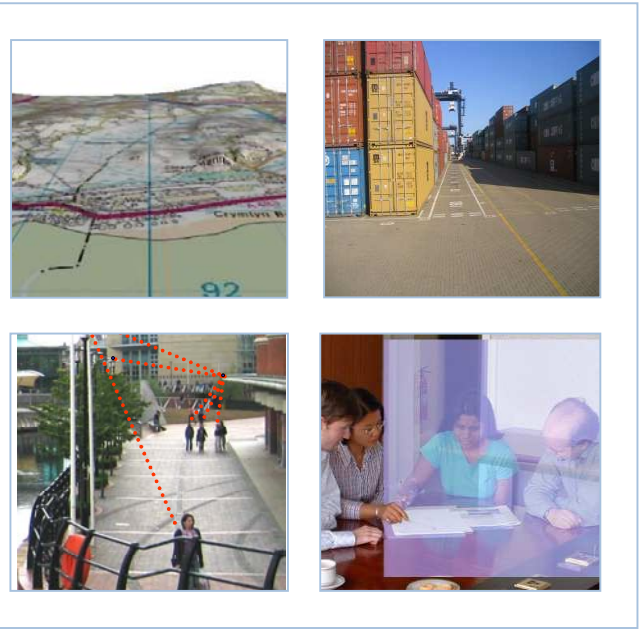
THALES



Privacy issues in security technology development

Peter Munday

Thales Research and Technology (UK)

Questions to consider

1. **What are the main issues concerning privacy and security from industry's perspective?**

2. **What is the level of awareness of privacy issues in security technology development?**

3. **Is there an added-value (comparative advantage) for security industry in privacy enhancing systems design?**

Main focus will be on Question 1, with 2 and 3 deal with at end

Main Issues for Industry concerning Privacy and Security

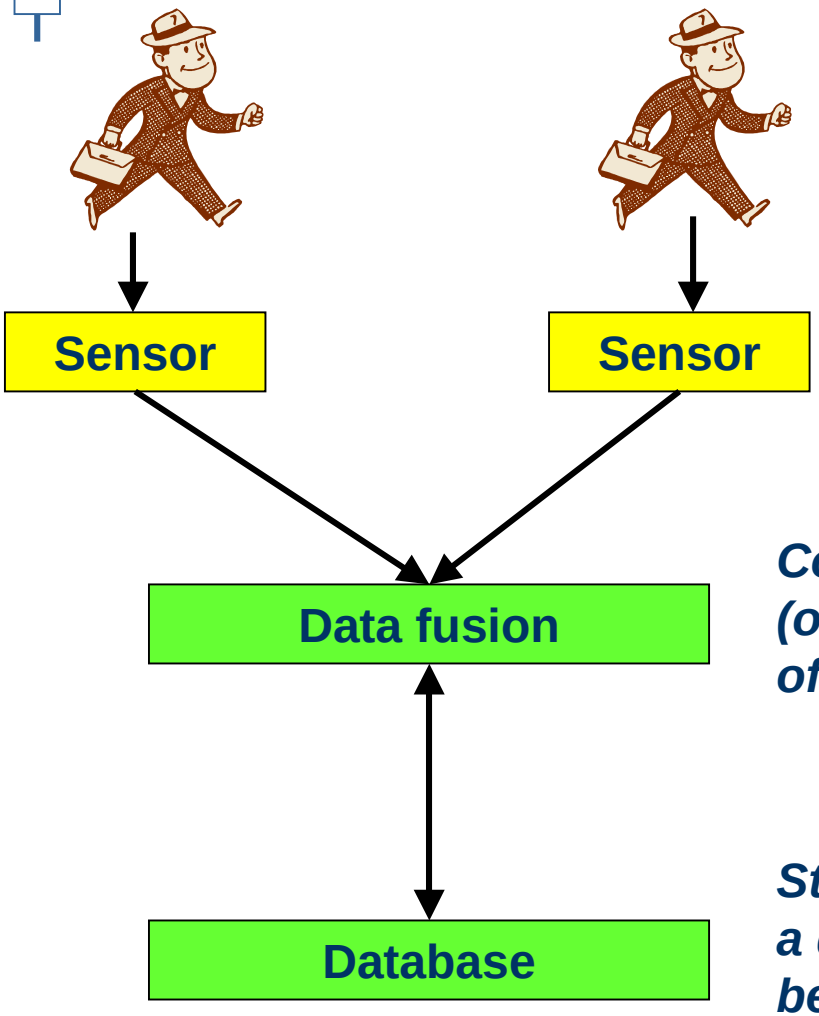
1. **Increasingly, industry has to take an overall system view of a new product or service, not just a technology view, e.g.**
   - ***What data will be used and how***
   - ***Where will data come from***
   - ***How and where will data be stored***
   - ***How do humans interface to the system***
   - ***How is access to data controlled***

