

DIGITAL SURVEILLANCE AND COUNTERTERRORISM



28 June 2023

Part 1: Manifestations and Risks



European Center for
Not-for-Profit Law



www.ecnl.org



[@enablingNGOLaw](https://twitter.com/enablingNGOLaw)

The increased use of new technologies in CT

Legal and political enablers: Calls by international organisations to increase data collection and use of surveillance

paired with

Technological enablers: Decline in cost of technology and data storage, ubiquity of devices, increase in computer processing powers

underpinned by

Misguided technosolutionism: the simplistic belief that technology is an easy “fix” to the problem of terrorism



“Policymakers opt instead for simplistic, tired tropes about the causes of violence and propose responses that simply do not work.

It is into this universe that the adoption of new technologies, often sensationalized as the “fix” to the phenomenon of terrorism, which is underdefined or simply not defined at all, occurs.”

UN Special Rapporteur on CT and Human Rights



Three overarching trends

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

- Leveraging of **terrorism as a policy rationale** to adopt high-risk technologies, with **the justification of exceptionality** contaminating legal and policy debates
- **Lack of consistent human rights analysis** and practice in the development, use and transfer of new technologies
- **Normalisation of surveillance**: the move from initial exceptional use of new technologies in narrow security contexts to general use in domestic law enforcement and everyday life



Types of digital surveillance & Impact on civic space

UN SR on CT and Human Rights:

The targeting of civil society is not a random or incidental aspect of counter-terrorism law and practice. It suggests the hard-wiring of misuse into counter-terrorism measures taken by States around the globe.



Underlying enabling practice: ubiquitous data collection



- Increased access of intelligence agencies and law enforcement to data
- Data sharing frameworks
- Specific legal and policy incentives to collect data, e.g. biometric data, travel data



Interception of communications data and metadata from service providers

What does it consist in?

- Gaining access to **the content of communications** hosted by technology and telecommunications companies (such as online communicators or email providers)
- Gaining access to **metadata** – “data about data”, e.g. information about who is making phone calls or using online services, recipients of all, times, location, devices used etc.
- Facilitated by so-called **data retention laws**

Impacts

- enables unprecedented tracking of people’s movements, behaviours and contacts
- people are often unaware of the modalities of private companies disclosing data to law enforcement or intelligence agencies, and hardly ever have a say in the matter
- advertently or not, HRDs, activists, journalists end up in the surveillance dragnet
- repurposing of data collected for CT purposes for domestic surveillance
- chilling effects on freedom of assembly, association and expression





How Bulk Interception Works

PRIVACY
INTERNATIONAL

All communications - emails, phone calls, text messages, social media posts, search engine queries - that use the internet are broken down into small fragments, called packets.



Packets can take any viable route, regardless of distance. Even an email between two people in the same country might travel around the world before it reaches its destination.

Packets making up a single communication may take different paths to reach their destination.

Governments conduct bulk interception by tapping high capacity fibre optic cables, which carry the world's internet communications. Many of these cables are laid under the sea. The TAT-14, for example, is a transatlantic cable system with landing stations in the US, UK, France, Germany, Denmark and the Netherlands.



Spyware

What does it consist in?

- Malicious software that is installed on a device in order to extract information from that device and/or take control thereof, without the end user's knowledge and consent.
- Often initially introduced under the assumption of targeted use against specific individuals or risk groups. However, vague or discriminatory definition of risk groups can lead to expansion beyond the initially stated boundaries.

Impacts

- Allows gaining access to the most intimate details of a person's daily life
- Modern spyware, such as Pegasus, is extremely difficult to detect and existing technical tools make it impossible to prevent its installation
- Violates the essence of the **right to privacy**
- Has been used to deliberately target, intimidate and silence activists, journalists and political opponents – it undermines the very essence of democracy and is a **severe violation of civic freedoms**





Predictive algorithms

What does it consist in?

