Privacy and Security

Overview of Security Technologies

PASR - Preparatory Action on the enhancement of the European industrial potential in the field of Security research

Grant Agreement no. 108600

Supporting activity acronym: PRISE
Activity full name: Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

ISBN 978-82-92-44712-3

Published: Oslo, August 2007
Cover: Enzo Finger Design AS
Print: ILAS Grafisk

Electronic version published on: www.teknologiradet.no

Table of contents **page**

Preface

The **PRISE**-project aims at contributing to a secure future for the European Union consistent with European citizens' civil rights - in particular privacy – and their preferences.

The project will:

- Develop criteria and guidelines for privacy compliant security research and technology development.
- Transform the results into scenarios that present applications of security technologies and measures that comply with civil rights and privacy to a varying degree.
- Test these scenarios in a set of participatory technology assessment procedures in different European states, allowing for a substantiated indication of public perception and citizens' preferences.
- Elaborate the sets of criteria and guidelines with direct involvement of providers of security technologies, private and public users and implementers, institutions and bodies shaping policies and regulation as well as organisations representing potentially and actually conflicting interests.
- Disseminate the results to actors relevant for the shaping of technologies and policies.

This document is the main deliverable of Work package 2, and provides an overview of security technologies. The technology overview will constitute the basis for the further work in the project – in particular with mapping privacy implications in Work package 3 and developing scenarios for the participatory technology assessment in Work package 4.

The PRISE project would like to thank all the experts that have contributed with their time and knowledge through the interviews (see Appendix A for list of interviewees). We would also like to thank Einar Aas (the Norwegian University of Science and Technology) and Ove Skåra (the Norwegian Data Inspectorate), who have read and supplied comments to the contents of this document throughout the work.

Executive Summary

What is security technology?
Security can be defined as the absence of danger – that is a state where the desired status quo is not threatened or disrupted in any way. In the context of the PRISE project, security is understood as the security of the society – or more precisely – of the citizens that constitute the society.

The term *security technology* can cover everything from private alarm systems and virus protection systems for PCs, to border control systems and international police co-operation. In order to focus our work, the participants of the PRISE consortium have defined a set of criteria that security technologies and means (systems, legislation etc.) should fulfil in order to be relevant to the project:

- The technologies or means are intended to, or have a significant potential to, enhance the security of the society against threats from individuals, or groups of individuals (not from states). This covers crime-fighting, anti-terror activities, border control activities etc.
- As the focus is on the security of the society, we will not cover technologies that focus on protecting specific individuals or businesses, such as home alarm systems or security systems for computers and computer networks aimed at individuals and businesses.
- We will only discuss technologies that directly or indirectly may infringe the privacy of individuals.
- The technologies and means discussed are either existing technologies, technologies that are perceived to be important in the foreseeable future or that are part of an on-going R&D project.

Technology model
Even with the criteria presented above, the field of security technologies and means is rather large. In order to structure our findings, we classified the technologies: Basic technologies are the foundation of the security Application areas. To illustrate some of the application areas we give a number of System examples. These examples are known real-world implementations of the application areas. We identified four basic technologies: Communication technology, Sensors, Data storage and Analysis and Decision support.

The idea of the technology model is to show that security applications draw on many different basic technologies and in doing so they also inherit the risks to privacy intrinsic to those technologies. For example: Because Machine Readable Travel Documents (MRTDs) are based on communication technology, sensors, data storage and biometrics, this application faces privacy challenges related to all these basic technologies.

The strength of this model lies in the ability to analyse application areas that are still at the research stage, and even future technologies that currently only exist as ideas. If these applications combine one or more of the basic technologies described, they may also inherit

the privacy properties of these technologies. This will make it possible to analyse these technologies' privacy impact, and thus relevance to the PRISE project.

Basic technologies
The basic technologies are technologies that can be found in many areas of society – not only in security applications. It is, however, important to look more closely at these technologies and their privacy implications in order to better understand the privacy implications of the application areas and system examples.

The first basic technology presented in this report is *Communication technology*. Communication is a prerequisite for almost all application areas: There is communication between sensors and readers, between local computer systems and central databases etc. The main privacy challenge is that communication containing sensitive data may be intercepted. Communication technology can also reveal the location of a person – either directly or through further analysis of the communication data. In addition, communication between applications that use radio frequency identification (RFID) may not be transparent– the person involved will not be able to check what is communicated.

A Sensor is a device that converts a property of the physical world into an electrical signal. Sensors can be found in a number of applications, ranging from CCTV (electro optical sensors), to readers for ID cards that contain integrated circuits. The main privacy challenge related to sensors is the lack of transparency. The data subject normally does not know that his or her information has been collected or processed (e. g. image captured through CCTV, conversation captured through a microphone or RFID chip read by a reader from a distance).

Biometric technology is a subset of sensors, but because it is so much used in security technologies, we give this technology a broad presentation in the report. Biometrics can be used to identify individuals by using their biological or behavioural characteristics. The most commonly used biometrics are facial characteristics and fingerprints. Biometrics affect privacy in a number of ways:

- Biometrics relate to behavioural and physiological characteristics of a person and can be used to uniquely identify that person. There is no opportunity for biometric authentication that allows pseudonymity or anonymity.
- Biometric data like fingerprints and DNA samples may be collected without the data subject's knowledge.
- Biometrics can reveal intimate information like ethnicity, mood – and in the case of DNA – hereditary factors and medical disorders.
- Biometric systems are vulnerable to spoofing. Because there is such a strong connection between the data subject and the biometric, it is very difficult for a victim to prove misuse by an impostor.

Data storage and *Analysis and Decision support* are the final basic technologies described in this report. The storing of personal data provides a number of privacy challenges. When different pieces of data about a person are linked together, more information is revealed than when the information items are only available separately. This challenge increases when several data sources are linked together and analysed (data mining, search) often without the data subject's knowledge. Databases are also vulnerable to function creep – the

use of data for a different purpose than it originally was collected for. Central databases are also exposed to breaches in security.

In this report we have chosen to include some applications that today only are used in the US, and even some that are no longer in use. The aim of this report is to give an overview of what technologies may be used for security purposes in Europe. The described technologies exist and can in theory be implemented in Europe. The fact that US policy seems to have a great impact on European security, make technologies and applications currently only used in the US relevant to the PRISE project. Also, the data of EU citizens are already collected and processed by security systems and applications in the US.

Some of the *System examples* described in this report are not security technologies as we have defined them in this chapter - such as black box insurance (see chapter 0) or systems to handle immigration, like EURODAC (see chapter 3.5). These systems are described because of the potential the described use of the technology has for surveillance and security applications.

Some of the technologies in this report are described in detail, and others are given a more brief presentation. This is because some of the technologies and their privacy implications can be understood sufficiently by a brief description. For other technologies, technical details are necessary in order to be able to analyse and evaluate privacy impacts properly (see PRISE deliverable D 3.2).

First in this report we provide an overview of legal requirements related to the issues of privacy and security. We then proceed to present the different technologies: *Communication technology, Sensor technologies, Data storage* and *Analysis and Decision support*.

Chapter 1 Legal Requirements

1.1 Introduction

This chapter aims at giving an overview of the regulations that cover the application of security technologies and the privacy and data protection law. A more detailed description of the legal requirements can be found in deliverable D 3.2.

Generally speaking the parties involved in data processing occurring when security technologies are applied can be public authorities, citizens and companies. The addressees of some regulations, such as police law, are public authorities only. Other regulations do not differentiate between addressees and are directed at public authorities as well as companies or individuals.

1.2 International sources

The EU Member States are not only bound by the supranational law of the EU but also by international law. On an international level the first steps with respect to ensuring privacy as a human right date back to 1950.

1.2.1 Regulations on Privacy and Data Protection

Privacy in most Western states is a constitutional right protected by explicit rules.

The first international regulation introducing a rule on the protection of privacy as a human right is article 12 of the Universal Declaration of Human Rights adopted in 1948 by the United Nations.[1] Almost the exact same wording is repeated in article 17 of the International Covenant on Civil and Political Rights the United Nations adopted in 1976. While this convention is a binding law, the declaration on human rights is not legally binding for national law.

The Council of Europe with its 46 member states adopted the European Convention for the protection of human rights and fundamental freedoms (ECHR) in 1950. The ECHR is a binding treaty. In article 8 of the ECHR the right to respect for private and family life is stated.[2] In 1981 the Council of Europe adopted the Convention for the protection of individuals with regard to automatic processing of personal data, called Convention 108. All EU Member States ratified this convention which lays down data protection as protection of fundamental rights and in particular the individual's right to privacy. Additionally, the Council of Europe has issued recommendations on a vast number of special areas of privacy

---

[1] Universal Declaration of Human Rights, Article 12: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.* See http://www.un.org/Overview/rights.html

[2] ECHR Article 8: *Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

law, as for example the protection of personal data in the area of telecommunication services or the communication to third parties of personal data held by public bodies.

The Organization for Economic Cooperation and Development (OECD) adopted the Guidelines on the protection of Privacy and Transborder Flows of Personal Data in 1980. The OECD Guidelines, the Treaty 108 and the Data Protection directive 95/46/EC each mark a fundamental data protection instrument.

1.2.2 Regulations on the protection and enforcement of inner security

In May 2005 seven Member States signed an international treaty, the Prüm Convention, on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration.[3] It introduces measures to improve information exchange for DNA and fingerprints. The Convention is open for all Member States of the European Union to join. The contracting Member States aim to incorporate the provisions of the Prüm Convention into the legal framework of the European Union. The Prüm Convention aims at implementing the principle of availability as set out in the Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final) on an intergovernmental level.[4]

The Council of Europe adopted a Convention on the Prevention of Terrorism in 2005. The Convention aims at the implementation of measures that may be necessary to improve and develop the co-operation among national authorities in order to prevent terrorist offences. This includes the exchange of information and improving the physical protection of persons and facilities.

1.3 EU regulations

The European Union is built on three pillars. The first, or *Community*, pillar is supranational law. The second and third pillars are intergovernmental law.

The first pillar comprises the three European Communities and embodies Community jurisdiction. Within the framework of the EC, the institutions of the Community may draw up legislation in the respective areas of responsibility that applies directly to the Member States. Art. 249 of the treaty establishing the European Community provides several tools to the Community institutions to regulate European law: regulations, directives, decisions and recommendations.

[3] As published by Statewatch at http://www.statewatch.org/news/2005/aug/Pr%FCm-Convention.pdf .
[4] See Chapter 1.3.2

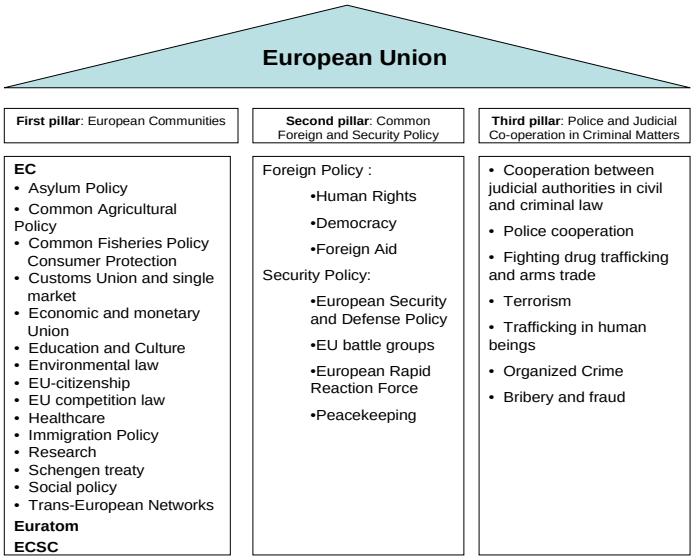

Figure 1: The three pillars of the EU

The Common Foreign and Security Policy (CFSP) makes up the second pillar and is regulated in Art. 11 - 28 of the treaty on the European Union. The Police and Judicial Co-operation in Criminal Matters (PJCC) makes up the third pillar and is regulated in Art. 29 - 42 of the treaty on the European Union. The three pillar-structure of the European Union results from the negotiations leading up to the Maastricht treaty and is reflected in the structure of the treaty on the European Union.

Within the second and third pillar the European Community has no express or implied powers and jurisdiction is mostly intergovernmental. Decisions on common foreign- and security policy are taken on the basis of cooperation between the Member States. Tools in the context of this intergovernmental practice are for example decisions of principle, joint actions, common positions or framework decisions. Framework decisions can be compared to an EU directive.

1.3.1 Regulations on Privacy and Data Protection

Starting from the regulations of Convention 108 the European Commission adopted the Directive 95/46/EC (Data Protection) after four years of discussion and obliged the Member States to bring their legislation into line with the Directive. The Directive contains fundamental rules on the lawfulness of the processing of personal data as well as on the rights of the data subject.

It lays down a number of general principles of data protection:

- *Legitimacy*: Personal data[5] must be processed[6] lawfully and the processing requires a legal basis or the consent of the data subject.

[5] See article 2 (a): *"personal data" shall mean any information relating to an identified or identifiable natural person ("data subject").*

- *Necessity*: Personal data may only be processed if
  - i) the data subject has given his consent or the processing is necessary for the performance of a contract (to which the data subject is party)
  - ii) or processing is necessary for compliance with a legal obligation to which the data controller[7] is subject
  - iii) or if the processing is necessary for the performance of a task carried out in the exercise of official authority.
- *Purpose binding*: Personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- *Transparency*: The data subject has to be aware of data processing taking place and of what data is being processed by which party.
- *Quality of the data*: The personal data collected shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data that is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
- *Security of the data*: The controller shall implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.