   Privacy issues can significantly affect system design

2. **Improving civilian security is increasingly challenging:**
   - ***We need to find a "needle in a haystack" – the one terrorist or criminal among the millions of people on trains, aircrafts or in shopping malls***
   - ***Security must be reliable: find a bad guy without hindering the good guys***
   - ***Many technologies are nearing their theoretical limit of performance***
   - ***A major help for security is data fusion, data mining and data sharing***
   - ***We may have to act very fast (in minutes) to stop a potential attack – not the time to have to ask someone for permission to access data***

Things that may be worries from a privacy viewpoint are needed for good security

Security Benefits of Data Fusion and Databases



Sensors may give:
- ***False alarm (Says something is wrong when it is not)***
- ***Missed detection (Says something is all right when it is not)***

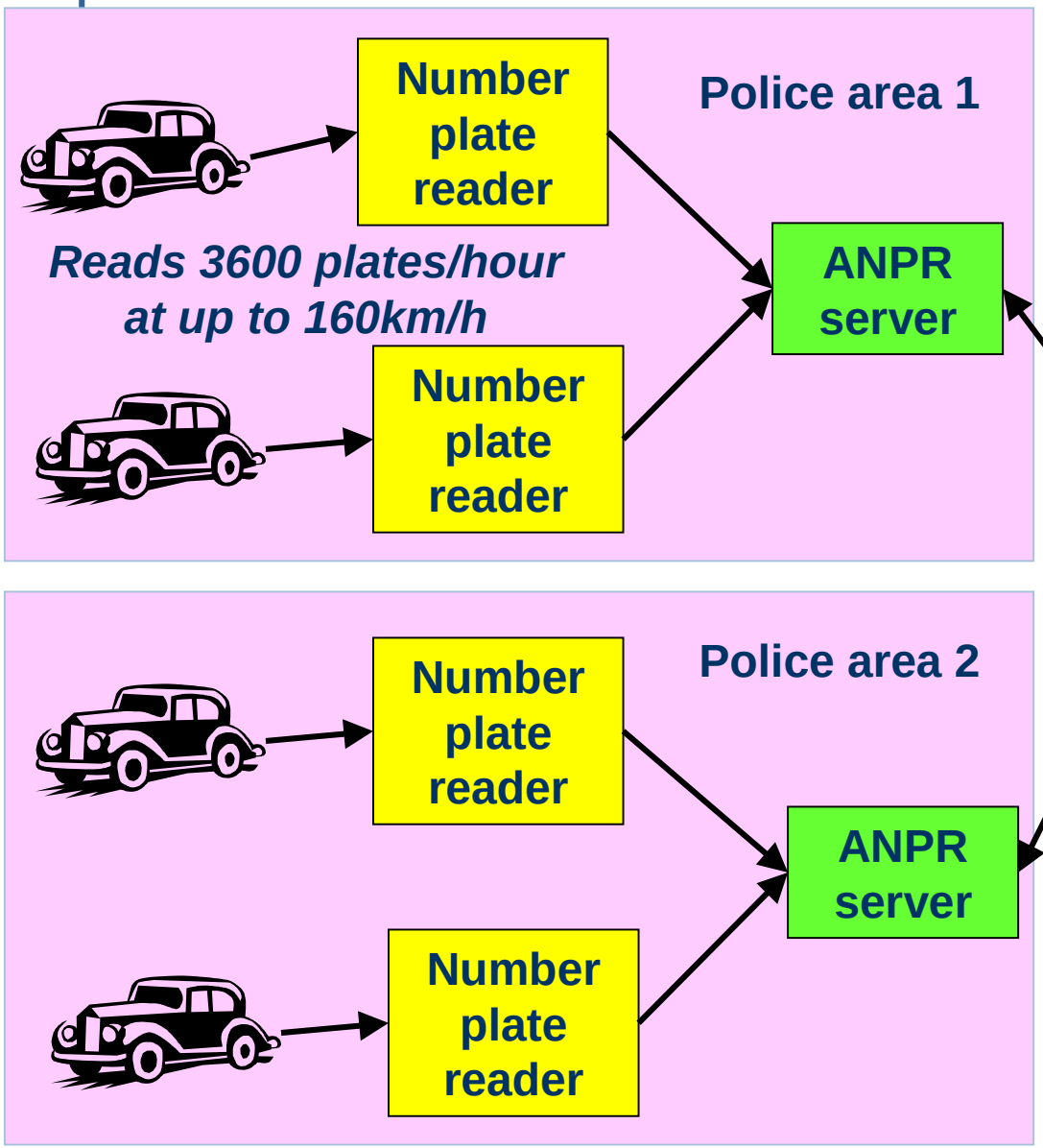
Combining (fusing) data from several sensors (of same or different type) can reduce number of false alarms or missed detections

