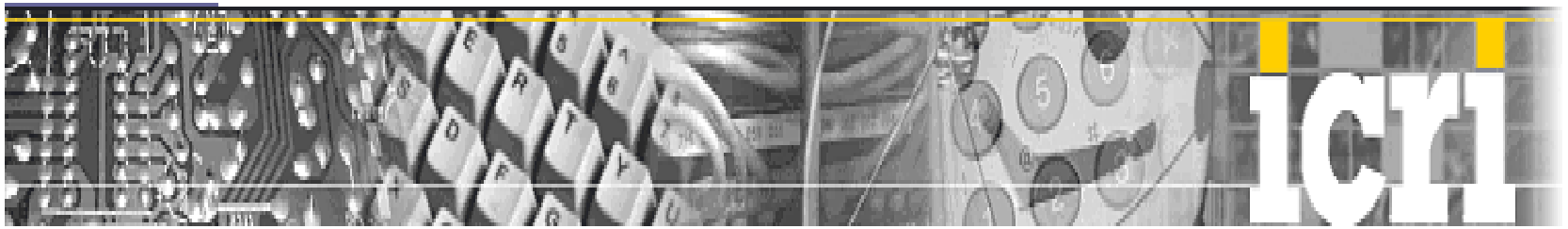


Interconnection of video surveillance networks: balancing the needs of increased security and the right to privacy

Fanny Coudert

Legal Researcher, ICRI – K.U.Leuven

Outline

- Towards a new generation of video surveillance networks: DYVINE prototype
- Main data protection safeguards at stake:
  - Purpose specification principle
  - Proportionality principle
  - Transparency principle
- Proposed solutions

TOWARDS A NEW GENERATION OF VIDEO SURVEILLANCE NETWORKS (VSN)

Videosurveillance Trends

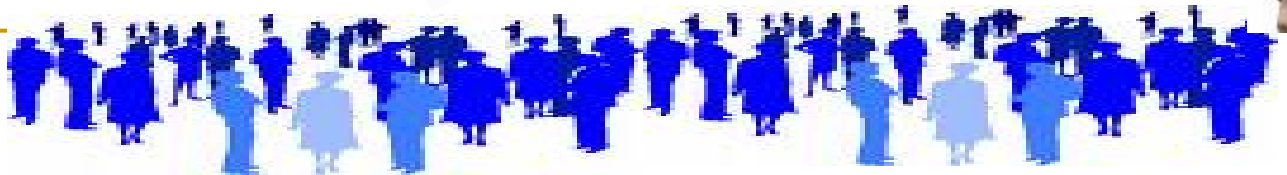
- **Objective:** improve video surveillance efficiency

- **Technological trends:**
  - From fixed to re-configurable networks
  - From CCTV to networked digital surveillance
  - Increased use of intelligent video analytics

DYVINE system

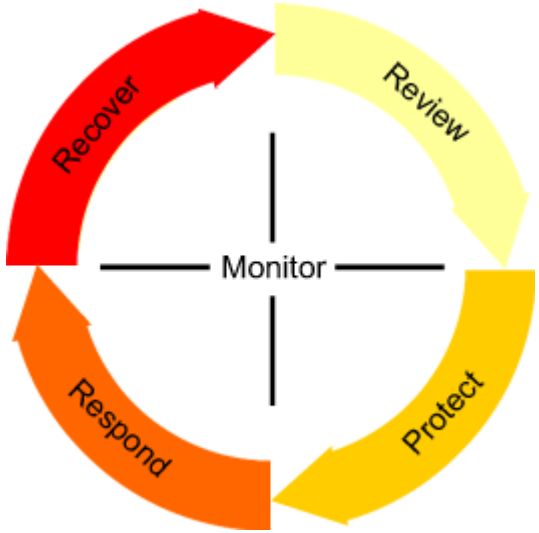
Crisis management (prevention of catastrophes)

PROCESSING



Other possible uses of DYVINE

CRISIS MANAGEMENT: MARIUS



LAW ENFORCEMENT: HITS

Challenges to data protection principles

Role of data protection legislations

The use of **videosurveillance** is by itself a **threat** for **fundamental rights** such as:

- **Privacy**
- **Freedom to come and go anonymously**
- **Freedom of expression**
- Others

Data protection laws aim to secure individuals respect for his rights and fundamental freedoms in the field of processing of personal data.