Since 1995 further Directives in specific areas have been adopted. The Directive 2002/58/EC on privacy and electronic communication cover issues like security and confidentiality of communications, the storage of traffic data[8] and location data.

The European Commission has drafted a proposal for a framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM 2005(475)). The proposal aims at improving the judicial co-operation, in particular regarding the prevention and combating of terrorism. The Directive 95/46/EC (Data Protection) does not apply to activities that fall outside the scope of Community law such as the judicial co-operation in criminal matters.

The treaty establishing a constitution for Europe has not entered into force as currently not all Member States have ratified the treaty. Article II-67 of the constitution lays down privacy as a fundamental right: *Everyone has the right to respect for his or her private and family life, home and communications.* The protection of personal data is regulated in article II-68:

---

[6] See article 2 (b): *"processing of personal data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*

[7] See article 2 (d): *"controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes of the processing of personal data.*

[8] The provisions on the storage of traffic data for billing purposes were replaced by the Directive 2006/24/EC (data retention), see chapter 1.3.2.

Everyone has the right to the protection of personal data concerning him or her.

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

1.3.2 Regulations on the protection and enforcement of inner security

Generally speaking, rules on law enforcement practices and obligations, and thus the application of security technologies by law enforcement authorities, are still regulated within the national law. Crime fighting methods, like video surveillance, covert surveillance of telecommunications and private premises, the use of location technologies or DNA databases are regulated in national law.

Regulations on a European – supranational – level with regards to the application of security technologies by law enforcement authorities exist only for issues that arise in areas the European Community has jurisdiction over. The Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States for instance, was to lay down rules giving effect to the Convention implementing the Schengen Agreement.[9] Also provisions on the border control and visa information systems SIS (Schengen Information System), SIS II and VIS (Visa Information System) are regulated on a European level.[10]

Furthermore, the proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final) aims at establishing rules to ensure that information needed for the fight against crime should cross the internal borders of the EU without obstacles. The principle of availability aims at ensuring that information available to certain authorities in a Member State must also be provided to the equivalent authorities in other Member States. The proposed Council Framework Decision follows the same goal as the Prüm Convention. The exchange of law enforcement information includes sensitive data like fingerprints or DNA information.

At the beginning of this year the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks was adopted. The Directive regulates the scope of the retention of traffic and location data in the Member States in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

Previous to the new directive traffic and location data had to be erased when it was no longer needed for the purpose of the transmission of a communication, respectively after the duration necessary for the provision of a value added service. A processing of traffic data was permissible only to the end of the period during which the bill could lawfully be

---

[9] Protocol 2 annexed to the Treaty on European Union integrates the Schengen acquis into the framework of the European Union.

[10] See chapter 5.3

challenged or payment pursued. The new directive extends the period of storage until *not less than six months and not more than two years from the date of the communication.*

The Member States Ireland and Slovakia have issued a legal challenge to the Directive 2006/24/EC at the European Court of Justice (ECJ) claiming the wrong legal basis was chosen for the Directive.[11]

[11] The European Court of Justice ruled in May 2006 that the Agreement between the European Community and the United States of America on the Passenger Name Records of air passengers transferred to the United States was based on a wrong legal basis and annulled the respective Decisions. The data was initially collected for a purpose that falls under Community law (the purchase of an airline ticket) while the transfer for the purpose of safeguarding public security falls within a framework on public security. The Directive 2006/24/EC changes the purpose of data storage from providing a communication service to enabling the investigation, detection and prosecution of serious crime. See also chapter 5.4

Chapter 2 Communication technologies

By communication technologies we mean mobile communications, fixed network telecommunications (PSTN), and communication over the internet protocol (IP). Because location tracking through satellite positioning and the GSM network have much in common, we have also chosen to include the description of satellite positioning in this chapter, even though it is not a communication technology.

Exchanging information using communication technologies can provide data which falls into three categories:

- *Traffic data*: who exchanged information, when, and for how long?
- *Location data*: where were the involved parties were at the time they had contact? From a legal perspective, location data needed to handle a connection, like the ID of the base station (Cell ID) is considered traffic data.
- *Content*: what information was exchanged?

Security means and technologies related to communications technologies usually involve gaining access to one or more of these types of data, either in real time or by storing the information for later use.

2.1 Personvernutfordringer i forbindelse med kommunikasjonsteknologi

Den mest åpenbare personvernutfordringen i forbindelse med kommunikasjonsteknologi er at kommunikasjon som inneholder sensitive opplysninger kan fanges opp av uvedkommende: Telefonsamtaler kan avlyttes, og tekstbasert kommunikasjon som ikke er kryptert kan leses av alle med tilgang til serveren meldingen er lagret på. Selv radiokommunikasjonen mellom RFID-brikker og deres lesere kan fanges opp av hvem som helst med riktig utstyr.

Kommunikasjonsteknologi kan også avsløre hvor en person er eller har befunnet seg. Så godt som alle bruker mobiltelefon – som kan lokaliseres gjennom basestasjonene den kommuniserer med. Mobiltelefoner er i økende grad utstyrt med GPS-moduler som gir en enda mer nøyaktig posisjon.

I tillegg er ikke kommunikasjon mellom apparater som bruker radiofrekvensidentifisering (RFID) nødvendigvis transparent – det vil som regel ikke være mulig for den berørte personen å sjekke hva som er blitt kommunisert.

2.2 Privacy challenges with communication technologies

The most obvious privacy challenge connected to communication technologies is that communication containing sensitive data may be intercepted: Telephone conversations can be eavesdropped, and textual messages that have not been encrypted can be read by anyone with access to a server the message is stored on. Even the radio communication between radio frequency identification (RFID) chips and their readers can be intercepted by anyone with the correct equipment.

Communication technology can also reveal the location of a person. Practically everyone carries a mobile telephone that can be located through the base stations it communicates with. Mobile phones increasingly come equipped with GPS-modules that give an even more accurate location.

In addition, communication between applications that use radio frequency identification (RFID) may not be transparent– the person involved will not be able to check what is communicated.

2.3 Public Switched Telephone Network (PSTN)

The PSTN is the traditional circuit-switched telephone network. In practice, this network covers both traditional fixed-line communication and mobile telephony, but as the information that is recorded for communications over mobile devices deviate from that for fixed-line telephony, mobile telephony will be described separately in the next section.

The PSTN has been in use for over 100 years, and covers large geographic areas and billions of users. Because of this, it has been important to develop standards that describe how user information should be coded, how information on multiple conversations should be handled (multiplexing) and how requests for connecting and disconnecting conversations should be coded and transmitted (signalling).

- The following information is registered for each connection:
- start time
- routing information (what number is making the call, and what number the call is to)
- stop time

The telephone number is associated with the outlet for the cables, i.e. the number is not associated with a specific person or telephone, but with the outlet the telephone is plugged into. The location can be found through the customer information (address) for the given number.

2.4 Mobile telephony

A mobile terminal, like a GSM phone (Global System for Mobile communications), establishes communication through so called base stations. These are antennas with receivers/transmitters which relay the signal between the network and mobile terminals. Traffic from a mobile phone is sent through radio waves to the nearest base station. From there the signal goes through the cable based network to either a fixed telephone or to a mobile terminal through the base station closest to the receiver's position.[12]

Unlike with the switched network, the telephone number for mobile phones is associated to the device, or more correctly to the Subscriber Identity Module (SIM card) in the device.

[12] The technical information about mobile telephony is mainly based on Riksaasen T. (1993/94) *Telematikknett*

To be able to establish a connection, the mobile network must know where each terminal is at any time. To enable this, the mobile unit sends regular reports to the network, and receives information in turn, for instance when:

- It has been switched off, and is turned on again
- When it is switched on and moved from one location area (base station) to another
- A defined time interval has passed

Location information is stored in two different registers that are maintained by the mobile operator: The *Home Location Register (HLR)* and the *Visitor Location Register (VLR)*. These registers are used to keep track of where mobile units are roaming, and are necessary in order to provide the mobile service.

The HLR contains information about:

- Code and number allocated to the subscriber
- What services are subscribed to
- Restrictions to the services (i.e just domestic calls etc.)
- Information about which VLR the mobile unit is registered in. This enables incoming calls to be routed to the mobile unit. When the unit moves, the information is updated.

The VLR contains information about:

- Subscriber identity codes
- Subscription information (like HLR)
- Location Area Identity (LAI)

This means that the position of the mobile unit is known to the system at all times as long as it is switched on, not only when it is in active use. When communication takes place, the operator stores data on which base stations were used as part of the traffic data. This is later used for billing purposes.

Important data involved in mobile communications are:

Telephone number: This is a number assigned to a SIM card by a network operator. The number can be "moved" from one phone to another by moving the SIM card, and it can also be assigned to a new SIM card should the user choose to change operator (number portability).

IMSI – International Mobile Subscriber Identity: All mobile phone subscribers are assigned a unique 15-digit IMSI number. The IMSI consists of three components:

- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Mobile Subscriber Identity Number (MSIN)

The IMSI is stored in the Subscriber Identity Module (SIM).

TMSI – Temporary Mobile Station Identity: This identifier is used instead of the IMSI in the radio interface to limit the possible tracing of a subscriber. Protection of identity is of special importance in mobile communications systems, where the subscriber and the network identify themselves to each other before the connection is made.

IMEI – International Mobile Equipment Identity: All GSM phones are assigned a unique 15 digit IMEI code. Through this code, manufacturer, model type, and what country that has approved the handset can be found. The IMEI is stored in the Equipment Identity Register (EIR).

Cell ID – The identification number of a specific base station.

SIM number: All mobile phone SIM cards have each been assigned a unique SIM card number.

GSM communication is encrypted using the stream cipher A5/1. It was originally to be kept secret, but was leaked in 1994. There is now commercially available equipment that can intercept and decrypt GSM communication (see further description in chapter 2.4.2). Some of the listening systems also have features like word identification. This means that the system, in addition to intercepting and storing the communication, can identify words and phrases from a pre-defined database.[13] In most countries it is illegal to sell such equipment to other than law enforcement agencies or other authorised government agencies. Despite this there is a tendency that such, and other types of surveillance technology, is becoming more available in the private market.[14] In fact, private subjects, like private investigators and criminals in many cases have access to surveillance equipment that the Police are barred from using for legal purposes.

2.4.1 Eavesdropping

Basic technologies: *PSTN*
Mobile communication
Internet communication
Satellite communication

There are different applications designed for monitoring citizens and interaction between citizens, either over the Internet, telephone network or in defined areas. One form of eavesdropping is often referred to as *wiretapping*. This is essentially to install a listening device in the path between two phones that are part of a conversation. Wiretapping can be set up on the subject's telephone, but also on the telephones of persons he or she is expected to contact. For the police, installing a device is often unnecessary – they can simply get access to the data required through the systems of the network operators.

[13] See for instance a presentation of *GSM Intercept A5.1 Chatter Guard* at http://www.gcomtech.com/product.aspx?ID=37&CID=6
[14] Hegghammer T (2006) *Terrorisme og ny kommunikasjonsteknologi*

For mobile networks, the police will normally have to supply the network operator with the IMSI of the telephone they want to eavesdrop. They will then be able to tap (and decrypt) the communication through equipment supplied by the network operator.[15]

An extended version of wiretapping is to more indiscriminately tap all communication lines (phone, mobile, Internet) in search of conversations that may be of interest.

System example: Echelon
The Echelon network is run by an alliance between the USA, UK, Canada, Australia and New Zealand. The system has been in operation since the Cold War. It was initially set up to monitor communication in or to the Soviet Union and Eastern Europe. The existence of the system was widely publicised as a result of a report from STOA (Scientific Technology Options Assessment).[16] As the alliance itself refused to comment, the EU Parliament appointed a committee to consider the existence of Echelon and its methods. The committee concluded[17] that the system exists, and that its purpose is to monitor private and commercial communication. Patterns of communication can be analysed, and content can be scanned for interesting keywords. Messages that are identified by the system are copied for manual evaluation.[18]

It is stated that the system can perform quasi-total surveillance, which means that all types of electronic communication – telephone conversations, SMS, fax, e-mail and Internet traffic – can be monitored. The surveillance system depends, in particular, upon worldwide interception of satellite communications. The network seems to not be as extensive at previously assumed, as only a small proportion of the communications in areas with much traffic are transmitted by satellite.

2.4.2 Technical identification of telephones and communication equipment

Basic technologies: *Mobile communications*

The identity of the mobile telephones used in suspected criminal activity is often unknown to the police, as criminals tend to change phones often, use anonymous phones (where available) or stolen phones. In order to get a court warrant to perform wiretapping, the telephone or communication equipment will have to be identified.

This identification can be achieved through equipment called an IMSI catcher. An IMSI catcher logs the IMSI numbers of all mobile phones in the area. In many cases, the phone can be identified by directing the equipment at the subject on two or more occasions, and cross reference the IMSI numbers to eliminate other phones that happen to be in the area. In other cases it is necessary to listen in on the conversations that take place in order to

[15] Source: Telenor
[16] Wright S. (1998) *An appraisal of the Technologies of Political Control* and Campbell D. (1999) *Interception Capabilities 2000*
[17] Temporary Committee on the ECHELON Interception System *(2001)Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*
[18] The Norwegian Board of Technology (2005): *Elektroniske spor og personvern*

identify the person that holds the phone. In such instances there is a risk that the conversations of innocent 3rd parties could be captured.[19]

This also means that mobile conversations within a limited geographical area can be intercepted. Such an area can for instance be a building complex. In Denmark it has been proposed that the police should be allowed to perform such scanning under special circumstances.

