the linking of datasets set up for different purposes. And according to publicly available information, the CTTP seeks to support interoperability of its goTravel software solution. Notably, it aims to develop integration module to "enable [Passenger Information Units] PIUs and other stakeholders to cooperate, coordinate and exchange information domestically and internationally. The Integration module will interface goTravel with national and international databases including the watchlist system, INTERPOL's I-24/7, MIDAS and

[26] CTTP Mid-term Joint Evaluation Report, UNCCT-2018-02-82, March 2023, https://www.unodc.org/documents/evaluation/indepth-evaluations/2023/Midterm_Joint_Evaluation_Report_UN_Countering_Terrrorist_Travel_Programme.pdf

[27] OCT, Annual Report 2022 for the government and the Shura Council of the State of Qatar, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/qatar_annual_report_2022_en.pdf

PISCES through the middleware goConnect and PIU Matching Interface."[28]

Interoperability, integration, synergies - these neutral, reassuringly sounding terms are a sure sign of mission creep and raise red flags about the risk of processing personal data for incompatible purposes.

A telling example of this concern is the ongoing collaboration between CTTP and the Immigration and Border Management programming of IOM. With the signing of a Memorandum of Agreement (MoA), the IOM became a fully-fledged partner of the CTTP in January 2022.

While the text of the MoA is not public, the partnership is said "to promote the joint delivery at country level programming, where API intersects strongly with ongoing IOM migration governance support in areas such as border security or countering migrant smuggling, especially in countries where the IOM Border Management Information System (MIDAS) is operational".[29]

The IOM describes MIDAS as a "fully customizable Border Management Information System", capable of capturing, inter alia, biographical data and biometric data of travellers as well as API data.[30] MIDAS processes biometric data such as fingerprints and facial images collected from travellers at borders. It "automatically checks all recorded entry and exit data against national and INTERPOL Alert Lists".[31] Its intended purpose is extremely wide and vague, covering border security as well as managing/monitoring migration flows. Giacomo Zandonini describes the IOM's MIDAS biometric

[28] See CTTP, goTravel FAQ 3.12, https://www.un.org/cttravel/faq

[29] OCT and IOM, Press Release, Memorandum of Agreement IOM and UNOCT sign an agreement to collaborate on API/PNR technical assistance, 28 January 2022, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20220128_moa_cttravel_iom_press_release.pdf

[30] IOM, MIDAS: a comprehensive and affordable border management information system, https://www.iom.int/sites/g/files/tmzbdl486/files/documents/midas-brochure18-v7-en_digitall.pdf

[31] IOM, MIDAS: a comprehensive and affordable border management information system, https://www.iom.int/sites/g/files/tmzbdl486/files/documents/2023-08/2023_midas-brochure-updated_en-1-161.pdf

border management database as a "rugged, low-cost solution to monitor migration flows" which itself has been heavily employing interoperability.[32]

This cavalier attitude towards the principle of purpose limitation, one of the central tenets of data protection,[33] is concerning because the necessity and proportionality considerations that may allow the use of certain privacy intrusive surveillance measures for counter-terrorism purposes are entirely different from those applicable to other legitimate aims, such as monitoring migration flows. Concretely the risk is casting the surveillance net far too wide and treating any individuals crossing international borders as potential terrorist suspects. The fact that IOM's MIDAS operates in many of the UN Member States beneficiaries of the CTTP and therefore potential future recipients of the goTravel software solution further heightens the risk of misuse of travellers' data.[34]

3.3 Specific concerns related to the goTravel software

The goTravel software solution is a very significant feature in the vast array of support that the UN counter-terrorism programmes offers to UN Member States.[35] It is significant because it provides technical capabilities to beneficiary Member States that enable to process travellers' data.

[32] Giacomo Zandonini, "Biometrics: The new frontier of EU migration policy in Niger" in The New Humanitarian (2019) https://www.thenewhumanitarian.org/news-feature/2019/06/06/biometrics-new-frontier-eu-migration-policy-niger

[33] PI, "The Keys to Data Protection: Part 3 – Data Protection Principles" (2018) https://privacyinternational.org/report/2240/part-3-data-protection-principles

[34] For list of countries operating MIDAS, see IOM, MIDAS, a comprehensive and affordable border management information system, https://www.iom.int/sites/g/files/tmzbdl486/files/documents/2023-08/2023_midas-brochure-updated_en-1-161.pdf