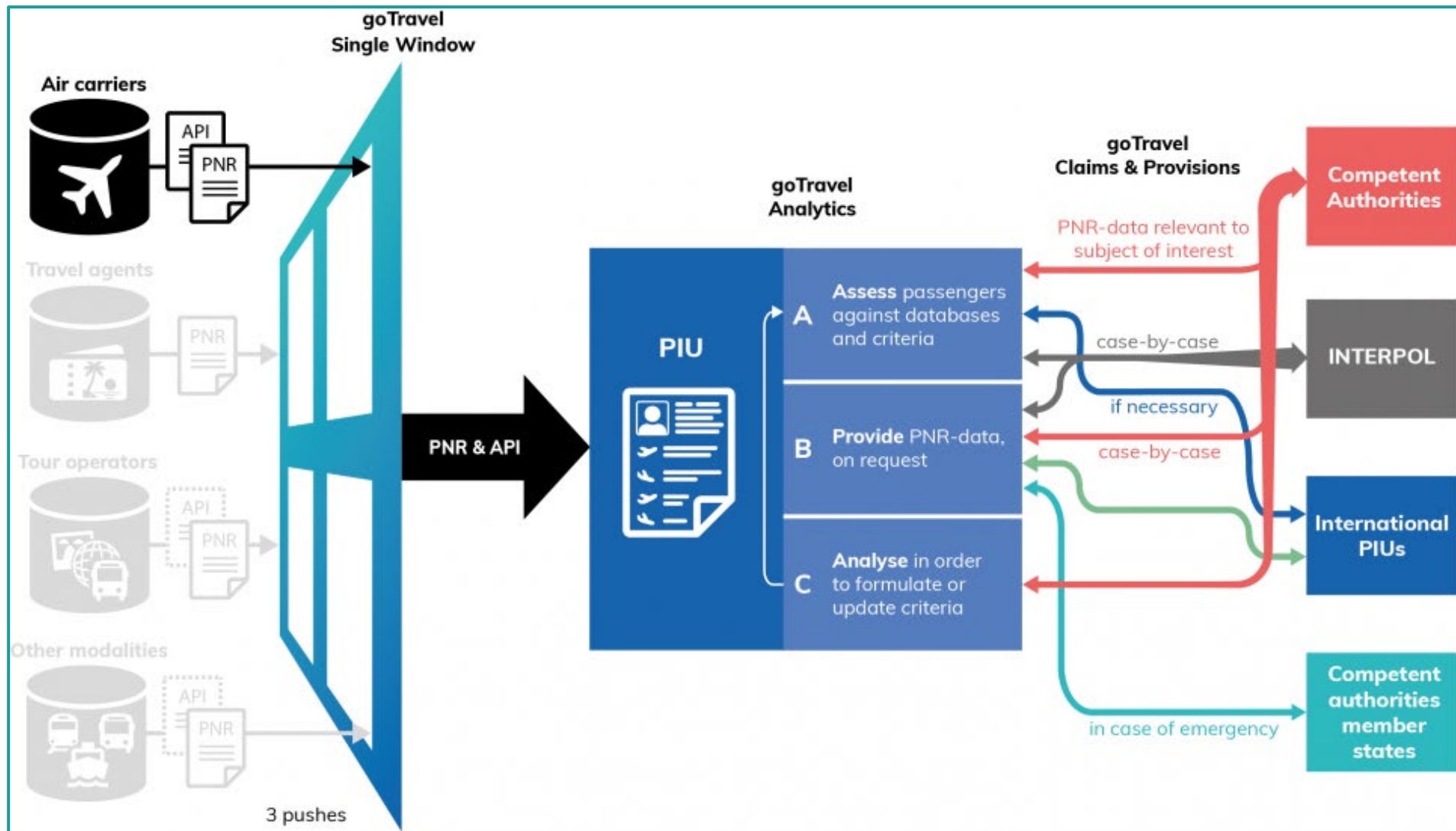
algorithm-driven analysis of large datasets focused on detecting patterns, anomalies, and “suspicious” behaviour in order to:

- **Forecast trends**, e.g. where terrorist attacks will occur
- **Assess the risk** of individuals

Impacts

- can encompass **deliberate government policies** and institutional practices that disadvantage certain groups, for example, treat members of some groups, such as human rights activists, dissidents, or dark-skinned people, as “threats”
- inherently probabilistic nature can lead to false positives (and negatives)
- algorithms trained on biased datasets can lead to **discriminatory outcomes**
- lack of transparency and accountability





Biometrics-based technologies

Biometric data – physical properties of the body and/or behavioural traits, such as fingerprints, face, voice, retina, gait, iris