The IMSI number is normally protected in the telephone, but it is transmitted openly when the phone attaches itself to a new base station.[20]

An IMSI-catcher is normally part of equipment used to intercept GSM communication, and there are several commercially available products on the market. A typical IMSI catcher will have a monitoring radius of a few hundred metres, and be able to register a range of IMSI, TMSI and IMEI numbers associated with a specific base station. It will also be able to listen to one or more conversations. In such cases the equipment simulates a cell, and it is possible to eavesdrop because the connection is made by the catcher cell.

2.5 Communication over the Internet Protocol

Networks using the Transmission Control Protocol (TCP) / Internet Protocol (IP) route packets of data from one unique identifier (IP address) to another. This is a very different approach from the circuit-switched networks described above, where a line is established for each connection made, and reserved for that connection for the duration of the call.

Within a private network, IP-addresses can be assigned at random as long as each address is unique. Connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates. The *Data retention directive* (see chapter 5.2) will require Internet Service Providers (ISPs) to store information on what customer is assigned which IP-address at any time for up to two years.

Some of the most important terms associated with the use of the Internet and the Internet protocol are:[21]

IP-address: An IP-address is an identifier for a computer or device on a TCP/IP network. When a user visits a web-server, it will often store information about the user's visit on its various web pages. This information will typically be time, the user's IP-address, user-name for the Internet account and which pages were visited. If the user has a fixed IP-address and is not using address mapping in a firewall, the user's machine can be uniquely identified.

URL: Uniform Resource Locators are strings that identify resources in the web: documents, images, downloadable files, services, electronic mailboxes, and other resources. They make

[19] The Norwegian Ministry of Justice and the Police (2005) Ot.prp. nr. 60 (2004-2005): *Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)*
[20] Source: Telenor
[21] The descriptions are taken from Teknologirådet (2005) *Elektroniske spor og personvern*

resources available under a variety of naming schemes and access methods such as HTTP and FTP addressable in the same simple way.[22]

HTTP-reference: The HyperText Transfer Protocol (HTTP) is the protocol used to deliver virtually all files, search results and other data on the world wide web. It works so that when a link from one page to another is followed, the address (URL) from this page is sent with the request for the new page. The new site can then see which site the user came from, and in this way gather information about the user's activities on the net. When clicking a link after a search, the words in the search string will normally be part of the URL, and thus passed along to the new web site.

Cookies: Cookies are messages given to a Web browser by a web server. The browser stores the message in a text file on the user's computer. The message is then sent back to the server each time the browser requests a page from the server that supplied it. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. The server can use the information in the cookie to present custom Web pages.

Two different types of actors can store cookies on the user's computer. First party cookies are created by the web server visited by the user. Third party cookies, on the other hand, are created by companies advertising on the site visited. These cookies can be used for gathering information about the user's surfing habits on pages where the company advertises.

The three most important exchange methods for *content* over the IP protocol are:

E-mail: E-mails are messages transmitted over communications networks. When a message is sent, it can be stored on two or more different servers on its way from sender to recipient. Unless it's encrypted, it can be read by people who have access to these servers. Apart from the content of the message, information about sender's and recipient's IP-address and which addresses the message has passed through on the way between them can be logged.

Instant messaging: Instant messaging (IM) is a cross between a telephone conversation and an e-mail. IM systems allow you to maintain a list of people that you wish to interact with. The user can see which of these people are logged on at any given time, and can engage in a conversation (in writing) in a separate window on the screen. Instant messaging uses the IP address of the recipient to open up a connection between the two computers. Messages and connection information are maintained on servers controlled by the provider IM service.

Internet telephony (VoIP): VoIP, or Voice over IP, is a method for taking analogue audio signals and turning them into digital data that can be transmitted over the Internet. Because VoIP uses broadband networks to transmit calls, conversations that are not encrypted are vulnerable to eavesdropping.

There are three different ways to use VoIP:

---

[22] Definition from www.w3.org

- An ATA (analog telephone adaptor) allows the user to connect a standard phone to a computer or Internet connection for use with VoIP. It takes the analog signal from the traditional phone and converts it into digital data for transmission over the Internet.
- IP phones are specialized phones which look just like normal phones, but that connect into your router. They have all the hardware and software necessary handle an IP call.
- Software installed on the user's computer, together with a headset and a microphone can be used for VoIP. Skype is currently the most popular VoIP software.

In the following sections we will look at technologies used to get access to information transferred over a computer network or generated in a computer.

2.5.1 Packet sniffing

Basic technologies: *Internet communication*

A packet sniffer is a program that can see all of the information passing over the network it is connected to. A computer will normally only look at packets addressed to it. A packet sniffer, on the other hand, will look at everything that comes through. It can then either capture all the communication, or use a filter to capture only packets that contain specific data.

A packet sniffer located at one of the servers of an ISP is potentially able to monitor all online activities, such as:

- Which Web sites are visited
- What is being looked on at the site
- Whom e-mail is sent to
- The content of the sent e-mail
- What is downloaded from a site
- What streaming events are used, such as audio, video and internet telephony
- Who visits a specific website

System example: Carnivore
Carnivore is probably the most famous packet sniffing system. It was developed by the FBI to wiretap electronic communication.[23] The Carnivore system is installed at the facilities of an Internet Service Provider (ISP) and can monitor all traffic moving through that ISP. The FBI claims that Carnivore "filters" data traffic and delivers to investigators only those "packets" that they are lawfully authorized to obtain.[24] It has been reported that the system is no longer in use by the FBI, [25] as they now rely on the internet providers to supply them with the

[23] CDT (2000) *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age*
[24] EPIC (2005) Carnivore page
[25] FOX News (2005) *FBI Ditches Carnivore Surveillance System*

information they need. Critics claim that this has lead to even more intrusive surveillance methods.[26]

2.5.2 Keystroke logging

Basic technologies: *Internet communication*

Keystroke logging runs in a targeted computer in a trojan style. When installed on a target computer it will log all keystrokes, including text that is later deleted by the user. The tool can be installed on the subject's computer physically, or sent as a virus. One problem with packet sniffers (see previous section), like Carnivore, is that they cannot understand encrypted messages. The purpose of keystroke logging is to get access to passwords and encryption keys, and to be able to read the plain-text version of messages sent over the internet in encrypted form. The most commonly known keystroke logger is the FBI's Magic Lantern system.[27]

2.6 Locating systems[28]

Mobile communication can give an approximate idea of where the user is located. There are, however, more specialised technologies to establish more accurate positions. These technologies are based on calculations of the position of the user's equipment, rather then just giving information on which base station that established the connection to the user. The technologies use fixed or known positions to calculate the user's whereabouts. Such technologies may be ground based, satellite based, or a combination.

2.6.1 Locating through GSM Base stations

It is possible to calculate the position of the user's mobile equipment by using known coordinates of for instance GSM base stations.

The calculations give an approximate position that can vary from a few hundred metres in densely populated areas to several kilometres in rural areas. The accuracy can be enhanced by taking the signal delay into consideration. More accurate methods are *Enhanced time difference* (for GSM) or *Observed time difference of arrival* (For UMTS). These methods take advantage of the fact that users normally are within range of several base stations at once and use the relative delays to the different base stations to calculate the position, normally within 100-300 metres.

The same principles can be used with other types of base stations, such as WLAN or Bluetooth. These technologies have a shorter range, and the accuracy will therefore be higher.

There are both professional and more entertainment orientated services based on GSM location:

---

[26] McCullagh, D. (2007) *FBI turns to broad new wiretap method*
[27] The Norwegian Board of Technology (2005) *Elektroniske spor og personvern*,
[28] The contents of this chapter are based on Teknologirådet (2005) *Elektroniske spor og personvern*

System example: Radio cell query in Germany
Law enforcement authorities in Germany can based on a warrant obtain traffic data of all GSM subscribers who at the time a serious crime was committed where in range of the radio cell closest to the crime scene. This method of obtaining past traffic data of all individuals using a telecommunications service close to a crime scene is called radio cell query (Funkzellenabfrage).[29] It is currently not known what specific data are obtained, but it is clear that it is at least enough data to identify the subscriber.

System Example: Buddy/KidsOK
A Norwegian mobile operator offers its customers a service called "Buddy". This means that a set of friends (two or more) can make an agreement that they want to be able to request positioning information about each other. Once the agreement is made (this is done by SMS), any one of the registered "buddies" can request the position of any of the others by sending an SMS. He or she will then receive information on the general location of his/her "Buddy".[30]

A similar system in the UK (KidsOK) lets parents track their children. The position is shown on a map or sent to the parent as a text describing the child's location.[31]

The same technology can be used by police or government agencies to track a suspect after their mobile unit has been identified (see chapter 2.4.2).

2.6.2 Satellite based positioning systems

Basic technologies: *Mobile communication*
Satellite communication

The operating principle for positioning systems is simple: the satellites in the constellation are fitted with an atomic clock measuring time very accurately. The satellites emit personalised signals indicating the precise time the signal leaves the satellite. The ground receiver has in its memory the precise details of the orbits of all the satellites in the constellation. By reading the incoming signal, it can thus recognise the particular satellite, determine the time taken by the signal to arrive and calculate the distance from the satellite. Once the ground receiver receives the signals from at least four satellites simultaneously, it can calculate the exact position.[32]

GPS
GPS is short for *Global Positioning System*, a worldwide satellite navigational system formed by 24 satellites orbiting the earth and their corresponding receivers on the earth. By using three satellites, GPS can calculate the longitude and latitude of the receiver based on where the three spheres intersect. By using four satellites, GPS can also determine altitude. GPS is a US military system that has been made available to the public.

---

[29] Section 100g of the German Code of Criminal Procedure*: If certain facts substantiate the suspicion that a person was the perpetrator or inciter, or accessory, of a criminal offence of considerable importance[...] it may be ordered that those who provide telecommunication services on a commercial basis without undue delay disclose telecommunications traffic data as far as necessary for the solving of the crime.*
[30] Source: Netcom. https://netcom.no/privat/kundeservice/veiledninger/buddy.html
[31] KidsOK: http://www.kidsok.net/how.php
[32] D-G Energy and Transport: *Galileo – Satellite Navigation System,* http://ec.europa.eu/dgs/energy_transport/galileo/index_en.htm

Because telephone operators in the US have an obligation to locate where an emergency call is coming from, it is expected that more and more mobile phones will come equipped with GPS. In Japan, all mobile phones must include GPS by 2007.

Galileo
Galileo will be a global network of 30 satellites providing precise timing and location information to users on the ground and in the air. It is planned to be fully operational in 2010. It will be more accurate than the GPS system, and it will have greater penetration. Galileo is a civilian system, run by a private consortium.[33]

System example: Black box insurance – "Pay as you drive"
An insurance company in the UK has introduced an insurance product called *Pay as you drive*. In order to benefit from the product, the driver has to install a *black box* in his or her car. The black box uses GPS technology and records *how often, when* and *where* the car-owner drives.[34]

In the US, Progressive Insurance Company is using so-called "black box" technology to offer drivers discounts based on how much, how fast and when they drive. A device called the TripSensor plugs into the On-Board Diagnostic port found near the steering column of most cars made after 1996. The TripSensor records mileage, the time of engine start up and shut down, and the speed at which customers drive. The device also records information on braking and acceleration for safety purposes.[35]

System example: eCall
eCall is an initiative intended to save lives by getting rescue workers faster to the scene of an accident. From September 2009, all new cars sold in countries that have signed the *memorandum of understanding* will be equipped with eCall devices.[36] The device contains sensors that are activated after an accident. It calls the emergency number and communicates information about the accident, including the time, the precise location, the direction the vehicle was travelling in and the identification of the vehicle.[37] The same data is transmitted if the eCall is activated manually.

The device will not permanently be connected to a mobile communications network, it will only connect after it has been triggered. There is however concern about the transmitting of additional data (for instance for insurance companies), and about possible unauthorised access to databases where eCall data is stored.[38]

---

[33] Source: ESA. http://www.esa.int/esaNA/SEM5K8W797E_galileo_0.html
[34] Norwich Union: *Pay as you drive.* http://www.norwichunion.com/pay-as-you-drive/index.htm
[35] Love, D. (2004): *Progressive's Black Box: Is Big Brother Good for the Industry* http://www.insurancejournal.com/magazines/southeast/2004/12/06/features/50322.htm
[36] European Commission. Information Society and Media: *eCall.*
[37] Safety Support *eCall: Saving a life every four hours!*
[38] Article 29 Data Protection Working Party (2006) *Working document on data protection and privacy implications in eCall initiative*

Chapter 3 Biometrics

Biometrics is not a *basic technology* in the same way as communication technology, sensors, data storage or analysis and decision support. But because so many sensors used for security applications apply biometrics such as face recognition, fingerprinting or iris scanning as an essential part of their operation, we have chosen to include a chapter on biometrics before we proceed to present sensor technologies in 0.

Biometric technology identifies individuals automatically by using their biological or behavioural characteristics. Biometrics can be used to control access to physical locations or to information (computers, documents). The technology can also be used to find out if a person is already in a database, such as for visa applications.

A model to describe and evaluate different biometrics can be characterised by the following criteria.[39]

Universality	All human beings have the same physical characteristics – such as face or DNA - which can be used for identification.
Distinctiveness	For each person these characteristics are unique, and thus constitute a distinguishing feature.
Permanence	These characteristics remain largely unchanged throughout a person's life.
Collectability	A person's unique physical characteristics need to be collected relatively easy for quick identification.
Performance	The degree of accuracy of identification must be quite high.
Acceptability	Applications will not be successful if use of the biometric is not publicly accepted.
Resistance to circumvention	In order to provide added security, a system needs to be difficult to circumvent.

The most commonly used biometrics for security systems are fingerprint and facial characteristics, which we will describe in greater detail later in the chapter. We will also look at iris recognition, as this is one of the technologies recommended by ICAO (International Civil Aviation Organisation) for biometric passports.