[35] It might not be unique for long, given the announcement that another UN counter-terrorism project, Global Programme on Detecting, Preventing and Countering the Financing of Terrorism (CFT Programme), is "developing the "goFintel" software in collaboration with the Office of Information and Communication Technology (OICT) in order to assist requesting Member States in their efforts to cooperate and appropriately target financial transactions that could potentially be utilized to finance terrorism". OCT, Countering the financing of terrorism, https://www.un.org/counterterrorism/cct/countering-the-financing-of-terrorism

PI understands that as of October 2024, three countries, Botswana, Mongolia and Norway are using the goTravel software solution for live operations.[36] Publicly available information suggests that 10 countries are in 'pre-production testing' with goTravel.[37]

The CTTP claims that privacy and data protection safeguards are embedded in the goTravel software solution. For example, it claims that "privacy sensitive data (like dietary preferences) contained in the Passenger Name Record (PNR) data sets are filtered out and cannot be used for rule-based targeting easing Member State's efforts to remain in compliance with human rights and privacy protection international standards."[38]

However, based on the information publicly available, PI has the following concerns related to the goTravel software solution.

[36] Norway launches passenger information unit with the support of the United Nations Countering Terrorist Travel Programme, 30 September 2022, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/norway_official_launch_of_piu_and_golive_of_gotravel_-_press_release.pdf; Botswana, 23 November 2022, https://twitter.com/UN_OCT/status/1595547957939544067; Mongolia launches passenger information unit with the support of the United Nations Countering Terrorist Travel Programme, 1 December 2023, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20231201_press_release_unoct_ct_travel_programme_piu_inauguration_in_mongolia.pdf

[37] See CTTP Newsletter, 1 January – 31 March 2024, https://www.un.org/cttravel/sites/www.un.org.cttravel/files/un_ct_travel_programme_quarterly_newsletter_-_2024_q1.pdf. The Mid-term joint evaluation report on the UN CTTP published in March 2023 listed the following countries where CTTP initiated pre-production deployment of goTravel software in respective testing environments: Azerbaijan, Côte d'Ivoire, the Gambia, Morocco, the Philippines, the Sudan, Switzerland, Norway plus CARICOM on behalf of its 15 Member States. UN CTTP Mid-term Joint Evaluation Report, UNCCT-2018-02-82, March 2023, https://www.unodc.org/documents/evaluation/in-depth-evaluations/2023/Midterm_Joint_Evaluation_Report_UN_Countering_Terrrorist_Travel_Programme.pdf. The UN OCT, Annual Report 2022 for the government and the Shura Council of the State of Qatar, instead notes the programme "initiated pre-production deployments of the goTravel software in testing environments in Moldova, Sierra Leone, the Philippines, Luxembourg, Mongolia, and Namibia"

[38] UN CTTP, goTravel FAQ 3.6, https://www.un.org/cttravel/faq

- **Data retention**

Data retention periods are entirely dependent on Member States legislation.[39] The Court of Justice of the European Union has noted with concern how "the effect of a retention period [of 5 years] is that a very large part of the population of the European Union is liable to have its PNR data retained, repeatedly, […] and, accordingly, be accessible for analyses carried out in the context of advance and subsequent assessments by the PIU and competent authorities over a considerable – even indefinite – period of time, in the case of persons who travel by air more than once every five years."[40] It further noted that "the continued storage of the PNR data of all air passengers after the initial period of six months is not therefore limited to what is strictly necessary."[41]

'Depersonalisation' or 'masking' of data which is contemplated for PNR data processing[42] included in the goTravel software solution is not full anonymisation and can hardly be considered an effective safeguard against abuses if it is not accompanied by robust procedures to limit the demasking, such as being subjected to judicial or other independent authorisation, justified on a clear legal basis. Further, the 'masked' data may still lead to identification of individuals.[43]

[39] "The system can be configured so that data is stored (and masked) in line with Member State's legal provisions. The data retention provisions are fully configurable within the system depending on the legislation in each individual Member State." CTTP, goTravel FAQ 2.4, https://www.un.org/cttravel/faq

[40] Case C-817/19 Ligue des Droits Humains v Conseil des Ministres ECLI:EU:C:2022:491, para 110, https://curia.europa.eu/juris/document/document.jsf;jsessionid=AB7512C2D94F06AD226B884E431210B1?text=&docid=261282&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=143815

[41] Case C-817/19 Ligue des Droits Humains v Conseil des Ministres ECLI:EU:C:2022:491, para 258.

[42] CTTP, goTravel FAQ 2.4, https://www.un.org/cttravel/faq

[43] Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, "Estimating the success of re- identifications in incomplete datasets using generative models", 23 July 2019, https://www.nature.com/articles/s41467-019-10933-3.