Core principles of data protection legislations

- Purpose specification
- Proportionality of the processing
- Transparency of the processing to the data subject

1. Purpose specification principle

- *Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*
- Principle of forseeability: *an interference should be formulated with sufficient precision as to enable the citizen to ajust his conduct accordingly*
- To prevent:
  - abusive interconnection of databases
  - Function creep (illicit use of data)

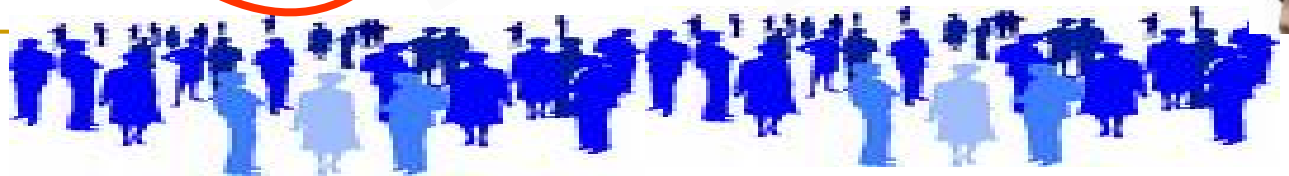
DYVINE: re-use of personal data

Crisis management (natural catastrophe)

PROCESSING

UNDERGROUND

Police



2. Principle of proportionality

- ‘Not using a sledgehammer to crack a nut’:
  - Adequacy test: able to achieve the goal
  - Necessity test: Strictly necessary
  - Proportionality test stricto sensu: Sufficient benefits to overcome the negative impact on fundamental rights
- To prevent the emergence of pervasive surveillance and an increased vulnerability of individuals

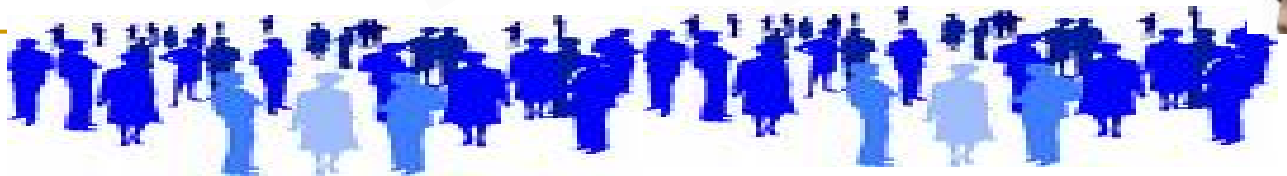
DYVINE: Massive data processing

Crisis management (natural catastrophe)

PROCESSING

UNDERGROUND

Police



3. Transparency

- From right to privacy to the right to data protection
- The individual is at the center of the protection → tools to exercise a control upon the processing:
  - Information right
  - Access, rectification and objection rights

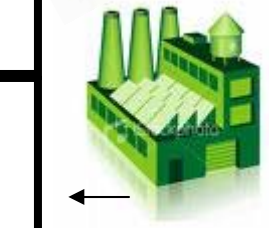
DYVINE: Opaque system

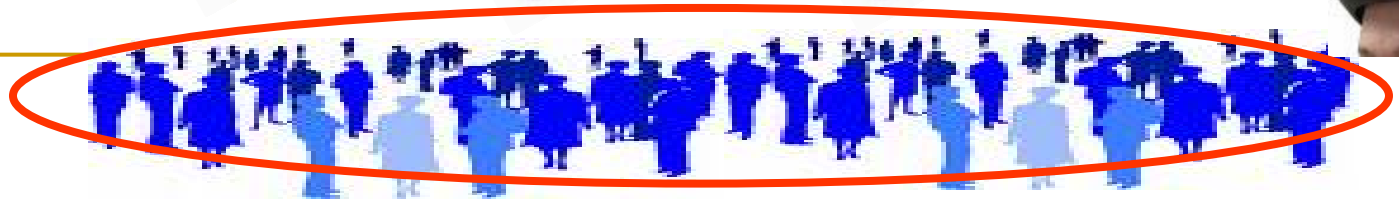
Crisis management (natural catastrophe)

PROCESSING

UNDERGROUND

Police





Solutions proposed

Privacy by design

DORMANT SYSTEM : **Legacy systems are actively linked only when certain pre-defined conditions occur**

ACCES RIGHTS: **Every user can only access the data he/she needs to perform his/her task**

PRE-CONFIGURABLE ALARMS: **Display only suscpicious events/behaviours**

Better application of current safeguards

MANDATORY PRIVACY IMPACT ASSESSMENT :
Helps the controller to identify and manage privacy risks. Prepare the prior checking procedure.

MANDATORY PRIOR CHECKING PROCEDURES :
Increased role of Data Protection Authorities. They would have the opportunity to control the conformity of the processing with data protection safeguards, in particular its proportionality.

Legislation needs to be reviewed

INDIVIDUAL TRACKING/BEHAVIOUR ANALYSIS : **Better protection of individuals against automated individual decisions is required.**

NEW ACCOUNTABILITY MECHANISMS : **To compensate the loss of transparency. The "watchers" need to be watched.**

SPECIFIC REGULATION FOR MORE SENSITIVE PROCESSING : **To define, e.g.:**

- **when public authorities can access private networks**
- **when the system can be used by civil protection and police.**

Conclusion

New safeguards needed?

- Important challenges raised by the interconnection of video surveillance networks
- Existing efficiency mechanisms insufficiently used
- Data protection as dynamic process:
  - Progressive shift in the perception of the risks
  - Define intrusions that can be tolerate in a democratic constitutional state
  - Improve the regime of accountability

Thank you for listenning,

Any Questions?

fanny.coudert@law.kuleuven.be