[39] Jain, Bolle and Pankanti (1999): *Personal Identification in Networked society*

Other biometric technologies include:

- *hand geometry*: the analysis of the shape of the hand and the length of the fingers
- *retina*: the analysis of the capillary vessels located at the back of the eye
- *signature*: the analysis of the way a person signs his/her name
- *vein*: the analysis of pattern of veins in the back of the hand and the wrist
- *voice*: the analysis of the tone, pitch, cadence and frequency of a person's voice
- *gait* (the manner of walking)
- *ear structure*
- *odour*

These biometrics score differently on the criteria mentioned above and may be useful for different types of applications in different settings and for different levels of security. In some settings speed of processing is important, whereas a high degree of accuracy may be crucial in others. Fingerprints and facial characteristics are not necessarily the "best" biometrics based on a neutral evaluation, but their history with the public make them widely deployed.

DNA recognition is currently not considered a biometric, as it cannot be done by an automated process.[40] It is nevertheless a biological characteristic that can be used to identify an individual, and the speed of the process may change in the future. We will therefore discuss DNA profiling in chapter 3.6.

3.1 The process

The process associated with a biometric system can be split into different tasks: Data collection, processing, storage and matching.

3.1.1 Data collection

Biometrics are typically collected using a sensor. Common sensors known from everyday life can be cameras (optical sensors), and microphones (for voice recognition). Recently capacitive fingerprinting sensors have become integrated in high-end laptops and other electronic equipment.

The biometric image may be compressed in order to reduce the file size for transmission and storing. Encryption may also be implemented at this stage.

3.1.2 Processing

In most cases, the biometric image is turned into a *template*, which is a digital representation of the biometric. The template is created mainly using an algorithm that in most cases is proprietary. These algorithms take the raw image or input data and extract

[40] See Biometrics Catalog; www.biometricscatalog.org

whatever relevant features are required to turn this into a mathematical format, called a feature set. This process is also referred to as *extraction*. If the template is of sufficient quality it may be stored either in a database, or in a chip.[41]

3.1.3 Storage

In most biometric systems, only the template is stored, and the original image is discarded. However, in law-enforcement systems and facial recognition systems, the original image may be retained.[41] This is also the case with the ICAO biometric passport (for more details, see chapter 4.6).

These three stages (collection, processing and storage) are also referred to collectively as enrolment.

3.1.4 Matching

The process of comparing a biometric sample against a previously stored template is called matching. The matching results in a score. An accept or reject decision is then based upon whether this score exceeds a given threshold.

We can distinguish between two types of matching:

- *Identification*, which is a one-to-many process where one biometric sample is compared to all stored templates in order to establish the identity of the person who gave the sample.
- *Verification,* where the biometric sample of a given identity is compared to the stored template of the same identity, in order to verify that the person who gave the sample is who he or she claims to be (one-to-one).

There are two sources of error when it comes to biometric matching: The system may identify an individual incorrectly against the claimed identity. This is referred to as *false acceptance*. If a biometric system fails to identify an individual that is registered in the system, it is referred to as *false rejection*. The probability that a system will incorrectly identify an individual is thus referred to as the *False Acceptance Rate (FAR)* whereas the probability that the system will fail to identify an enrolee is called *False Rejection Rate (FRR).*[42]

One of the challenges with tuning a biometric system is that if you set the threshold at a level where no one is falsely identified, the rejection rate will increase, and vice versa. The given threshold should therefore be set to a level where both the FAR and the FRR are at an acceptable level for the system in question.

[41] Albrecht, A. (2003) *Privacy Best Practices in Deployment of Biometric Systems*
[42] ICAO TAGMRTD/NTWG (2004) Biometrics Deployment of Machine Readable Travel Documents

It is also a challenge, that while other authentication techniques may offer degrees of pseudonymity or anonymity (for instance by attribute authentication), this is not possible with biometric authentication.[43]

3.2 Fingerprints

Fingerprints are the most commonly used biometric, and it has been used to identify criminals since the 1880s.[44] It is easy to use, and it has the advantage that large amounts of data already exist for comparison.

Each finger has a unique fingerprint, and as most individuals have multiple fingers, there are alternatives if one finger should be damaged. This means that the criterion of *universality* is fulfilled for this biometric. There are some exceptions to this – fingerprints can be worn down by labour or filed down, but in those cases, they will normally "grow back". Some people have fingerprints that are unsuitable for biometric identification. Fingerprints are also *distinctive* and relatively *permanent*. Live-scan fingerprint sensors can capture high-quality images, and fingerprint-based biometric systems offer good *performance*. When it comes to *acceptability,* fingerprinting has normally been associated with criminals, but as more businesses start using fingerprinting[45] (for laptop computers, access to gyms etc.) the acceptance is likely to grow.

3.2.1 What is fingerprint recognition?

A fingerprint consists of the features and details of a fingertip. There are three major fingerprint features: the arch, loop and whorl. Each finger has at least one major feature. The minor features (or minutiae) consist of the position of ridge ends (ridges are the lines that flow in various patterns across fingerprints) and of ridge bifurcations (the point where ridges split in two). Fingerprint matching done on the basis of the three major features is called pattern matching while the more microscopic approach is called minutiae matching.[45]

The most common form of the fingerprint biometric system has two primary components: The sensor and the algorithm that processes the image to a template and subsequently compares a captured print with one or more stored templates.

Seven types of sensor are recognised:[46]

- Optical sensors
- Capacitive Silicon sensors. These sensors are getting increasingly cheap, something that will contribute to the deployment of this technology in the private sector
- Electric field sensors
- Thermoelectric sweep sensors
- Ultrasonic sensors

---

[43] From Extract from ESSTRT *Deliverable D1-6 "Responses to Terrorist Threats"*
[44] Cole, S. A. *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*
[45] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*
[46] Rejman-Greene, M. (2003) *BIOVISION Roadmap for issue 1.1*

- Pressure array. This type of sensor is claimed to be more resistant to spoofing by a synthetic finger
- Electro-optic plastic sensors combined with a photodiode array

For international security applications it is currently a problem that most of the fingerprint recognition systems are based on proprietary algorithms associated with the manufacturer of the sensor. This means that in order for the system to work, the sensor and algorithm used for capturing and storing the biometric template must be the same as the one used for identification or verification at a later stage. Due to the lack of interoperability and standardisation in the field, this is not always possible, in particular with law enforcement systems and border control systems where different countries and organisations are involved. As a result, the original image has to be stored in the database for these kinds of systems (see Chapter 3.7 for more details on the consequences of this).

System example: Biometric boarding (SecBoard)[47]
SecBoard is a joint project between Lufthansa Systems and Bundesdruckerei. When the passenger enrols, his or her fingerprints are recorded, digitised and stored onto a smart card. At check in, the passengers gives his or her fingerprint again, and this is compared with the fingerprint on the card. If it is the same, the passenger may board. The smart card uses the same security as the biometric passport, BAC (see Chapter 4.6.2). Lufthansa anticipates that passengers with an electronically readable identity card in the future will be able to move through airport security more quickly and easily than conventional travellers.

System example: Biometric boarding (Scandinavian airlines)[48]
Scandinavian airlines (SAS) will implement a system of biometric boarding in order to comply with requirements to ensure that the person checking luggage to a plane is the same person who is boarding the plane. This will be done by capturing the passenger's fingerprints at check-in. The print is digitised and the template is stored in a local database together with the luggage ID. Scandinavian airlines say that they store only 20 of the 180 measuring points, and that it is impossible to recreate the fingerprint based on the template.

The passenger then gives his or her fingerprint again at boarding, where it is checked with the database. The fingerprints will be deleted from the system once the plane has landed. The system is voluntary – the passenger may request manual ID check instead.

3.3 Facial characteristics

The face is an obvious choice for a biometric, as it is used by people every day in order to recognise others. *Face recognition* is the automated process of matching facial images.

When we evaluate face recognition using the criteria introduced in the introduction to **Feil! Fant ikke referansekilden.**, we see that it does well in the areas of *universality* (everybody has a face), *collectability* (2D face recognition uses a photograph, which is easy to acquire)

[47] The description is based on: Lufthansa Systems (2005) *Boarding with biometric data*
[48] The description is based on: Strande M. (2006) *Ingen finger-id på norske flyplasser* and Halvorsen, F. (2006) *SAS får benytte fingeravtrykk*

and *acceptability* (people are accustomed to the idea of using the face for identification and the technique is non-intrusive).

There are problems with *distinctiveness* and *permanence*, as facial patterns are not as unique as for instance fingerprints, and they change over time and under different conditions. Hair, glasses, hats and scarves – even a smile – may obstruct the face. The technology is also sensitive to lighting, pose and the quality of the images. Face recognition accordingly has much lower accuracy rates than other biometric technologies.

Face recognition's resistance to circumvention depends on the application (see Chapter 3.3.1 for more on spoofing). The low accuracy rate of face recognition also makes it easier for impostors to be falsely accepted than with for instance fingerprints.[49]

Sensors for capturing facial characteristics include:

- 2D camera (ordinary photo)
- 3D camera
- Infrared camera

Even though face recognition is not yet a mature technology, it is the technology chosen by ICAO as the primary biometric for the biometric passport.

3.3.1 Automatic face recognition

Automatic face recognition systems are systems where a person's image is captured automatically and compared to a database for identification or verification. As identification of a random person based on this technique would require an extremely large database and processing capacity beyond what is feasible today, such systems are normally used to verify that a person captured is not on a list of for instance known criminals or terrorists. The increase in CCTV over the last 10 years has led to more interest in the application of automatic face recognition.

Tests done by the German magazine c't show that systems may be fooled by still images or video loops.[50] Another security limitation is the high incidence of twins. In addition to the spoofing potential, several other arguments have been launched against Automatic face recognition systems.[51]

High potential for abuse
Pervasive automatic face recognition could be used to track individuals. If systems operated by different organizations can be matched to each other, it will be possible to track an individual from place to place.

Information may be combined with information from other technologies
Face recognition is the biometric technology that requires the least cooperation from the

[49] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*
[50] Thalheim et.al (2002) *Body Check*
[51] Agre, P. E. (2003) *Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places*

individual. This means that there is a bigger chance of having your biometric features captured without your knowledge with this technology. Information from face recognition systems is also easily combined with so-called location technologies.

Low accuracy rate
The technology has a low accuracy rate. Among the potential downsides are false positives, where a person might mistakenly be confused with a criminal or a terrorist. Conditions for image capture and recognition in most public places are not ideal, and this makes it more likely that errors will occur. As the database of facial images grows bigger, the chances of a false match to one of those images grows proportionally larger.

Citizens are unaware of the capabilities of surveillance systems
The public is poorly informed about the capabilities of surveillance cameras. They usually do not realize that through infrared images, or by extracting facial expressions, also elements relating to health or mood can be analysed.

No real choice for the privacy aware citizen
It is very hard to provide effective notice of the presence and capabilities of cameras in most public places, much less obtain meaningful consent. Travel through many public places, for example government offices and centralised transportation facilities, is hardly a matter of choice. Even in the private sector it can be difficult to do essential tasks like grocery shopping without being captured by a camera.

Not all countries take civil liberties seriously
If face recognition technologies are pioneered in countries where civil liberties are relatively strong, it becomes more likely that they will also be deployed in countries where civil liberties hardly exist.

3.4 Iris

The iris is the externally visible, coloured ring around the pupil. It is a physical feature of a human being that can be measured and thus used for biometric verification or identification.

3.4.1 Iris recognition

First of all, we should note that here are two separate methods that make use of the eye as a biometric. Iris recognition is the newer approach. An older and very different approach is retinal scanning. Retinal scanning is the imaging of the pattern of red blood vessels behind the eyeball. This technique requires considerably more co-operation from the user, and more sophisticated optical instrumentation. Retinal scanning is no longer actively marketed.[52]

An iris scan is a high-quality photograph of the iris taken under near-infrared (near-IR) illumination. Iris recognition systems generally use narrow-angle cameras and ask the user to position their eyes correctly in the camera's field of view. The resulting photograph is analysed using algorithms to locate the iris and extract feature information, in order to

[52] Rejman-Greene, M. (2003): *BIOVISION Roadmap* issue 1.1

create a biometric template. Current systems may operate at a range of about 10-20 cm, but systems exist that operate at a range of 5 metres.[53]

Iris recognition performs very well against the criteria introduced earlier in this chapter. All humans (including blind people) possess irises with some exceptions: A small, but obvious group, are people with aniridia, which is the absence of an iris. Further cases are blind people who may find it difficult to align their eyes with the camera; and those with nystagmus (tremor of the eyes).[54]

Iris patterns are scientifically proven to be *distinctive*, and they are *permanent* from infancy to old age with the exception of the effects of some eye diseases. Existing sensors can capture high-quality images *(collectability)* although several trials may be necessary. The iris recognition system offers excellent *performance* even in identification mode with huge databases of enrolled users.[55]

Newer iris recognition systems are difficult to *circumvent*, but the technology struggles with a low level of *acceptability* in the general public. This is partly due to a misconception on how the system works – many people assume that the iris is scanned by a laser that may damage the eye.[55]

3.5 Automatic identification systems

Basic technologies: *Various sensors*
Biometrics
Communication technologies
Data storage

Automatic identification solutions help government agencies use fingerprint analysis, facial recognition, photo imaging, and biometric information to identify, track, and monitor individuals.

System example: EURODAC
EURODAC[56] is a Community-wide (including Norway and Iceland) system for the comparison of the fingerprints of asylum applicants. The system enables member states to compare the fingerprints of asylum-seekers or someone illegally present and determine if he or she previously has claimed asylum in another country. EURODAC is the first common Automated Fingerprint Identification System (AFIS) within the European Union, and it was put in action in January 2003.