- **Data Security**

The concern related to re-identification is compounded by the fact that most key security safeguards in the goTravel software are entirely conditional on the way that beneficiary UN Member States choose to implement them. In particular, goTravel software solution is deployed and hosted within UN Member States' data centers or in their own cloud-based environment. Member States also define which domestic authorities have access to the data. It follows that the security of the data against unauthorised access or accidental loss as well as the sharing of data across government agencies would depend on UN Member States' own legislation, policies and infrastructures.[44]

- **Profiling**

The functionalities of the goTravel software described in the section above suggest that the software is able not only to identify whether the passengers' data match that of an individual in a watchlist, but also to flag individuals for their potential risks even if they are not already included in a watchlist. These steps would amount to profiling of individuals on the basis of PNR data.

The probabilistic nature of profiling, with the associated consequence of false negative and false positive outcomes, the risk of discrimination resulting from biased data or flawed algorithmic decision-making are all factors that caution against profiling, particularly when the consequences

[44] See concerns expressed by the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism in her Position Paper on the United Nations Countering Terrorist Travel ('CT Travel') Programme and the goTravel Software Solution, 30 October 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023-10-30-a-ct-travel-gotravel-position-paper.pdf

can have such significant effects on individuals' human rights.[45] As noted by the Court of Justice of the European Union, "the number of positive matches from automated processing [...] which prove to be incorrect following individual review by non-automated means is fairly substantial".[46]

- **AI and Machine learning**

PI is also concerned by the potential scope to develop goTravel software to incorporate Artificial Intelligence and machine learning.[47] The Court of Justice of the European Union (CJEU) has clearly articulated the risks related to using AI or machine learning technologies for processing PNR data, noting that "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."[48]

[45] For an analysis of fallacy rate as applied to the processing of PNR data, see Douwe Korff, Did the PNR judgment address the core issues raised by mass surveillance?, 27 November 2023, https://onlinelibrary.wiley.com/doi/epdf/10.1111/eulj.12480

[46] Case C-817/19 Ligue des Droits Humains v Conseil des Ministres ECLI:EU:C:2022:491, para 106, https://curia.europa.eu/juris/document/document.jsf;jsessionid=AB7512C2D94F06AD226B884E431210B1?text=&docid=261282&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=143815

[47] "AI capabilities are currently not available and might be engineered in the next generation of goTravel. AI might be introduced within a supervised environment and relevant algorithms that might be enabled in future will be producing results that will have to be vetted and actioned (or otherwise) by PIU human operators", CTTP, goTravel FAQ 3.8, https://www.un.org/cttravel/faq. See also the stated 2023 priorities for the CTTP: "CT Travel [...] will continue its technical development, including compatibility with external solutions, incorporation of biometrics, data analytics, artificial intelligence, and machine learning." OCT, Annual Report 2022 for the government and the Shura Council of the State of Qatar, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/qatar_annual_report_2022_en.pdf

[48] Case C-817/19 Ligue des Droits Humains v Conseil des Ministres ECLI:EU:C:2022:491, https://curia.europa.eu/juris/document/document.jsf;jsessionid=AB7512C2D94F06AD226B884E431210B1?text=&docid=261282&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=143815

Is the CTTP a joint data controller?

It is unclear from the information publicly available whether the CTTP may be considered a joint data controller[49] in relation to API and PNR data processed via the goTravel software solution.

The goTravel software solution is provided to Member States free of charge and is deployed within Member States' administrations, in Member States' data centers. CTTP claims that "the UN does not have access to the data managed by these solutions", but they are "centrally maintained by UNOCT to ensure seamless operations".[50] The UN further notes that it only processes personal data in very limited range of circumstances when the relevant state authorities (the Passenger Information Unit) allow them to carry out specific activities on the data.[51]

However, the CTTP has developed the goTravel software (updating it from the original version received from the Netherlands) and continues to update it to allow to process passengers' data and to provide its main functionalities. Further, OCT "develops and maintains goTravel's source code under the neutral United Nations "Blue Flag", with guidance from Member States who are using goTravel and are the key drivers for platform enhancements and new software

[49] "Joint controllership" is a concept found in various countries' data protection frameworks, such as in Article 26 of the EU General Data Protection Regulation which defines joint controllers as "two or more controllers jointly determine the purposes and means of processing".

