Technology and Privacy in the EU Legislation to Fight Terrorism and Other Serious Crimes

Niovi Vavoula

Post-Doctoral Research Assistant, QMUL

Sensing and Privacy Workshop 20/06/2017

Overview of the lecture

- How are **biometric identifiers** deployed at EU level and for what purposes?

- What does the **EUROSUR Regulation** envisage?

- What does the **EU PNR Directive** entail for travellers?

- What are the **fundamental rights concerns** raised by the operation of these schemes?

Biometric identifiers

Immigration databases	Biometric Passports Regulation
Schengen Information System (SIS II) * Full set of fingerprints (subject to change)	EU nationals applying for a passport Two fingerprints and a photo No centralised storage at EU level, but there is such possibility
Visa Information System (VIS) * Full set of fingerprints and photo	
Eurodac * Full set of fingerprints and photo	
Use for a variety of purposes from immigration control to law enforcement	Use for verifying the identity of the passport holder
Lack of proper impact assessment and guarantees that raises proportionality concerns	*Schwarz* judgment

Is centralised storage inherently problematic? The case of *Schwarz* (C-291/12)

- The **bad** news:

  Biometrics is not the best solution, but at the moment it is the best one we have!

- **Good** news for centralised databases?

  1) Only two fingerprints are stored
  2) The passport remains with the owner
  3) Use for verification purposes only
  4) Impact of a false match to an individual

Does centralised storage of biometrics violate the essence of privacy?

- Article 52(1) EU Charter of Fundamental Rights

- Characteristics of databases

1. Millions of records on individuals
2. Possibility of false matches exacerbated by lower quality of data
3. Changing purposes
4. In central systems, whereby the individual loses control over their personal data
5. Long retention periods
6. Changing safeguards (particularly conditions for police access)

The more these features remain, the closest to the core of privacy we get!!

European Border Surveillance System (EUROSUR)

What is it? Computerised network for ‘real-time’ monitoring of land and sea external borders

It allows the collection, exchange and analysis of information

What means? Combination of sources: radars, drones, satellites, ship reporting systems

Ambition: to combine in a single visualisation information flowing from a variety of sources

Improvement of situational awareness and reaction capability with a **threefold purpose**:

a) Detect, prevent and combat *illegal* migration

b) Detect, prevent and combat cross-border crime

c) Save lives (really **not a primary one** though!)

European Border Surveillance System (EUROSUR)

NCC operational in all Schengen MS

NCC **exchange information and coordinate**:

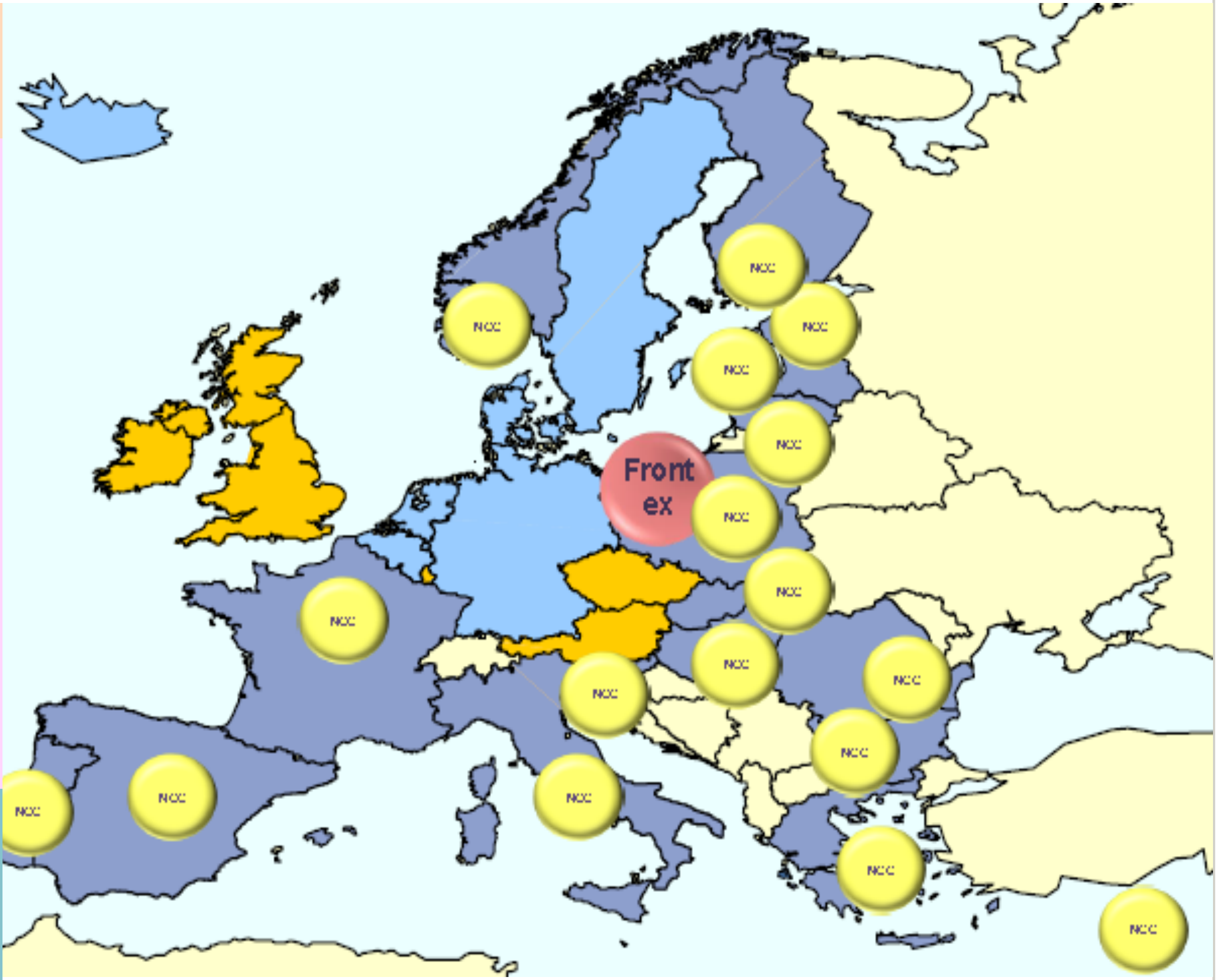
a) between other national *border surveillance* authorities