[53] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*
[54] Rejman-Greene, M. (2003): *BIOVISION Roadmap* issue 1.1
[55] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*
[56] The information on EURODAC is based on available information from the European Commission.

The system consists of a central database and a system for electronic transmission between the different members and the central unit. The data transmitted include:

- Fingerprint
- Member state of origin
- Place and date of the asylum application
- Sex
- Reference number

Data are collected for all asylum seekers over 14 years, and are kept for up to 10 years. If the person in question obtains citizenship or a residence permit in a member state, or leaves the territory, the data is deleted.

System example: Guardia Control System
This Danish system generates a three-dimensional copy of a human head. The system combines multiple biometric factors such as 3D facial geometry, skin texture analysis and temperature pattern. The information is stored in a central database. Because the system can measure the heat pattern of the face by using an infra-red camera, it can reveal potential diseases that cause fever, such as SARS and the bird flu.[57]

System example: FaceIt
FaceIt software works with security cameras at the Keflavik airport on Iceland. Keflavik was the first airport to introduce this kind of technology. The purpose is to identify subjects on wanted lists, and to prevent them from boarding a plane.

The system examines 80 facial characteristics and then compares the resulting template to a database of suspected terrorists and criminals. After six months, no wanted terrorists had been identified at Keflavik.[58]

3.6 DNA profiling

DNA or deoxyribonucleic acid, is perhaps thought of as the ultimate identifier. Each person carries a unique genetic code (except for identical twins). Unlike fingerprints, there's no way to change a person's DNA by surgery or by rubbing away the prints.[59]

Taking a DNA sample from a suspect is considered a breach of bodily integrity, and very stringent rules have been installed to protect the rights of those suspected, and to some extent those convicted of crimes. The reason for this is not that it is particularly traumatic to give a DNA sample (for instance saliva), but that the analysis and processing of a DNA sample may reveal intimate information about a person, like hereditary factors and medical disorders. If a DNA sample is stored for an indefinite period of time, future technology may make it possible to extract even more information than today.[60]

---

[57] Information from www.guardia.dk
[58] Petrie, E. (2002): *Iceland places trust in face scanning*
[59] OECD Working Party on Information Security and Privacy (2004): *Biometric-based technologies*
[60] Van der Ploeg, I. (2005): *Biometric Identification Technologies: Ethical Implications of the Informization of the Body*

There is a general trend towards using DNA profiling and identification more and more in law enforcement. Some countries already allow the collection of DNA for everybody convicted of a crime, even minor ones, while other have set the limit at felons who get a sentence above a defined level.

In Norway, for instance, it has been proposed to increase the police's access to storing DNA samples to everybody who is convicted to a prison sentence.[61]

DNA-databases are described in chapter 5.2.

3.7 Ethical implications of biometric systems

The Article 29 Data Protection Working Party specifically states that biometric data is of a special nature as it relates to the behavioural and physiological characteristics of an individual and may allow his or her unique identification.[62]

We mentioned previously that face recognition may be used to capture the emotional state of the subject. Other biometric characteristics also have "side-effects" that can be problematic from an ethical point of view.

Fingerprinting is normally considered to be a neutral characteristic that only can be used for identification and verification. This is, however, not the case. From the 1890s research has taken place to correlate fingerprint patterns with race, ethnicity and character traits, such as insanity and criminality. In fact, the classification scheme for sorting all fingerprint patterns into three groups: arches, loops, and whorls – was devised chiefly for the purpose of using fingerprint patterns as bodily markers of heredity and character. A study by Norwegian biologist Kristine Bonnevie found that Asians had a higher proportion of whorls, and fewer arches, than Europeans.[63] In addition certain papillary patterns depend on the nutrition of a person's mother in the third month of her pregnancy.[64]

Also certain chromosomal disorders – such as Down's syndrome, Turner's syndrome, and Klinefelter's syndrome - are known to be associated with characteristic fingerprint patterns in a person. It is important to state, though, that it is not possible to determine race, ethnicity or certain types of diseases directly from the fingerprint, merely to state a statistical probability. For instance, one study shows that 50% of people with a given type of fingerprint have a certain type of stomach problem.[63]

Iridology is the study of iris texture. Its followers claim that systematic changes in the iris pattern reflect the state of health of each of the organs in the body, one's mood or personality, and can even reveal one's future. Iridology is considered questionable by scientists, who often compare it to palmreading, and it is not recognised as a medical

---

[61] The Norwegian Ministry of Justice and the Police (2005) *NOU 2005:19. Lov om DNA-register til bruk i strafferettspleien*
[62] Article 29 Data Protection Working Party (2003) *Working document on biometrics*
[63] Cole, S. A.: *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*
[64] Lyon, Hardenberg (2001) *Warum Neugeborene mehr wissen als Grosse manchmahl ahnen*

practice.[65] But from the (raw) picture of the iris certain diseases such as glaucoma and iritis can be diagnosed.[66]

Spoofing is one problem with biometrics that we have mentioned previously. One way to try and avoid spoofing is by implementing so called liveness detection. By monitoring live characteristics like pulse or papillary response, the biometric devices become a source of sensitive biometrical data:[67]

- Pupillary response depends on whether one has been drinking or taking drugs, pregnancy and age
- Changes in blood flow are associated with several medical conditions, as well as with emotional response
- Nervousness can be recognised in a voice-pattern

Finally, use of biometrics could lead to people being socially excluded without a reason. As mentioned under the presentation of the different biometrics, for most of them there is a small percentage that cannot enrol to a system that uses the biometric that they have a problem with.[68]

3.8 Security of biometric systems

One of the major advantages with biometrics is that they are so strongly linked to a person. They cannot be lost or revealed by accident, like a password or a PIN code. This means that other types of personal data can better be protected by using biometrics, than by traditional methods. Biometric authentication provides better access control, and identity theft becomes a lot more challenging when personal data are linked exclusively to the right person.[69]

Ironically, this is also the greatest liability of biometric systems. Once a set of biometric data has been compromised, it is compromised forever. For authentication systems based on physical tokens such as keys and badges, a compromised token can be easily cancelled and the user can be assigned a new token. Similarly, user IDs and passwords can be changed as often as required. But the user only has a limited number of biometric features (in most cases one face, ten fingers, two eyes). If the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication.[70] In cases of identity theft, it would be very difficult for the victim to prove misuse by an impostor.

The risks to a system vary with the application. For access control, the risk is typically someone trying to gain access by passing as someone who is enrolled in the system. For other applications, like Visa and immigrations systems, the problem is different - users are

[65] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*
[66] Gasson et.al. (ed.) (2005) *D 3.2: A study on PKI and biometrics*
[67] From www.biteproject.org
[68] From Extract from ESSTRT *Deliverable D1-6 "Responses to Terrorist Threats"*
[69] Albrecht, A. (2003) *BIOVISION: Privacy Best Practices in Deployment of Biometric Systems*
[70] Ratha, Connell and Bolle (2001) *Enhancing security and privacy in biometrics-based authentication systems*

trying to pass as someone different from themselves, so as not to be recognised by the system. This is generally easier than to appear as someone else.[71]

3.8.1 Spoofing

There have been several informal tests of different fingerprint systems, showing that the systems can be spoofed using re-activation of latent prints (the print of the last person to use the device), synthetic fingers etc. A way of securing a system against circumvention can be the use of multiple fingers, cryptographic techniques or liveness detection.[72] Automatic face recognition systems have been spoofed using still images, or video loops.

3.8.2 Security of DNA profiling

DNA tests are difficult to circumvent under certain conditions (supervised sample collection with no possibility of data contamination). If sample collection is not supervised however, an impostor could submit anybody's DNA. We all leave DNA traces wherever we go (a single hair can provide a sample) and so it is impossible to keep DNA samples private.[72]

[71] Rejman-Greene, M. (2003): *BIOVISION Roadmap issue 1.1*
[72] IPTS (2005) *Biometrics at the Frontiers: Assessing the impact on Society*

Chapter 4 Sensor Technologies

A Sensor is a device that converts a property of the physical world into an electrical signal[73] Such a property can be thermal energy, electromagnetic energy, acoustic energy, pressure, magnetism, or motion.[74]

A sensor that can operate without input from an operator or another system is called *autonomous*. Such sensors are also referred to as *self organising* or *unattended*. We also distinguish between *active* and *passive* sensors, and between *mobile* and *stationary* sensors.[75]

An active sensor emits energy that is reflected when it hits an object. It then receives and analyses the reflected energy. Radar is an example of an active sensor. A passive sensor does not emit energy, but receives energy that in one way or another indicate human presence or other activity.

Basic sensor technologies include:

- Biosensors
- Chemical sensors
- Sensors for ionising radiation (i.e. radioactive radiation, X-rays)
- Electro-optical sensors (cameras)
- Acoustic sensors (microphones)
- Radars
- Terahertz technologies
- Electromagnetic sensors
- Mechanical sensors
- Heat sensors
- Radio Frequency Identification

Many security applications are based on sensors, such as scanners that look for weapons and explosives in airports, radars and different types of applications related to RFID, like biometric passports. We will describe some of the sensor types most relevant for security technologies in greater detail in this chapter.

[73] Wilson, D. H. (2005): *How to survive a robot uprising. Tips on defending yourself against the coming rebellion*
[74] See *FS 1037C. Federal Standard*, August 7th, 1996
[75] Most of the general descriptions of sensors are based on Berg et al. (2004) *Autonomous sensor systems. Communication needs for independent sensors*

4.1 Sensors used for scanning applications

4.1.1 Sensors for ionising radiation

Ionising radiation is radiation that contains enough energy to remove one or more electrons from an atom or molecule. This includes radioactive radiation, X-rays and short wave ultra violet radiation.

An application used in for instance airport security is *X-ray backscatter technologies (XBT)* that utilises active sensors with high energy X-rays to create images of objects composed of materials with varying density. This will reveal what is hidden under a person's clothing. The main security application is to identify concealed weapons or explosives, but it will effectively show what the person looks like in the nude, what they have in their pockets etc. This can reveal a lot about a person's private life, and thus be seen as a privacy violation.

4.1.2 Terahertz technologies

Frequencies from 0.1 to 10 THz are considered THz radiation.[76] THz systems can be used to monitor public facilities and high-occupancy buildings for toxic industrial chemicals, chemical agents, and trace explosives in a continuous and autonomous manner.

Because Terahertz radiation has better penetration in materials than optics, it can be used for detection and imaging of weapons concealed under clothing. The image is built from the pattern of reflection and absorption of terahertz waves. The depths of the structures can be calculated by the time delay between the wave being emitted and reflected back.

Apart from providing structural information, terahertz waves can identify materials. Different molecules absorb and reflect terahertz waves in a recognisable way, what could be described as a *terahertz fingerprint.*[77] This will make it possible for instance to distinguish Semtex from modelling clay. From a privacy perspective, the same issues as with ionising radiation apply.

System example: The "Naked Machine"
A "naked machine" utilises sensor technologies like backscatter X-rays to reveal if a person has weapons or explosives concealed on their body. There are different systems in use. Some reveal everything under the clothes – not just guns and explosives – hence the name "the naked machine". This type of airport security has been tested at Heathrow (Terminal 4) since 2004.[78] Other applications take the images of concealed objects and project them onto a sexless mannequin. Scanners used in this way could reduce the invasion of privacy, because they will also limit the number of manual physical searches needed.[79]

System example: PROBANT
PROBANT (People Real-time observation in buildings: Assessment of new technologies in support of surveillance and intervention operations) is a PASR 2005 project. It focuses on the

[76] The content of this section is mainly based on information from Argonne National Laboratory, US, Homeland Security Applications. http://www.et.anl.gov/sections/sinde/highlights/homeland_security.html
[77] Description by Dr. David Cumming, leader of the Microsystems Group, University of Glasgow in The Royal Society: *Superhuman vision – seeing with terahertz*. http://www.royalsoc.ac.uk/exhibit.asp?id=4661&tip=1
[78] Gadher, D. (2004) *Plane passengers shocked by their X-ray scans*
[79] From Extract from ESSTRT *Deliverable D1-6 "Responses to Terrorist Threats"*

development, integration and validation of technologies enabling operators to observe individuals located inside buildings and trace them in real time. In addition to locate and identify humans hidden behind walls, measurements of biometric values will help determine if they are alive, nervous, sleeping etc.[80]

4.2 Electro-optical sensors

This type of sensor is sensitive to light that ranges from Ultra Violet (UV) to Infrared (IR). Typical applications include image generation (two- and three-dimensional), measurement of radiation intensity and temperature, motion detection and long-distance identification of different materials. Electro-optical sensors include ordinary cameras and video cameras, as these in reality are sensors that operate with visual light.

Typical applications for the different types of light are:

Ultra Violet, UV (0,2-0,4 µm): Used by radiometers, which can detect flames, UV radiation from the sun and snow and ice.

Visible light (0,4-0,7 µm): Used by ordinary cameras and video cameras, and for light-enhancing.

Near infrared, NIR (0,7-1,1 µm): Used by radiometers, active and passive sensors (binoculars). NIR enhances contrasts between materials and can give two- and three-dimensional images. NIR is less sensitive to fog and smoke than visible light.

Short Wave Infrared light, SWIR (1,1-2,3 µm): Used by radiometers, in active and passive sensors, FLIR (Forward-looking infrared) and in thermal cameras. SWIR is used for imaging and tracing, and is less sensitive to fog and smoke than NIR.

Medium Wave Infrared light, MWIR (2,5-7,0 µm) and *Long Wave Infrared light, LWIR (7-15 µm):* Used in passive sensors, FLIR and thermal cameras. MWIR enhances contrasts between materials and objects that emit different thermal radiation and is used for imaging and tracing.