[50] CTTP goTravel software solution, https://www.un.org/cttravel/goTravel

[51] According to the UN CTTP website "the UN does not have mandate to access data on passengers travelling in any country in the world. The Country's Passenger Information Unit is the passengers' data owner. goTravel processes and procedures ensure that no UN staff members obtain access to goTravel (and any other) production systems and data, unless specifically authorized by the data owner to carry out specific, authorized, and time-bound set of activities (e.g. in case of troubleshooting problems and/or implementing emergency changes in systems for which UN staff's intervention is required).", CTTP, goTravel FAQ 2.5, https://www.un.org/cttravel/faq

features through established governance in the form of the goTravel International User Community."[52]

This suggests that the CTTP can determine how the goTravel software process the personal data by the software design choices it makes. Depending on the extent of its control over the way data is processed, the CTTP may therefore be considered as a joint controller (together with the relevant PIU), triggering a range of significant responsibilities.

For example, under the European Union's General Data Protection Regulation (EU GDPR),[53] joint controllers are those who "jointly determine the purpose and means of processing" (Article 26). The European Data Protection Board (EDPB), in its guidelines on the concepts controller and processor in the EU GDPR,[54] provides that joint controllership "can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing". Importantly, "[i]t is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller". Recent jurisprudence of the CJEU also adopts a wide understanding of joint controllership.[55]

[52] CTTP goTravel software solution, https://www.un.org/cttravel/goTravel

[53] Regulation (EU) 2016/679.

[54] EDPB, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0" (2020) https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

[55] See for example Tietosuojavaltuutettu v Jehovan todistajat – uskonnollinen yhdyskunta (C-25/17) and Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17).

If it were a joint controller, the CTTP would be responsible (jointly with the relevant Member State) to comply with the UN data protection and privacy policy,[56] including ensuring security of the personal data and that individuals can exercise their data protection rights (such as access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making), maintaining records of data processing and carrying out data protection impact assessments. The CTTP and the relevant national authority should also have a transparent, publicly available arrangement to set up their respective roles.

While there are claims that UN agencies are exempt from national or regional data protection laws, this is not settled and laws like the EU GDPR do not make express exemption for UN agencies.[57] The CTTP may also carry additional responsibilities under relevant Member States' data protection legislation, such as implementing appropriate technical and organisational measures to ensure that processing is performed in accordance with the relevant legislation, enabling the exercise of data subjects' rights, or providing relevant information to data subjects.[58]

3.4 Inadequate legislation

Under the CTTP, the UN Office on Drugs and Crime (ODC) is providing beneficiary Member States with legislative assistance to establish the laws governing the processing of API and PNR data and the establishment of

[56] UN doc ST/SGB/2024/1.

[57] Petruta Pirvan, "EU GDPR applicability to international organizations" in IAPP News (2021) https://iapp.org/news/a/eu-gdpr-applicability-to-international-organizations

[58] See for example Article 24 Regulation (EU) 2016/679.

Passenger Information Units.[59] Since the programme started, ODC has conducted legislative reviews and assisted in drafting laws of at least a dozen countries.[60] ODC has also developed legislative recommendations in the form of Recommended Provisions on the Collection, Processing, Use, Transfer, Retention and Protection of API and PNR. Regretfully, these Recommended Provisions are not public.

While PI is not in a position to assess to what extent ODC legislative assistance has contributed to changes in national laws, PI is concerned that data protection legislation of some of the UN Member States currently receiving support by the UN CTTP are often non-existent or inadequate to ensure that the processing of API and PNR data complies with the right to privacy, including the protection of personal data.

Further, even when data protection laws are in place, they often include exemptions on national security grounds, or simply to not apply to processing of personal data by law enforcement and intelligence agencies, including those responsible for processing API and PNR data (such as the Passenger Information Units.)

For example, while the Philippines, a country that is receiving support by the CTTP, has enacted a data protection law, in the form of the Privacy Data Act in 2012,[61] the law does not effectively regulate the processing of API and PNR data. Firstly, the Act expressly excludes from its scope information

[59] See https://www.un.org/cttravel/sites/www.un.org.cttravel/files/general/english_ct_travel_summary_1.pdf

[60] Information is hard to come by, but the following countries are mentioned in publicly available documents as recipients of such legal assistance: Azerbaijan, Botswana, Djibuti, Côte d'Ivoire, France, The Gambia, Mongolia, Sierra Leone, South Africa, Switzerland, Togo, Samoa, the Sudan (Respectively: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/qatar_annual_report_2022_en.pdf; https://www.un.org/cttravel/sites/www.un.org.cttravel/files/ct_travel_programme_2023_q3_newsletter.pdf; https://www.un.org/cttravel/sites/www.un.org.cttravel/files/ct_travel_2023_q2_newsletter.pdf; https://www.un.org/cttravel/sites/www.un.org.cttravel/files/ct_travel_programme_2022_q4_newsletter.pdf; https://www.un.org/cttravel/sites/www.un.org.cttravel/files/ct_travel_programme_2022_q3_newsletter.pdf; https://www.un.org/cttravel/sites/www.un.org.cttravel/files/ct_travel_programme_2021_q4_newsletter.pdf).