Storing information captured by sensors in a database enables patterns of activity to be analysed and anomalies detected (e.g. "same" vehicle in 2 places at same time)

But this data sharing/storage can affect privacy, e.g. access by corrupt officials

THALES

Example 1: UK Police Automatic Number Plate Reader (ANPR) System



3000 cameras in total in 43 UK police areas

Records routes taken, closeness to crime scene unlicensed vehicles, duplicate number plates

National ANPR data centre

Police national computer

Driver & Vehicle Licensing Authority

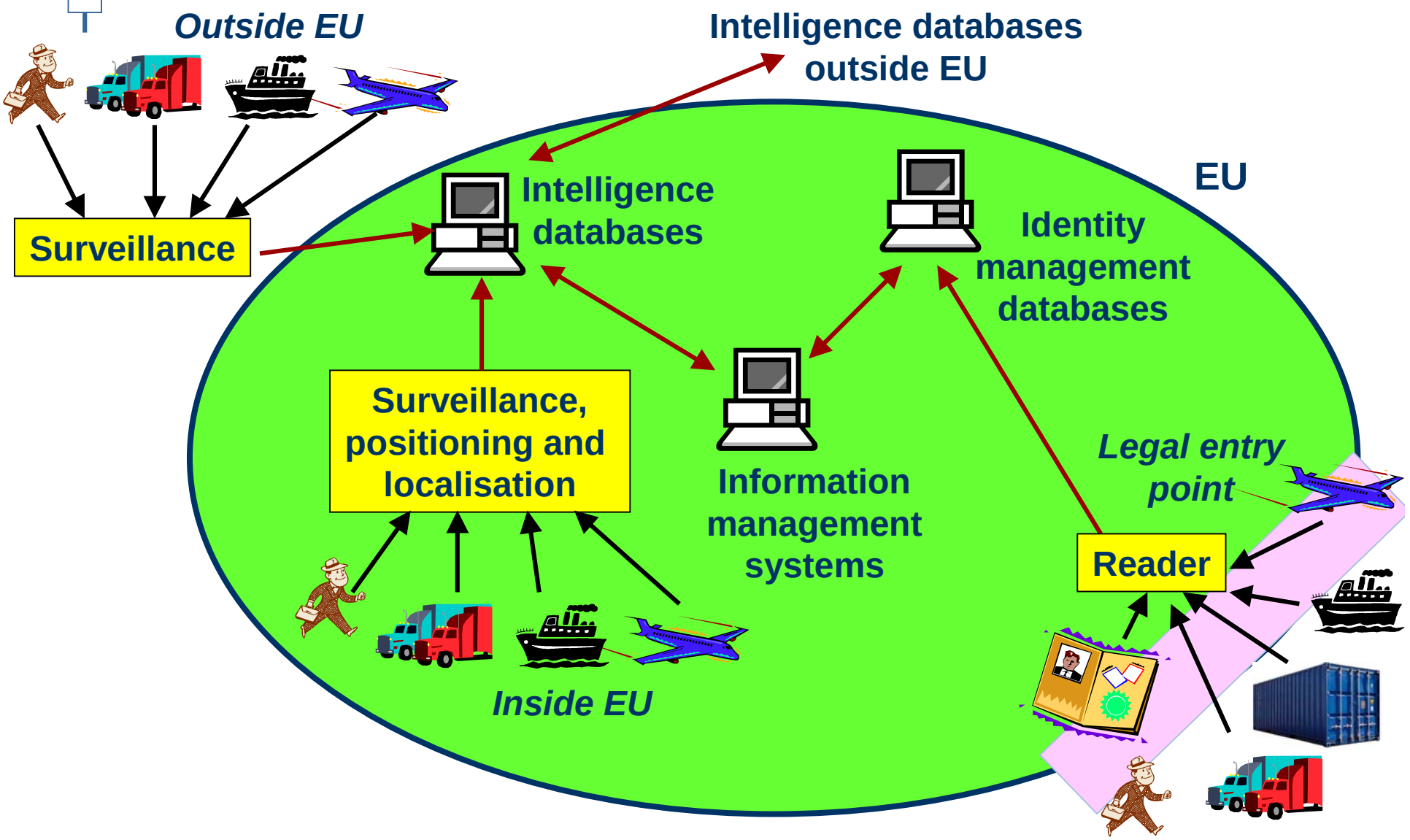
THALES

UK ANPR Data Access Rules

1. Data can be stored for up to 5 years for counter terrorism reasons
2. Data older than 2 years requires a chief officer's authority before being read
3. Data aged from 90 days to 2 years requires a superintendent's authority before being read, and must be for an investigation into a serious crime
4. Data aged up to 90 days can be read by an authorised police officer if for an investigation into a reported crime
5. Data is stored in a tamper proofed system (write once - read many) to prevent data corruption (accidental or deliberate)
6. An audit trail of all data reading is maintained
7. The UK Information Commissioner has approved the system

The privacy rules which require human permission could hinder rapid access to important information in an emergency