Even small thermal cameras can be used to trace people from long distances, ranging from several hundred metres up to several kilometres. FLIR technology can be used for camera surveillance under extremely poor light conditions. Passive infrared motion detectors can be used for covert surveillance.

Most of the electro-optical sensor technologies today operate on specific platforms with little means of communication between them. It is foreseen that future systems will operate platform independent, with a common interface to a communications network and decision system.[81]

---

[80] From the PROBANT project description: http://ec.europa.eu/enterprise/security/doc/project_flyers/766-06_probant.pdf

[81] Berg et al. (2004) *Autonomous sensor systems. Communication needs for independent sensors*

4.2.1 Closed Circuit Television (CCTV)

Basic technologies: *Electro-optical sensors*
Databases
Facial Recognition
Pattern recognition

Closed circuit television is in reality an application of electro-optical sensors (cameras). The idea of using television to assist the police dates far back: In 1947 it was suggested that the police should be allowed "to evaluate" the BBCs coverage of the royal wedding in London in order to assist in the deployment of patrol officers. In 1960 the Metropolitan police in London put up two cameras in Trafalgar Square to monitor the crowds during a State Visit to Parliament. As the video recorder became commercially available during the 60s, there was a growth of CCTV in the retail sector.[82]

This type of surveillance of public areas is widespread across Europe, but the extent of the use in open streets vary greatly – from over 500 systems in London, to zero in Copenhagen.[83] As CCTV-systems become more sophisticated, covert use is becoming easier.[84]

Different types of CCTV schemes
Camera surveillance should be divided into two categories: Active cameras and passive cameras. Only a few of the cameras that we see every day are active.[85]

With *active cameras* an operator watches the monitor and can control the camera (turn, zoom) to follow an individual or a situation that develops. With good quality cameras, you can get much closer to a situation than you could if you were actually present on the street. Active cameras can be used with automated visual surveillance programs that use algorithms to detect suspicious motion or identify people by comparing their image to a reference database (see chapter 0).

Passive cameras record what happens in a specific spot (for instance in a kiosk) on a tape. The tape is viewed only if there is an incident, like a robbery, fight etc. In many cases, the film has been used so many times (the tape has to be erased after 7 days in Norway, and is then normally taped over) that it is almost impossible for the police to use it if an incident needs to be investigated. In many cases, passive cameras do not work, or they are dummies intended just to scare unwanted activity away. Some places will even signpost that the area is surveilled by cameras, but not bother to invest in the actual equipment. In systems that have both active and passive cameras, only the active cameras are used in practice.

We should also distinguish between *private* and *public* camera surveillance: The Public surveillance is the one done by the police in open street systems. Private surveillance in

---

[82] Norris, McCahill, Woods (2004) Editorial. *The Growth of CCTV: A global perspective in the international diffusion of video surveillance in publicly accessible space*
[83] Hempel and Töpfer (2004) *CCTV in Europe*
[84] European Parliamentary Technology Assessment Network (2006) *ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries*
[85] From interview with Heidi Mork Lomell, May 18 2006

public places like shopping malls, banks and railway stations is normally done by private security companies.

Different uses of CCTV
CCTV schemes can be used for different reasons:[86]

- *Monitoring public areas*
  This is mostly done by using active cameras with a high resolution
- *Recording events*
  The events are recorded to be used for evidence and to inform investigations
- *Directed surveillance*
  The monitoring of areas where a suspect is expected to be
- *Deterrence*
  To prevent the criminal activity, or to move it somewhere else. Dummy cameras and signs with no surveillance system, as described above, are also part of such a strategy

There are some challenges with using recorded CCTV images as evidence.[86] The fist challenge is for the police to locate the image. Where CCTV systems are extensive, the police may have to look through thousands of hours of videotapes to locate the relevant images. A second problem is that images often are of poor quality. Even with images of good quality, it can be difficult to use CCTV images for identification by witnesses. Research shows that recognising CCTV images of unfamiliar people are very difficult.[87] In contrast, people are very accurate when identifying familiar faces, even from poor quality footage.

While the earlier CCTV systems were analogue, digital systems are becoming increasingly widespread. Digital image searching can save time in the locating of specific events or tracking crime suspects against an existing database. In 1998 the Science and Technology Committee of the House of Lords in the UK noted the potential ease with which digital images could be copied or manipulated, even on a home computer system.[88] Although authenticity can be established using audit trails or watermarks, the potential for image manipulation is still a concern.

Intelligent Video Management/Automatic monitoring

Basic technologies: *Electro-optical sensors*
Databases
Facial Recognition
Pattern recognition

Intelligent Video Management Systems are systems that can be programmed to record and mark footage of defined events (i.e. alarms going off, motion in a defined area etc.), persons (based on facial recognition), vehicles or other objects (defined for instance by size).

[86] Parliamentary Office of Science and Technology (2002) *Postnote number 175: CCTV*
[87] Henderson, Bruce and Burton (2001) *Matching faces of Robbers captured on Video*
[88] The House of Lords (1998) *Fifth report of the House of Lords Science and Technology Select Committee*

Automatic monitoring is closely related to intelligent video management. The idea is to couple CCTV systems with databases containing similar information as that described above. This can be used to track people's movements, and as such involves a threat to individual's privacy. Examples of systems are:[89]

Automatic face recognition (AFR)
There are automatic systems available that can correlate CCTV images with digital databases of photographs (see chapter 3.3.1). Automatic face recognition can be used to trigger alarms when individuals on a watch list enter an area covered by CCTV cameras.

A possible future scenario is the use of AFR systems to recognise a person, and then use the identity to get access to – and collocate – further information in other public databases. This is not feasible today, but the police in Oslo use a "light" version of such a system, where computer systems are used actively in combination with the cameras.[90] If they for example see a car that has been parked in a suspicious way, they check AUTOSYS (the car register) to find out who the owner is. They can then check the police database to see if the owner has a criminal record. If he doesn't, they can check his family ties in the central register of the population and find if he has a son/cousin/sister etc. with a criminal record. Based on this, they can evaluate the situation and how to respond. This is not as efficient as an automated process may be in the future, but it still means that it is possible to get a very comprehensive picture of a person through the technologies available today.

Automatic Number Plate Recognition (ANPR)
ANPR systems read number plates picked up by CCTV and match them against a database. This has been done in the UK, and a pilot in Northampton led to 364 arrests and the recovery of 31 stolen vehicles and property worth £150,000 in its first 7 months. Systems can have difficulty recognising number plates that do not conform to pre-determined specifications (e.g. lettering size or font) – so foreign and forged number plates may be missed or misread by the system.[89] Systems for number plate recognition are also in use in several other countries, often related to toll booth passing or speed cameras.

Tracking and identifying suspicious behaviour
Systems can track individuals and objects (e.g. cars) from camera to camera and alert operators to events such as overcrowding and vandalism. Automated recognition technologies could track "suspicious behaviour" or spot suspicious packages.[91] People that are about to jump in front of trains have a specific pattern of movements that can be programmed into a system. The same goes for people that are about to break into a car at a parking lot – they have a pattern that is very different from people who have legitimate business at the same place. On the other hand, pick-pockets are virtually impossible to spot and program patterns for. The same goes, surprisingly, for robberies, whereas fights are easy to spot. The ADVISOR project has worked on using computer algorithms to detect unusual

[89] Parliamentary Office of Science and Technology (2003): *Postnote 175: CCTV*
[90] From interview with Heidi Mork Lomell, May 18 2006
[91] Tendler, S. (2005) *"Smart" CCTV could fight terrorist threat in stations*

human behaviour, like vandalism and fighting. The project showed a very high recognition rate (89%) for the defined behaviour patterns, and a very low rate of false alarms (6,5%).[92]

The PASR 2005 project ISCAPS (Integrated Surveillance of Crowded Areas for Public Security) is currently researching automated surveillance of crowded areas by analysing patterns of suspicious behaviour.

4.3 Acoustic sensors

Acoustic sensors normally register sound through one or more microphones. The sound is then digitised and processed, before it is sent to a central unit for analysis. The central unit can take external factors like noise from traffic, weather etc. into account when producing the result. Acoustic sensors are normally passive, and small in size, and are therefore difficult to identify.

Acoustic sensors can be used for a number of tasks, including the measuring of distance (sonar) and detection of chemicals, but the most interesting capability for surveillance purposes is probably *bugging,* where different types of microphones are used.

4.3.1 Bugging

Basic technologies: *Acoustic sensors*
Electro-optical sensors

The term bugging is used for covert listening to conversations by using technical devices. Normally, microphones with transmitters or recording equipment will be placed in a room where the suspect is expected to stay, and the monitored conversation will be transmitted to a listening post near by. The bugging may also be conducted through directional microphones or other equipment that can be used at a distance (for smaller microphones approx. 100 metres, and for parabolic microphones up to 300 metres). A more extensive version of "bugging" is the placement of secret cameras in rooms or areas where a suspect is expected to stay.

Eavesdropping, or bugging, operations generally have three principal elements:[93]

- *Pickup Device:* A microphone, video camera or other device picks up sound or video images. It is possible to process the recording, for instance to filter out background noise.
- *Transmission Link:* The sound and/or video must somehow be transmitted to a listening post. This may be done by a radio frequency transmission or by wire. The transmitter may operate continuously or, in more sophisticated operations, be remotely activated.
- *Listening Post:* This is a secure area where the signals can be monitored, recorded, or retransmitted to another area for processing. The listening post may be as close as the next room or as far as several blocks.

---

[92] Naylor and Attwood (2003): *Annotated Digital Video for Intelligent Surveillance and Optimised Retrieval*
[93] Texas A&M Research Foundation *Employee's guide to security responsibilities. Bugs and Other Eavesdropping Devices*

Bugging can only be done legally by the police after a court warrant. Because of the explosion in miniaturized technology, tools for bugging have never been cheaper or easier to acquire. Both miniaturized eavesdropping equipment and directional microphones are commercially available from a range of so called "spy shops".[94]

Even in legal operations, initiated by the police, there is always a risk that the conversations of innocent 3rd parties may be recorded as part of the bugging. Both Norway and Denmark have recently passed laws that will make it easier for the police to use bugging and other means of covert investigation.[95]

System example: Sound Recognition Systems
In Chigaco city officials are using new technology that can recognise a gunshot, turn a surveillance camera toward the shooter and call the emergency number. 30 such devices have been installed in neighbourhoods with high crime rates. It is also planned to test out the system in a number of other US cities.[96]

Such systems may also be programmed to recognise other noises than gunshots. The system *sigard* is a sound detection system programmed to detect verbal aggression.[97] It is currently in use in 300 places in Holland (Amsterdam and Groeningen, among others), and is being considered by British authorities before the Olympics in 2012.[98] The microphones can detect sound over 300 metres away and record aggressive conversations before they become violent.

4.4 Unmanned Arial Vehicles (UAVs)

Basic technologies: *Electro-optical sensors*
Radars
Various other sensors
Communication technologies

UAV is defined as a powered aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry lethal or non-lethal payloads.[99]

In general, UAVs can be equipped with surveillance cameras with thermal and night-vision capabilities. Electro-Optical (EO) sensors (cameras) can identify an object the size of a milk carton from an altitude of 60,000 feet. UAVs can be equipped with radar systems to produce high-resolution imagery that can be transmitted to a ground operator. To some extent,

[94] See for instance http://www.endoacustica.com/ or http://www.thespystore.com/microphones.htm
[95] The Norwegian Ministry of Justice and the Police (2005) *Ot.prp. nr. 60 (2004-2005) Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet* (for Norway) and Ministry of Foreign Affairs of Denmark (2004) *The En verden i forandring - nye trusler, nye svar. Redegørelse fra regeringen om indsatsen mod terrorisme* (for Denmark)
[96] Reichgott, M. (2005) *Chicago Pairing Survaillance Cameras with Gunshot Recognition Systems*
[97] See http://www.soundintel.com/products.html
[98] The Sunday Times (2006): *Word on the street ... They're listening*
[99] Definition from the US Department of Defence Dictionary of Military and Associated Terms, Joint Publication 1-02

moving targets can be tracked.[100] Various UAVs can fly for 20-50 hours without re-fuelling. The planes also can be equipped with targeted weapons systems.[101]

Mini UAVs (MAVs) are UAVs that can be carried by a police officer or soldier to be used in areas where it's difficult to get an overview from great height. The MAV is designed to operate on the ground or in heights up to approximately 150 meters. They have an endurance of about an hour, and operate up to 10 km from their launch point. Hand-launched UAVs have been compared to a pair of long-distance binoculars that can see behind hills.[102] On the ground the MAV can act as a sensor and collect data the same way as in the air.

It has been suggested that such vehicles in the future may be used for civilian surveillance purposes.[103]

4.5 Radio Frequency Identification (RFID)

Basic technologies: *RFID*
Various sensors
Storage technology
Decision support
Communication technologies

RFID is a concept for automatic identification using radio waves. Tiny integrated circuits (tags) containing information are attached to documents or integrated in products or wrapping. A reader can be used to read the information on the RFID tags within range. A complete RFID application will normally involve tags, readers, a database system, and sometimes a form of decision support system.

Each RFID system is defined by the following three features:[104]

- *Electronic Identification*:
  The system makes possible an unambiguous labelling of objects or persons by means of electronically stored data.
- *Contactless data transmission:*
  Data identifying the object can be read wirelessly through a radio frequency channel.
- *Transmit when requested (on call):*
  A labelled object only transmits data when a matching reader initiates this process.