[61] Data Privacy Act (Rep. Act No. 10173), https://privacy.gov.ph/wp-content/uploads/2024/06/DPA-of-2012_1.pdf

deemed necessary for public authorities to carry out their functions,[62] and under the law's implementing rules, law enforcement and regulatory agencies are among those considered as public authorities.[63] Secondly, even assuming the Act may apply to the processing of API and PNR data, the law permits such processing if necessary to address public order and safety concerns,[64] or that it involves the transfer of data to the government or a public authority.[65] The National Privacy Commission, the country's data protection authority, has made it easier for state actors to engage in data sharing by setting aside the need for data sharing agreements as a prerequisite for data sharing involving government agencies. From a mandatory requirement, the Commission now treats the same as mere best practice.[66] It is also worth noting that the Commission has yet to sanction any entity for committing data protection-related violations since its establishment in 2016. This, despite frequent reports of personal data breaches and other related offenses, including those involving government entities and their personnel.

PI recommends that adequate national data protection law shall apply in relation to the processing of API and PNR data and such law should, at the minimum:

- incorporate the data protection principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitations; integrity and confidentiality; and accountability;
- ensure that every individual, irrespective of their nationality, enjoy the full range of data protection rights, including having the rights of information, access, rectification, erasure, restriction of processing, and to

[62] Rep. Act No. 10173, §4(e).

[63] Implementing Rules and Regulations of Rep. Act No. 10173, §3.r.

[64] Rep. Act No. 10173, §12(e).

[65] Rep. Act No. 10173, §13(f).

[66] NPC Circular No. 2020-03, §8.

compensation and judicial redress;

- provide for an independent data protection authority with powers and resources to receive complaints, investigate reports of abuses and impose adequate sanctions.[67]

In the absence of adequate, applicable national data protection legislation, API and PNR data should not be processed.

3.5 Information sharing without adequate safeguards

The UN Security Council Resolution 2396 (2017) "encourages Member States to share PNR data with relevant or concerned Member States."[68]

As noted in the CTTP information material, national "legal systems differ on key issues pertaining to the collection, transmission, use, retention and sharing of passenger data" and the conflict of laws related to the sharing of personal data between country of departure and destination, which unresolved "prevents the optimal use of PNR data, including for purposes of counter-terrorism".[69] Indeed, the level of protection of personal data varies across countries and it is a central tenet of international human rights law and of modern, effective data protection laws to ensure that transfer of personal data to third countries do not amount to or facilitate human rights abuses, including unlawful interference with the right to privacy.[70] So it should be clearly stated in laws and consistently applied in practice that

[67] For details of data protection principles and safeguards, PI, Data Protection Guide, 2018, https://privacyinternational.org/data-protection-guide

[68] Security Council Resolution 2396 (2017), https://www.un.org/securitycouncil/content/sres23962017

[69] CTTP, Counter-Terrorism Travel Programme Summary Building the Capacity of Member States to Prevent, Detect and Investigate Terrorist Offenses and Related Travel by Using Advance Passenger Information (API) and Passenger Name Record (PNR) Data, https://www.un.org/cttravel/sites/www.un.org.cttravel/files/general/english_ct_travel_summary_1.pdf

[70] See, inter alia, report of the UN High Commissioner for Human Rights on the right to privacy in the digital age, para 32, UN doc: A/HRC/39/29.

personal data, such as API and PNR, cannot be transferred to countries which do not guarantee adequate protection.

The emphasis on data sharing with other countries is reflected in the goTravel software solution which supports "the integration of a data sharing module to share data within the national competent authorities and with other goTravel instances in other countries".[71] However, it should be noted that the compilation of watchlists with names and other personal data of individuals as well as parameters of 'risk indicators' to be used for profiling purposes is entirely at the discretion of national state authorities.[72]

PI recognises the importance and benefit of sharing information in the context of preventing and investigating acts of terrorism or other genuine, serious threats to national security. PI is concerned, however, that unregulated, unfettered and unwarranted intelligence sharing poses substantive risks to human rights and to the rule of law.[73]