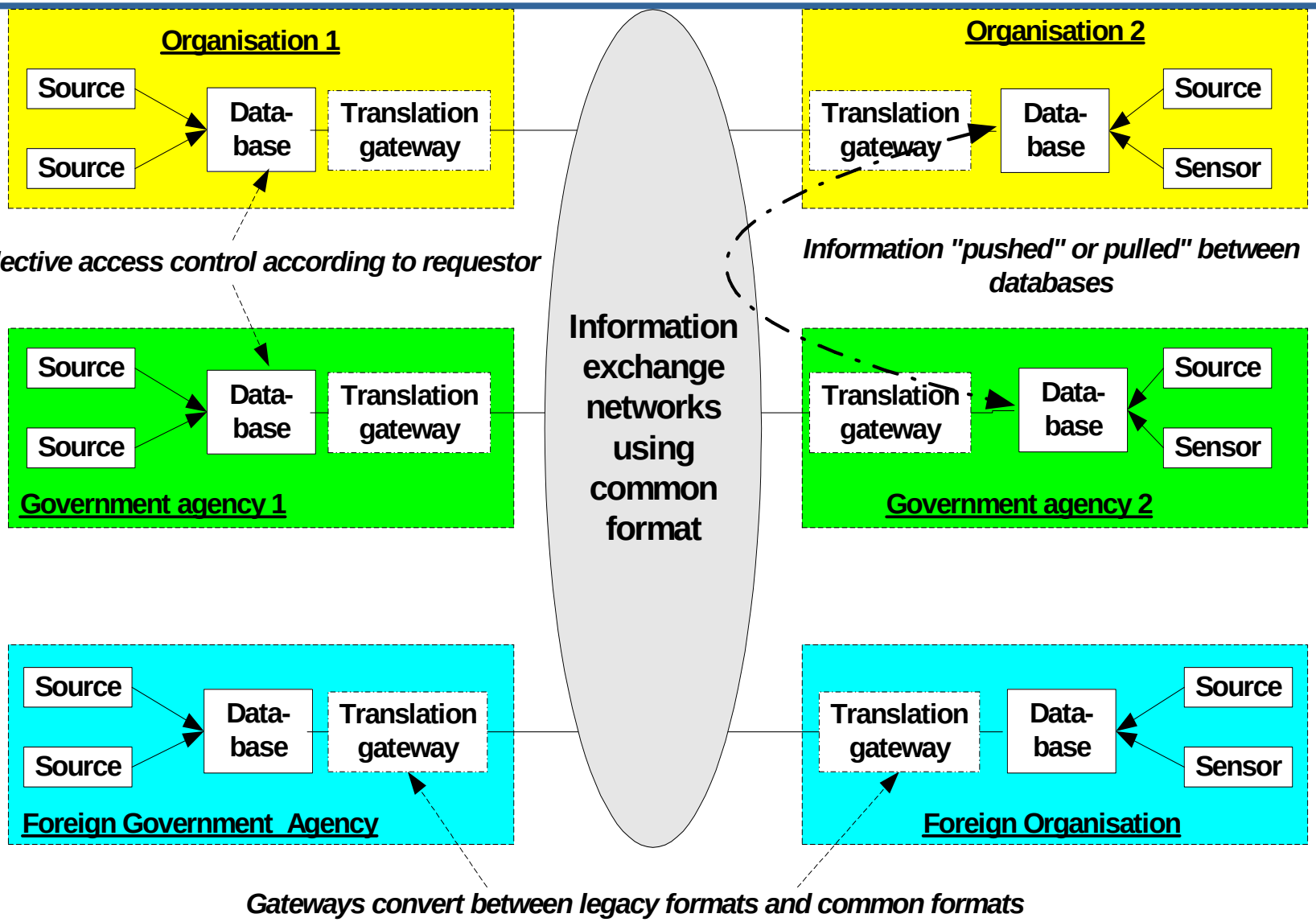
Example 2: EU Integrated Border Management Aspiration



This can be done technically. What privacy controls are needed?

THALES

Distributed Databases instead of Centralised Database



Distributed databases with *selective* sharing of information is a good way forward

THALES

Intelligence Sharing – Privacy Considerations

Rapid sharing of information is important in situations where rapid assessment and decision making is necessary, e.g.