4.5.1 Elements of an RFID System

Three basic components comprise an RFID system: the RFID transponder (also called tag or chip), the RFID reader, and a computer network (if any) that is used to connect the readers.[105]

---

[100] Bolkcom, C. (2005) Homeland Security: *Unmanned Aerial Vehicles and Border Surveillance*
[101] EPIC (2005) *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking*
[102] Sweetman, B. (2005) *Mini UAVs – the next small thing?*
[103] Surveillance Studies Network (2006) *A Report on the Surveillance Society*
[104] German Federal Office for Information Security (2005) *Security Aspects and Prospective Applications of RFID Systems*

The collection of data is done by sensors. The data stored on the tag is transmitted to the reader and possibly to a connected reference database through radio communication technology. Storage of data is realized on the tag and possibly at the connected backend system. The data transmitted to and stored at the backend system can be further analysed or used for profiling purposes and decision making.

The tag

The *tag* as the basic building block of RFID consists of an antenna and a small silicon chip containing a radio receiver, a radio modulator for sending a response back to the reader, control logic, some amount of memory and it may contain a power system. The tag is located on the object or person to be identified.

RFID tags come as both *active* and *passive* chips. Active tags contain a battery and will therefore be bigger than passive tags, but they can contain more information and work over longer distances. A typical example of active tags is tokens to allow toll-booths to recognise and bill passing cars.

Passive tags do not contain a battery, but get the needed energy from the radio signal from the reader. Typical security applications that utilise passive tags are Machine readable travel documents (biometric passports) and ID cards, but the most common use for this technology is in the retail industry, where RFID is used in the supply chain. In the latter case, the tags normally only contain an identifier, and the actual information is retrieved from a database. Passive tags can be very small, and a major concern is that users may not know that they are carrying a tag or know when it is being read.[106]

Tags exist in many different shapes and sizes. The Hitachi mu-chip[107] is less than 0.44mm on a side and was designed for tracking documents printed in an office environment. Hitachi has also presented an even smaller chip – which is only 0,05mm on each side and looks like spots of powder to the naked eye.[108] Also the VeriChip,[109] an implantable tag, has the size of a grain of rice and – being a passive tag – a very limited reading range.

As for transmission, we can distinguish between *promiscuous* and *secure* tags. While most tags are promiscuous and will communicate with any reader, secure tags require the reader to provide a password or a different kind of authentication credential before the tag transmits to the reader. Most tags, both active and passive, communicate only when they are interrogated by a reader.

Tags can be equipped with different types of memory:

- *Read-write*
  More complex RFID chips can contain a read-write memory. This means that the content of the chip may be changed by the reader. Such chips will normally have some form of basic security mechanism to avoid unauthorised changing of the data.

---

[105]See the detailed technical description in Finkenzeller (2003) *RFID-Handbook*, Second Edition, Chapter 3
[106]Article 29 Data Protection Working Party (2005) *Working document on data protection issues related to RFID technology*
[107]RFID Journal (2003) *Hitachi Unveils Smallest RFID Chip*
[108]BBC News (2007) *World's tiniest RFID tag unveiled*
[109]See the VeriMed Patient Identification website: http://verimedinfo.com/patient_demo/

- *Read only*
  Read-only tags can only be read by the reader but not be reprogrammed. Such tags will often only contain a serial number, and the actual data associated with the tagged item is stored in a database connected to the RFID system.

Some RFID chips have sensors allowing environmental monitoring such as temperature, air pressure, humidity, motion, biochemical agents, or acceleration. It is possible to store the results of the sensor in a read-write memory that can be read later, but the tag can also report the results to the RFID reader either at pre-defined times or when a pre-defined result appears.[110]

Finally, the tag can be equipped with a self-disabling or "kill"-feature which will render the tag inactive with or without the possibility of reactivating it.

The reader
The RFID *reader* (transceiver/transmitter/receiver) consists of a radio frequency module, a control unit, and a coupling element for interrogating electronic tags using radio frequency communication.[111] The reader sends a pulse of radio energy and then listens for the chip's response. The energy is detected by the tag which then sends back a response that contains the tag's unique identifier (serial number) and possibly other information. The pulse of radio energy in simple RFID systems functions as an on-off switch while in sophisticated RFID systems it can contain commands to the tag, passwords or instructions to read or write memory stored on the tag.

An RFID reader is usually on, continuously transmitting radio energy and awaiting tags that enter its range of operation. It is possible though, to configure an RFID reader so that it sends a radio pulse only when an external event occurs.

Just like the tags, readers' sizes vary. The size may vary from the size of a desktop personal computer with multiple antennas to readers of the size of a postage stamp, embedded in mobile phones.

The Backend system
In many RFID systems the data received by the reader is communicated via an interface on the reader to a data processing subsystem, (or backend system). Depending on the RFID System, this might simply be a computer that match the transmitted serial number to a reference database, or it could be more complex and consist of several computers and servers.

4.5.2 Classification of RFID Systems

A classification of RFID Systems can be made according to their respective performance features.[112] It is common to distinguish between low-end systems, medium-performance systems and high-end systems.

---

[110]Heinrich, C. (2005) *RFID and beyond. Growing your business through real world awareness*
[111]Sarma, Weis and Engels (2003) *RFID Systems and Security and Privacy Implications*
[112]German Federal Office for Information Security (2005) *Security Aspects and Prospective Applications of RFID Systems*

- *Low end systems*
  Low-end systems contain either a so-called 1-bit system or a read only memory. 1-bit systems indicate to a reader whether a tag is present or not in its range. Usually no encryption function is supported and any compatible reader can read the data stored on the tags.
- *Medium performance systems*
  Medium-performance systems have rewritable data-memories from a few to about 100 Kbytes. The systems usually contain anti-collision techniques in order to make it possible to address more than one tag in range of the reader. Medium-performance systems may contain authentication or crypto-functions protecting them from eavesdropping.
- *High end systems*
  High-end systems usually are contactless smart-cards, equipped with a microprocessor and a smart card operating system. They usually contain more complex algorithms for authentication and encryption and are used in use cases with high security requirements.

4.5.3 Challenges with RFID

The RFID chip will often contain only a unique serial number to allow unambiguous identification of the chip and thus the labelled object. From the identification of an object a person carrying the object may be identifiable.[113] Furthermore, RFID tags can also be placed directly on or in the data subject, for example by implantation, and thereby allow direct identification of individuals.

Depending on the RFID technology in question, information may be stored on the tags. If the information is not encrypted or secured in other ways, it can be read by anyone equipped with an RFID scanner/reader.[114] In Norway, it was recently uncovered that on the tags used for toll-booth passing, the last 100 passings are stored on the tag. This information, revealing the movement pattern of the car, can be read by using a standard reader.[115]

A number of possible attacks on RFID Systems exist with relevance for the integrity of the data transmitted or stored, and thus the quality of the data. The security of an RFID system can be broken for example by malicious code (malware) planted in the backend system and thereby gaining unauthorized access to the stored data, or by cloning of the data contained on the tag and simulating the original identity of the tag. In experiments, researchers have also successfully infected backend RFID middleware systems through the RFID tag.[116]

Attacks to RFID systems usually follow one of the four aims:[117]

---

[113] See Directive 95/46/EC, recital 26 on the term "identifiable": *"Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."*

[114] From Extract from ESSTRT *Deliverable D1-6 "Responses to Terrorist Threats"*

[115] The Norwegian Data Inspectorate (2007) *Statens Vegvesen holdt tilbake viktig AutoPASS-informasjon*

[116] Rieback et al *Is Your Cat Infected with a Computer Virus?*

[117] See German Federal Office for Information Security (2005) *Security Aspects and Prospective Applications of RFID Systems*

- *Spying*: The attacker gains unauthorized access to information for example by eavesdropping or unauthorized access to backend systems.
- *Deception*: The attacker deceives the operator or user of an RFID system by feeding in wrong information into the system.
- *Blocking, for example by applying Denial of Service (DoS)*: The availability of functions of the RFID system is compromised either on the level of a reader or the backend system.
- *Shielding or killing of tags for example by applying a Faraday-cage or destroying RFID tags*: A single tag is not readable through application of for example physical measures.

System example: OpTag[118]

The OpTag system will attach RFID tags to airline passengers in order to be able to locate passengers before boarding. The system is intended to increase security and safety, but also to speed up boarding times.

Each tag will send out a pulse twice per second, and the pulse will be received by at least two readers. The system uses the fact that multiple antennae are receiving the signal from one tag, and the angle of the signal to calculate the position of the tag. It should be possible to track passengers with an accuracy of 1 meter and update the information every second. Personal information in an airline's system, such as passenger name, age, sex and flight number can be linked to a tag's unique ID-number.

The data from the RFID system will be integrated with images from a panoramic camera system, so that the location of a tag is shown on the image. At boarding time, the system can generate a list of passengers far from the gate, and airlines could then send employees equipped with position and images to find the late passengers.

In the future, optag may also be used in combination with face recognition software, for security purposes.

The system is developed by a consortium of European companies, and receives funding from the EU.

System example: SECCONDD (Secure Container Data Device Standardisation)

The SECCONDD[119] project looks into this type of security technology for containers. The idea is to develop an interface that enables law enforcement and trade officials to read security data, including stored information from internal security and location sensors. It will thus be possible for them to determine where the container or vehicle has been, whether items (e.g. explosive devices) or people may have been inserted en route, and whether there may be hazardous items within it.

[118]This description of the system is based on: Wessel, R. (2006) *Airport monitoring system combines RFID with video*
[119]Secure Container Data Device Standardisation, PASR 2005

4.6 Machine Readable Travel Documents (MRTDs)

Basic technologies: *RFID*
Storage technology
Biometrics
Communication technologies

A Machine Readable Travel Document (MRTD) is an international travel document (e.g. a passport or visa) containing data that can be read by a human, as well as machine-readable data. All states that have a contract with the International Civil Aviation Organisation's (ICAO) must use Machine Readable Passports by 2010. 110 states use such passports today, and 40 are planning to upgrade to the biometrically enhanced version by the end of 2006.[120] MDRTs have so far (March 2006) been implemented in Belgium, Sweden, Norway and Germany.

There are three (3) types of MRTD:[121]

- A *passport* shows that the person is a citizen of the state that issued the passport
- A *visa* shows that the state that issued the visa has granted a person that is not a citizen the privilege of entering and remaining in the state for a specified time and purpose
- *Other travel documents* are essentially special purpose identification/border-crossing cards issued to persons that are not citizens.

This section will focus mainly on *passports,* referred to as *biometric passports*. The deployment of such passports will eventually affect a large number of people: 2 billion passengers a year fly on scheduled air services alone!

One of the main reasons for implementing Biometric passports is the need to make passports more secure against forgery, and to make border control more reliable. According to ICAO biometrics can be used to improve the quality of the background checking performed as part of the application process for passport, visa or other travel documents, and they can be used to increase the strength of the binding between the travel document and the person who holds it.[122]

The process of implementing biometric passports has also been driven by the United States. The US have insisted that countries whishing to use the Visa Waiver programme (where citizens don't have to apply for a Visa to get into the US), must have a programme in place for putting biometric chips in their passports.[123]

The new passports with Integrated circuits should have a maximum validity of 10 years. 5 years is recommended by ICAO.

---

[120]ICAO MRTD Report Volume 1/Number 1 (2006)
[121]ICAO TAGMRTD/NTWG (2004) *Biometrics Deployment of Machine Readable Travel Documents*
[122]ICAO TAGMRTD/NTWG (2004) *Biometrics Deployment of Machine Readable Travel Documents*
[123]Meints, Hansen (2006) *D 3.6 Study on ID Documents*

Identification, verification and authentication
Identification is about finding out who somebody is. This involves finding an answer to the question: *Who are you?* Authentication is closely linked to identification, as it deals with the verification of identity. Authentication – or verification – is about finding the answer to the question *Are you who you say you are?*

Three different characteristics are normally used to authenticate someone's identity:

- Something they know (i.e. a password or PIN-code)
- Something they have (i.e. ID, smart-card or other type of identification)
- Something they are (physical characteristics, biometrics)

The use of biometrics for identification and verification may be feasible in the following situations related to international travel:

- Initial MRTD issuance
- MRTD renewal
- MRTD document and document-holder inspection for purposes such as border control or airline check-in

4.6.1 Components of a biometric passport

A biometric passport consists of the actual document, normally in the form of a booklet, and a tiny chip.

The information in the passport may be found in three different places:

- In the Visual inspection zone (VIZ). This area contains mandatory and optional data in a layout specified by ICAO.
- In the Machine readable zone (MRZ). This area contains elements in a form and position that are absolutely mandatory, in a standard format (OCR-B).
- In the integrated chip's logical data structure (LDS). The chip contains mandatory and optional data in a data structure specified by ICAO. A symbol on the face of the passport shows that it contains a chip.

In addition, there is a photograph of the user as a visual link between the holder and the passport.

ICAO has made a set of criteria for the chips that should be used in the passports.[124] The Integrated Circuits (IC) have to conform to the ISO standard ISO/IEC 14443 (proximity – within 0 to 10 cm) type A and B. This standard has been chosen in order to ensure global interoperability and readability (that a passport can be read at any border). The chip must

[124]ICAO (2004) *Use of Contactless Integrated Circuits In Machine Readable Travel Documents*

also have enough storage space to be able to hold the information necessary (see description of the LDS later in this chapter).

ICAO has chosen to use a *contactless* IC, which means that it can be read at a distance. The contactless system consists of the actual IC, which is integrated into the travel document, and a Machine Reader. The Machine Reader communicates with the IC through radio waves, and may have either read or read/write capability. If the latter is the case, the IC can be initially programmed and then re-programmed via the Reader. The Reader will normally be connected to a computer system.