3.6 Insufficient capacity for independent monitoring

Perhaps the most concerning aspect of the CTTP is that once the goTravel software solution is released to a state, there is no effective mechanism of international, independent oversight of its use, nor, it seems, the possibility to recall the software should credible allegations of human rights abuses

[71] CTTP goTravel software solution, https://www.un.org/cttravel/goTravel

[72] As noted by Edward Hasbrouck "importing a blacklist is a drag-and-drop function. There's no provision for recording what official of the receiving government's judiciary or PIU has reviewed and approved the addition to that country's ruleset of a list sent by another country's PIU. No such review is expected. A person flagged as a "suspected terrorist" by any country in the world is expected to be treated as such, without further question, by every other U.N. member." Papers, Please, Precog in a Box, 25 February 2021, https://papersplease.org/wp/2021/02/25/precog-in-a-box/

[73] The potential negative human rights implications of such data sharing are significant. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism highlighted the challenges of data sharing, including of PNR and API data as well as information on watchlists, in a human rights compliant way and she noted that the intelligence-sharing measures "advocated by the Security Council is likely to contribute to greater privacy intrusions, which in turn leads to enhanced risk to the protection of interlinked rights." https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf

emerge. PI understands that CTTP is currently developing some monitoring policies to seek to address this gap.

However, PI believes that this lack of oversight is not accidental. Rather it is a consequence of the way the programme has been set up and of the mandate and capacity of the UN entities leading its implementation.

OCT and ODC do not have a mandate of monitoring implementation of legislation, policies and practices at a national level. During their periodic country visits, CTED do not have the mandate to query the implementation of the agreements (MoU and MoA) underpinning the relationship between the CTTP and a beneficiary Member State. Further the extent of their scrutiny of the human rights impact of processing travellers' data and the extent to which their recommendations are implemented by the relevant state authorities are not publicly available, as reports of CTED country assessments are confidential, unless the state concerned agrees to their publication (which rarely happens).

The Office of the United Nations High Commissioner for Human Rights (OHCHR), which would have the mandate - but rarely the capacity due to resource constraints - to carry out human rights assessments in countries, is not an implementing partner of the CTTP. As for the UN Special Rapporteur on Counter-Terrorism and Human Rights, its resources to carry out country assessments are extremely limited (they are restricted to a maximum of two country missions per year) and they have also been kept on the margins and with limited insight into the programme.[74]

These institutional and capacity constraints within the UN are further

[74] See 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, 30 October 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023-10-30-a-ct-travel-gotravel-position-paper.pdf

compounded by the failure of the CTTP to systematically include civil society organisations in the initial assessment, roll out and follow-up of the programme activities in support of beneficiary UN Member States. As noted in the CTTP midterm joint evaluation report, "there is relatively little engagement with Civil Society Organisations (CSOs), private sector or academia. For example, other than official human rights institutions (which are mostly official and semi-official), there is no engagement with CSOs, nor is there any specific examples of engagement with training institutes or research entities."[75]

3.7 Poor accountability

UN partners implementing the CTTP are bound to comply with the requirements contained in the UN Human Rights Due Diligence Policy, which applies to UN support to "non-United Nations security forces", including "border-control and similar security forces" and "national civilian [...] or military authorities directly responsible for the management, administration or command or control of such forces".[76]

The UN Human Rights Due Diligence Policy's obligations on UN support to security forces include prior human rights risk assessment, transparency and an implementation framework.

PI understands that CTTP is currently developing some policies to ensure its activities are in line with the requirements included in the UN Human Rights Due Diligence Policy. However, based on its assessment of publicly available information, PI believes that the current CTTP fails to adhere to some of

[75] CTTP Mid-term Joint Evaluation Report, UNCCT-2018-02-82, March 2023, https://www.unodc.org/documents/evaluation/indepth-evaluations/2023/Midterm_Joint_Evaluation_Report_UN_Countering_Terrrorist_Travel_Programme.pdf

[76] Human Rights Due Diligence Policy on United Nations Support to Non-UN Security Forces, UN Doc. A/67/775-S/2013/110.

these requirements.

- **Prior human rights risk assessment**

According to available public information, CTED (with ICAO and ODC) conducts "assessment and first 'deep-dive' missions in beneficiary countries".[77] In the absence of any meaningful publicly available information on the scope of these assessments and 'deep-dives',[78] one can only infer from the list of beneficiaries that any prior human rights risk assessment does not seem to have prevented CTTP from supporting a number of States with, in the words of the UN Special Rapporteur on Counter-terrorism and human rights, "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".[79] That fact alone, in the absence of other information, casts significant doubts on the effectiveness and thoroughness of any prior human rights impact assessments.