b) between other NCC

c) with Frontex (EBCG) and ;

maintain the national situational picture

Frontex allows the connection between NCC and maintains the ESP



Is EUROSUR actually working?

In short, **NOT REALLY**

- Difficulties in detecting small vessels and lack of mechanisms to force MS or Frontex to take action
- Component of obliging migrants to resort to unsafe routes and vessels
- 115.000 events recorded in EUROSUR (majority by FRONTEX itself)

≠

- Four ‘operational success stories’

✓ the rescue of 38 people travelling between Morocco and Spain;

✓ the seizure from a cargo ship of some 60 million cigarettes without documents;

✓ the seizure of around 5,000 weapons and 500,000 bullets headed for Libya; and

✓ the detection of rubber boats leaving Libya

Privacy concerns regarding Eurosur

- **Complete lack of rules** regarding the collection, processing and analysis of data at national level
- **Uncertainty** as regards how the Agency analyses the information
- Where is the information stored and for how long?
- Possibility of **exchange of information** between third countries and EU MS (some guarantees on non-refoulement and data protection)

The story behind the EU PNR Directive

- Impact of 9/11
- US legislature requiring airlines to provide PNR data for law enforcement purposes
- PNR data → travel document, destination, credit card details, seat preferences, meals
- EU PNR Agreements with the US, Canada and Australia
- Reciprocity clause
- Two proposals, final adoption 2016

The content of the EU PNR Directive

- Development of Passenger Information Units (PIUs) in EU MS
- Both international and internal flights will be monitored
- Identification of ***previously unknown*** suspect individuals
- **Profiling** at the heart of PIUs' operations (**risk assessment**)
- Retention period: 6 months (then, depersonalisation)

The EU PNR Directive and privacy

- Systematic collection and further processing of personal data in bulk
- Surveillance of **a priori innocent** individuals (*Watson and Digital Rights Ireland*)
- Lack of rules on how PIUs will operate
- Lack of definition of serious crimes (low threshold?)
- Is ‘sufficient indication’ sufficient?
- Random retention periods (lack of proper assessment)

Concluding remarks

- ✓ Strong surveillance of movement through technological instruments
- ✓ Confusion and intertwining between mobility and criminality
- ✓ ‘I travel, therefore, I am a suspect’ logic?
- ✓ Contrast between the case law of the CJEU (*Watson, Digital Rights Ireland*) and the EU legislation and priorities

Thank you for the attention!

Any questions are more than welcome!

n.vavoula@qmul.ac.uk