- ***A suspected suicide bomber is walking down the street***
- ***A small boat, possibly packed with explosives, is moving rapidly towards a passenger ferry***

Obtaining information rapidly about the suspect may help make a decision whether to take preventive action, which may have to be lethal

Measures, not all technical, need to be taken to ensure that information has not been corrupted, accidentally or deliberately:

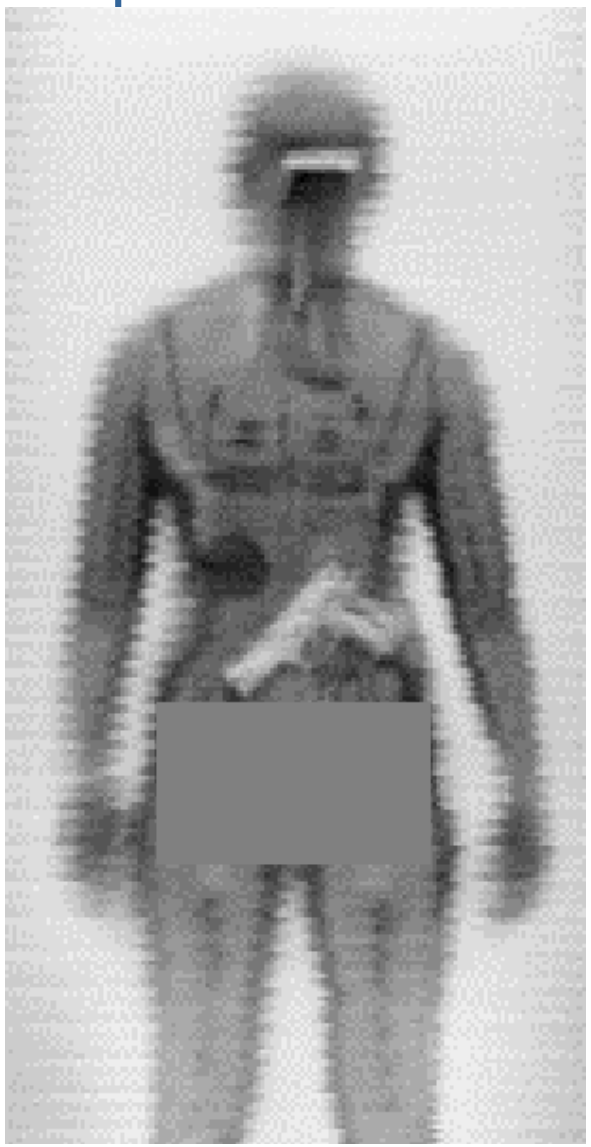
- ***Comparing information with that from other sources***
- ***Data mining to find such data***
- ***Artificial intelligence to look for potential anomalies in data***
- ***Authentication checks on data (e.g. error detection codes, digital signatures)***
- ***Authentication of source of information***

These need to be done when data is first stored, not when an emergency arises and quick decisions need to be made

Many of these measures require yet more data sharing

THALES

Privacy Issues in Person Scanning



Person scanners can detect objects hidden under clothing.

However they can potentially also reveal sensitive body parts, e.g. genitals.

Security usefulness and privacy sensitivity of images depends on technical choices

- ***X ray, mm wave or THz wave***
- ***Image resolution and quality***
- ***Contrast ratio between different parts of body (skin or hair) and non body objects***

Privacy problem can be eased, but not necessarily solved, by:

- ***Having person checking image in a different location to person being scanned***
- ***Automatic detection of dangerous items, i.e. no person is viewing image***
- ***Automatic removal of sensitive body features from image***

THALES

Summary of answers to questions

1. **What are the main issues concerning privacy and security from industry's perspective?**
   - ***We need data fusion, mining and sharing to help us against the modern terrorist or criminal***
   - ***Access to data may have to be very fast – privacy controls must not slow us down***

2. **What is the level of awareness of privacy issues in security technology development?**
   - ***Growing but could be improved***
   - ***Need for system level design is forcing an early focus on privacy issues***

3. **Is there an added-value (comparative advantage) for security industry in privacy enhancing systems design?**
   - ***Authentication and encryption are vital components of many security systems e.g. to stop the bad guy seeing sensitive data***
   - ***Other techniques like anonymity will be developed if there is a market for them***

Remember that engineers are also citizens

THALES