[77] CTTP, Counter-Terrorism Travel Programme Summary Building the Capacity of Member States to Prevent, Detect and Investigate Terrorist Offenses and Related Travel by Using Advance Passenger Information (API) and Passenger Name Record (PNR) Data, https://www.un.org/cttravel/sites/www.un.org.cttravel/files/general/english_ct_travel_summary_1.pdf

[78] The UN Special Rapporteur refers to a non-publicly available technical questionnaire "which indicates that information 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." 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, 30 October 2023, para 55, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023-10-30-a-ct-travel-gotravel-position-paper.pdf

[79] Position Paper of the UN 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, 30 October 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023-10-30-a-ct-travel-gotravel-position-paper.pdf, para 56, and https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023-10-30-a-ct-travel-gotravel-position-paper.pdf

- **Implementation process**

The implementation process outlined in the UN Human Rights Due Diligence Policy puts significant focus on setting up processes to monitor "recipient entity's compliance with international humanitarian, human rights and refugee law",[80] including collection and review of information from UN and non-UN sources, "including local protection of civilian networks".[81] As noted in the section above, these elements are currently deficient in the CTTP set up and make effective monitoring of human rights compliance of the beneficiary PIUs and other state security forces virtually non-existent.

The UN Human Rights Due Diligence Policy further requires the The UN Human Rights Due Diligence Policy further requires the establishment of "well-defined procedures to guide decisions by responsible United Nations officials on whether or not violations committed by the recipient entity require intervention with the recipient entity or its command elements or, as a final resort, require the suspension or withdrawal of support under this policy".[82] As noted above, PI is concerned that the CTTP may not have the technical capacity to a) assess whether the goTravel software has been used to facilitate a human rights violation, given that the UN has no access to the data processed and that implementation is at the PIU discretion, nor b) withdraw the goTravel software solution from any beneficiary Member States found to have misused it.

[80] Para 2(c)(i) of the UN Human Rights Due Diligence Policy. See also "(c) Mechanisms for the effective monitoring of the recipient's behaviour to detect grave violations of international humanitarian, human rights and refugee law and the recipient institution's responses to any violations;" (para 21(c) the UN Human Rights Due Diligence Policy).

[81] Para 21(d) of the UN Human Rights Due Diligence Policy.

[82] Para 21 (e) of the UN Human Rights Due Diligence Policy.

3.8 Lack of transparency

As noted repeatedly, public information about CTTP is particularly scant. The quarterly newsletters which gave a very broad, but regular overview on the programme activities seem to have been discontinued, while press releases and public statements do not provide details on the activities undertaken by the programme.

In the past three years, PI has sought to engage with the CTTP with the view to obtain more information on the programme activities and to advocate for the inclusion of data protection and other human rights safeguards in its work. In 2021, OCT organised an introductory briefing for PI, and in subsequent meetings and correspondence with OCT and ODC, PI was able to raise concerns and to provide comments on some of CTTP policies on a confidential basis.

While this engagement is welcomed, it does not address the need for significant improvement in transparency and meaningful consultation with civil society organisations and other external experts. Further, PI is concerned by the lack of publicly available documentation of CTTP policies.

PI sought CTTP policies both by requesting them to the OCT and by submitting an access to documents request to the European Commission, being the EU one of the funders of the CTTP. PI was told by OCT that the majority of the non-publicly available information requested relates to specific assistance and cooperation between the United Nations and its Member States and thus cannot be shared without the expressed consent of the Member States.[83] The European Commission motivated the refusal to disclose the information requested by stating that OCT "have objected to disclosure of the documents that they sent to the Commission and have

[83] E-mail from OCT, 14 April 2022, on file with PI.

motivated their position stating that the documents were created by the United Nations and form part of its archives, and are hence inviolable. The authors of the documents have also referred to the provision of article 6.1 of the General Conditions (annex II of their Contribution Agreement signed with the European Commission) which clearly states that the any document, information or other material directly related to the implementation of the action and communicated is considered confidential. The authors have detailed the level of confidentiality which relates in particular to the deliberations between the United Nations and beneficiary Member States on various aspects of the CT Travel Programme. Some of the information contained in the reports is considered sensitive as it pertains to safety and security aspects."[84] Our efforts to receive some clarity regarding this process has been undermined by each organisation invoking the other as the reason for not disclosing information.