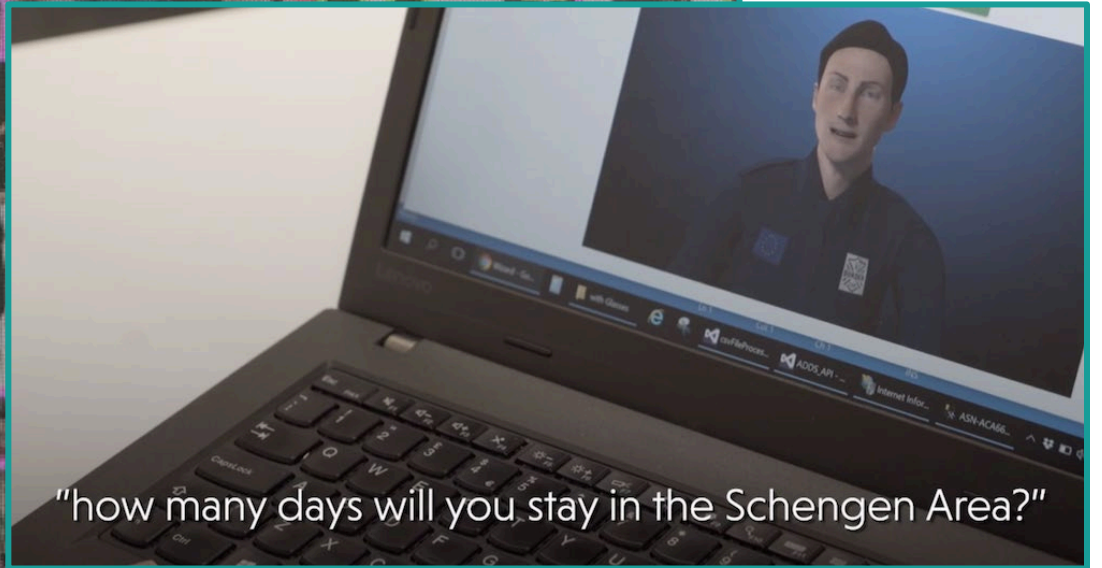
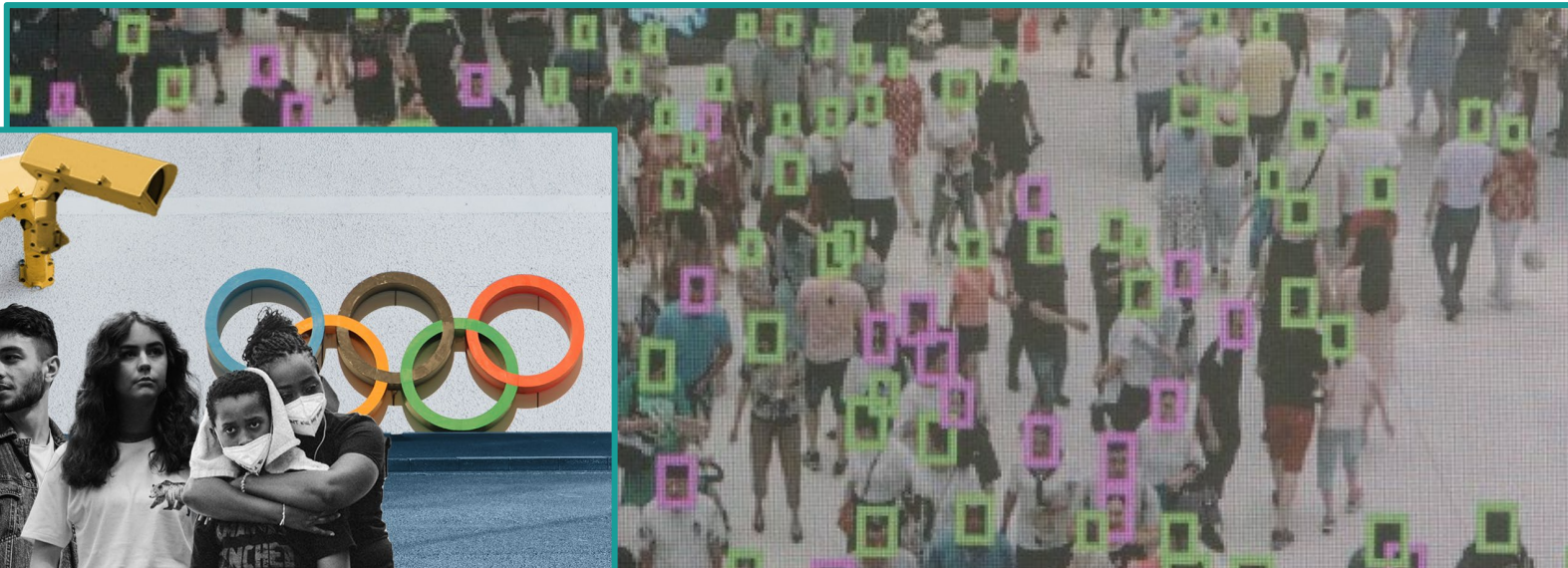
Types of biometric technologies:

- **Biometric identification** – measurement and recording of biometric data for the purposes of usually remote identification, either in real-time or retrospectively
- **Biometric categorisation** – assigning people to groups (e.g. “potential threat”) based on data about their bodies or behaviours
- **Emotion recognition** – analysis of facial expressions with the claim to infer emotional or psychological states

Impacts

- Affects everyone in public spaces and involves collection of data which is difficult to hide and impossible to change or reset. This poses an inherent threat to **the right to privacy**
- **Chilling effects**: the mere existence of indiscriminate biometric surveillance in publicly accessible areas stifles people’s reasonable expectation of anonymity in public spaces and reduces their will and ability to take part in demonstrations and express their views, for fear of being identified, profiled or even wrongly persecuted
- **Discriminatory** outcomes
- Impact on **the right to a fair trial**, incl. presumption of innocence





THANK YOU!

European Center for Not-for-Profit Law
Stichting




 Riviervismarkt 5, 2513 AM, the Hague, Netherlands

 www.ecnl.org

 [@enablingNGOLaw](https://twitter.com/enablingNGOLaw)

 info@ecnl.org

 0031 639029805