[84] See reply by the European Commission, 28 June 2022, https://privacyinternational.org/legal-case-files/5478/pi-un-ct-travel-access-docs-requests

PI understands that the UN Office of Legal Affairs considered some of the information to be privileged information between the UN and Member States. While some operational documents may need to remain confidential, PI sees no reasonable justification for not publishing the following:

- Technical questionnaire and other tools developed by CTED and others to conduct the human rights risk assessments;
- Model Memorandum of Understanding/Memorandum of Agreement and model road map used as basis for to develop country specific ones;
- The Recommended Provisions on the Collection, Processing, Use, Transfer, Retention and Protection of Advanced Passenger Information data ("API") and Passenger Name Record data ("PNR") developed by ODC;
- Guidance Note on human rights issues pertaining to API/PNR.[85]

These are all policies developed by CTTP and not pertaining to specific arrangement with particular UN Member States. They are also prima facie unlikely to include sensitive information that cannot be published for safety or security reasons.

[85] This guidance note was referred to in a document disclosed to PI following freedom of information request to the European Commission.

Similarly, CTTP should regularly publish updated information on the status of implementation of the programme in each beneficiary Member State, including:

- List of UN Member States and organisations which have signed MOU and MOA;
- Legislative support provided, listing the specific national legislation which has been supported and the status of it within each Member State);
- Up-to-date list of authorities testing the goTravel software solution and countries where it is fully operational.

There are also some country specific documents which PI expects should be made public, in line with recognised best practices, such as:

- Data Protection Impact Assessment conducted prior to the roll out of the goTravel software solution;
- Any agreements (including data sharing or processing agreements) between OCT and Member States setting out the terms of provision of the goTravel software;
- Terms of reference of national PIUs.

Finally, PI recommends that CTTP follows growing international practice on data protection standards and seeks beneficiary UN Member States to follow the same. This includes in particular developing and publishing a privacy policy specific to the goTravel software, setting out:

- The types of personal data collected;
- The categories of data subjects;
- The sources of personal data;

- The purpose(s) of processing personal data;
- The lawful basis(es) for processing personal data;
- Any third party recipients of personal data;
- The ability of data subjects to exercise their rights, in particular the right to rectification;
- A data retention policy.

While these various elements may vary across countries, the CTTP should adopt a policy template that reflects the functioning of the goTravel software, and require its adoption by beneficiary Member States.

4. Conclusions and recommendations

The UN counter-terrorism programmes are increasingly supporting UN Member States adopting surveillance technologies in border security to comply with UN Security Council resolutions. In this context, CTTP offers Member States a technical 'solution', the goTravel software, to enable the processing of travellers' data.[86]

On the basis of the limited public available information, PI believes, for the reasons outlined in this briefing, that the CTTP has not put in place the necessary tools to support Member States processing of travellers' data in accordance with international human rights law and it has not demonstrated its compliance with the UN Human Rights Due Diligence policy. As noted above, PI understands that CTTP is developing internal policies which may address some of these concerns. However, PI notes that CTTP is now in its 5th year of existence and has already supported a wide range of Member States to increase their surveillance capacity.

It is imperative that CTTP prioritises human rights protection and safeguards in its support to UN Member States, including by dedicating adequate resources and capacity to establishing independent monitoring mechanisms and improve transparency of its activities. In this regard, donors have a role to play in both ensuring CTTP prioritise human rights protection and in demanding adequate publicly available information to allow scrutiny of their activities.

[86] The UN Security Council resolution 2482 (2019) calls on States to "implement obligations to collect and analyze Advance Passenger Information (API) and develop the ability to collect, process and analyse [...] Passenger Name Record (PNR) data and to ensure PNR data is used by and shared with competent national authorities, with full respect for human rights and fundamental freedoms". Para 15(c).

PI recommends that CTTP:

- Suspends the roll out of the goTravel software solution until CTTP can publicly demonstrate its capacity to monitor its use by beneficiary UN Member States and has developed an effective mechanism to withdraw it if it receives reports of abuses/misuses of the software;
- Develops its capacity to monitor Member States' processing of API and PNR data in accordance with human rights law, including data protection;
- Develops and conducts human rights risk assessments (including data protection impact assessment) prior to providing any assistance to Member States;
- Regularly and meaningfully consults with national civil society organisations and experts during the prior human rights assessments and during the implementation of assistance programmes;
- Publishes the recommended legal provisions and other policy documents and tools used by CTTP to provide assistance to Member States, including but not limited to the documents identified in Section 3.8 above;
- Develops and publish a privacy policy for the goTravel software;
- Updates on a regular basis the list of beneficiary Member States, with details on the status of support, including up-to-date list of authorities testing the goTravel software solution and countries where it is fully operational.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org