The frequency used by ISO/IEC 14443 devices is 13.56 MHz. Water or human tissue does not absorb radio waves at this frequency, so the presence of one or more human beings, a hand, moisture etc. will not affect the readability of the chip from the reader. Encasing the passport in metal such as aluminium foil will, however, prevent reading.

The absolute minimum chip size for biometrics deployment in passports is 32K. But because the technological development in this area is so rapid, ICAO recommends that the states issuing biometric passports should target for chips that are 512K or larger.

The Biometrics
ICAO has chosen *face* as the primary biometric to be used in passports. This biometric is mandatory and will be used globally. *Finger* and *iris* are recommended as secondary biometrics. These can be used if the state issuing the passport chooses to.

There are several reasons given for the choice of face as the primary biometric (see also chapter 3.3): Facial images are available on virtually every person in the world. Face also permits 100% identity confirmation in the inspection process, as the photo could be used for machine assisted checks when a digital image is not available. Moreover, with the photo, facial recognition can be done visually, even when the chip, reader or processing system malfunctions.

The EU has chosen to base its recommendations for the EU-passport on the ICAO standard, with some minor adjustments. Face has been chosen as the primary biometric, and finger as the secondary biometric. Iris is not part of the EU-passport.[125]

For EU-passports, the primary fingerprints to be incorporated in the passports are a plain impression of the left and right index finger. If good prints of these fingers cannot be obtained, plain impressions of middle fingers, ring fingers or thumbs shall be recorded. The storage format is CBEFF – Common Biometric Exchange File Format.[125]

One of the main challenges with biometrics in passports is interoperability. Many different states, using different vendors, will issue passports, and these passports have to be read at every border:[126]

---

[125]EU – Passport Specification (2006) *Biometrics Deployment of EU-Passports*
[126]ICAO TAGMRTD/NTWG (2004) *Biometrics Deployment of Machine Readable Travel Documents*

Because there are no global standards in place for any of the biometrics chosen, ICAO has made it mandatory to store the actual image of the biometric in the Logic data structure on the IC. The issuing country can choose to store the template (see chapter 3.1.2) in addition to this, if they whish to.

For privacy reasons, it is normally recommended to encode biometric data as soon as possible after they are captured. Templates should be used instead of raw data, and raw data should be destroyed as soon as possible.[127] By choosing to store the image instead of a template, ICAO (and the EU) removes the basis of the privacy enhancing nature of biometric technology, which is based on the use and irreversibility of templates.[128]

The Logical Data Structure (LDS)
The Logical Data structure describes what data should be stored in the IC, and how the data should be stored.[129]

All the data from the Machine Readable Zone (MRZ) is mandatory in the Logical Data Structure, as is the facial image of the passport holder. In addition to these data, the security data that is needed to validate the integrity of the passport are mandatory. The rest of the data fields are optional, and some are reserved for future use.

The current recommendation is that the chip should be "write once". In the future, the chip will have to support "write many" applications. Among the uses foreseen for this are:[130]

- The state issuing the passport may whish to write a second biometric into the LDS, for example to update a facial biometric as a result of plastic surgery or to add a different type of biometric at a later date, for instance an iris image
- The state inspecting the passport may write a second biometric into the LDS – for instance to add a new and updated image of the passport holder
- The updating of visa data
- The updating of frequent traveller data
- The storage of travel records
- The storage of automated border clearance records.

If the state issuing the passport chooses to add fingerprints or irises, then at least one fingerprint image or iris image must be recorded.

[127]Albrecht, A. (2003) *BIOVISION: Privacy Best Practices in Deployment of Biometric Systems*
[128]Van der Ploeg, I. (2005): *Biometric Identification Technologies: Ethical Implications of the Informatization of the Body*
[129]The information in this chapter is based on ICAO (2004): *Machine Readable Travel Documents Development of a Logical Data Structure – LDS – for Optional Capacity Expansion Technologies*
[130]ICAO TAGMRTD/NTWG (2004) *Biometrics Deployment of Machine Readable Travel Documents*

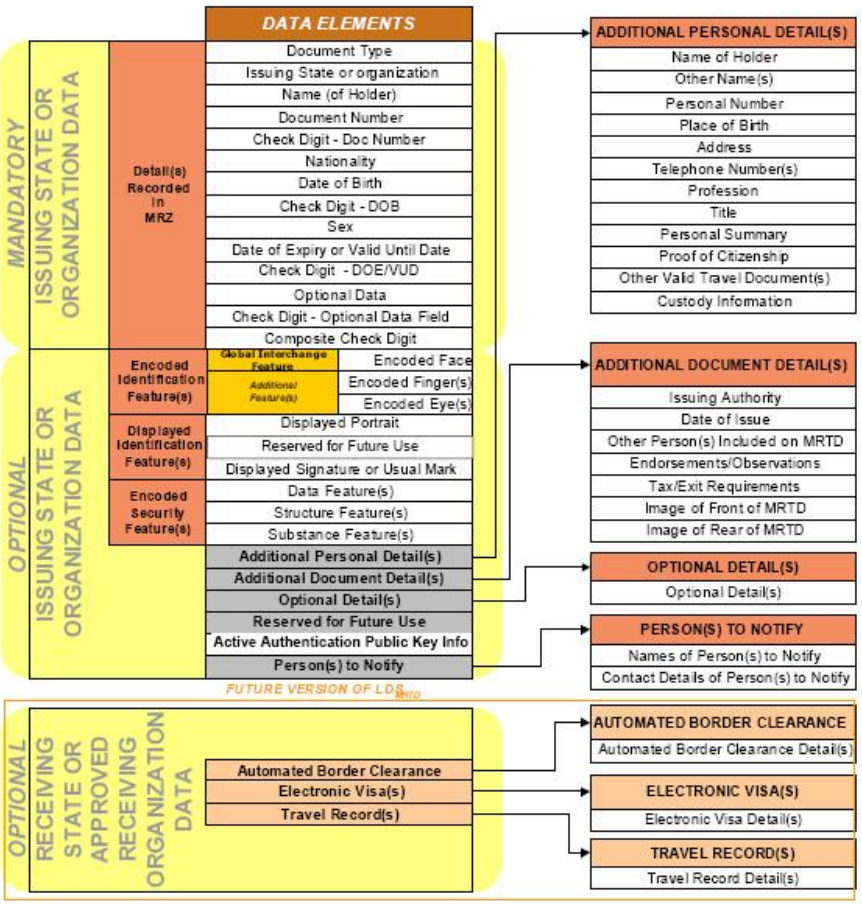

Figure 2: Mandatory and optional data elements defined for LDS (Version 1.7)

4.6.2 Security in biometric passports

Biometric passports have raised much debate, in particular related to the security of the biometric information. It is feared that the information can be stolen by skimming (reading the information at a distance without the owner's knowledge) or eavesdropping (intercepting the information when it is transmitted).

ICAO admits that both skimming and eavesdropping is feasible. To address these concerns a scheme for "basic access control" (BAC) has been developed and recommended for use by the issuing states. Under BAC the inspection system uses a "key" derived from numeric data elements in the MRZ to "unlock" the chip so that the system can read it. Thus the passport must be open in order for the chip to be read (unless the data from the MRZ is somehow known in advance), and the holder is assured that his data can be read only when he hands

over his passport.[131] This access control method is optional.[132] If it is implemented, it is required that the chip enforces encryption of the communication channel.

Organisations that have pointed to privacy and security requirements that should be addressed when combining technologies such as RFID and biometrics – like the Article 29 Data Protection Working Party – has not been heard.

The data from the MRZ and the photographic image will be stored unencrypted in the Logical Data Structure. States that wish to restrict access to the additional biometrics may do so by encrypting them.

Security issues with BAC
In order to achieve successful authentication the initial key of the passport is computed from the machine readable zone. For this purpose the parts which can be checked against a parity number are used (so called key seed material): passport-id, birthday and validity of the passport.

The calculative cryptographic key size of this initial key is ~56 bit: [133]

- passport-id: 10^9 possibilities (9 digits)
- birthday: 365*100 possibilities (~ 100 years)
- validity: 365*10 possibilities (~10 years)

Yet it is possible to limit some of the possibilities due to restrictions that occur with regards to possible birthdates and the validity of the passport: The birthday 14th of November 1965 will be turned into the digit 651114* (*stands for check digit). The birthday 14th of April 1965 will be turned into the digit 650414*. The third and fourth number map the month in which the passport holder was born. This means the third number can only be a 1 or a 0. As the passport is valid for a maximum of 10 years it is possible to limit the possible numbers of the validity date, too. The date of expiry 14.04.2016 is printed as 160414**. Thus the known structure of the machine readable zone reduces the entropy of the key seed material.

Dutch security experts presented a cryptographic key size reduced to 35 bit due to further assumptions of the age of the passport holder and the passport-id derived from the date of issue.[134] With a brute force attack they were able to find the correct key within a few hours.

4.6.3 Passport databases

Different European states follow different strategies when it comes to how they handle and store passport data: Central databases are planned in the UK, The Netherlands, Norway and Sweden (storage planned at the police). In Norway, there is currently a centralised database for passport data, and it has been proposed to expand this to also include fingerprints when

[131] McMunn, M. K. (2006): *Machine Readable Travel Documents with biometric enhancement: The ICAO Standard*
[132] ICAO (2004) *PKI for Machine Readable Travel Documents offering ICC read-only access*
[133] German Federal Office for Information Security (2005) *Common Criteria Protection Profile. Machine Readable Travel Document with „ICAO Application", Basic Access Control* and German Federal Office for Information Security (2005): *Digitale Sicherheitsmerkmale im elektronischen Reisepass*
[134] Heise Online (2006) *ePass-Hack im niederländischen TV demonstriert*

these are included in the passport in the future. Both the Norwegian Board of Technology and the Norwegian Data Inspectorate have advised against this in their response to the official hearing on the matter.[135] In Italy and Germany the data needed for the passports, including biometric data, will be stored decentralised.[136]

A challenge is that even if a citizen has a passport issued in a country where the passport data are handled according to a good privacy practice, there is no way of controlling what happens to the data – for instance where and how it is stored – when they are read at the border of a country that may have a different view on privacy.

It has been discussed to have a central European passport database, but there are no plans for such a database at the moment.

4.7 ID cards

Basic technologies: *RFID*
Storage technology
Biometrics
Communication technologies

Most EU member states have implemented a form of ID card - the only members without any form of identity card scheme are the United Kingdom, Ireland, Denmark, Latvia and Lithuania.[137] ID card systems are implemented in a number of different ways: Some use RFID technology, and it is supposed that biometrics will become a feature in the near future.

ID cards can be used in conjunction with digitized information (for example biometrics or digital signatures). These provide the ability to uniquely identify an individual, and thus could be used, for example, to prevent fraud, control immigration and combat crime as well as for non-security applications – e.g. access to public and private sector services.

There has been heated debate in the UK – one of the above mentioned countries that still does not have a national ID card – over government plans for ID cards. Under current UK government plans, ID cards would be used in conjunction with a biometric identifier, which would allow access to over fifty different types of data on an individual, stored on a centralized database. This controversial scheme has been described as the most comprehensive card system proposed in Europe to date.[138]

A standard for a European Citizen Card (ECC) is currently being developed. The work is done under the European Committee for Standardisation (CEN), and should be published in October 2006 according to plan. In July 2005, the Presidency of the Council of the European

[135] See http://www.teknologiradet.no/hringsuttalelse%20biometrisk%20pass_N-AIN.pdf.file (Norwegian) and http://www.datatilsynet.no/templates/Page____1113.aspx (Norwegian)
[136] Meints, Hansen (2006) *D 3.6 Study on ID Documents*
[137] UK Home Affairs Committee Publication: *Home Affairs – Fourth Report*
[138] European Parliamentary Technology Assessment Network (2006) *ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries*

Union invited the Article 6 Committee to draft common security standards for national identity cards. It is specifically requested that they focus on:[139]

- Use of biometrics
- Common standards for the card interface
- Measures to ensure that the data stored on the card is protected, but can be read by other member states (including measures like Enhanced Access Control and PKI).

System example: Belgian ID card[140]

Belgium was the first country in Europe to introduce digital ID cards. The cards are issued to all citizens aged 12 years or older. The card is the size of a normal bank card, and contains the following information:

- name
- title
- nationality
- place and date of birth
- national number
- picture
- signature
- signature of issuing civil servant
- validity dates
- card number
- place of delivery of card

The chip on the card contains the same information, but includes an address file in addition to the above mentioned information.

The Belgian card holds three different 1024-bit RSA private signing keys. In order for the citizen to use the keys to generate a digital signature, a PIN-code must be entered. This is done through trusted hardware, like a smart-card reader.

All paper-based cards should be replaced by the new cards by the end of 2009.

---

[139]Council of the European Union (2005) *NOTE from Presidency to Strategic Committee on Immigration, Frontiers and Asylum: Minimum common standards for national identity cards*

[140]Meints, Hansen (2006) *D 3.6 Study on ID Documents*

System example: Project INES (France)[141]

Project INES ('*Identité Nationale Electronique Sécurisée*', or 'Secure Electronic National Identity') is a project to produce a new, compulsory, electronic ID card in France.

The current paper ID in France is not mandatory, and is distributed for free. This has led to a problem with ID fraud, as over 500 000 ID cards were reported missing in 2004. One of the proposed solutions to this is to make the new card mandatory, and to include biometric information in the card. Two biometrics have been proposed: Face will be the primary biometric. The secondary biometric may be scanned fingerprint images, but iris scans have not yet been ruled out as an alternative.

In addition to being an identity card, the new electronic ID can also be used as an electronic signature for e-government and e-commerce services. The holder's personal information and biometric identifiers will be stored in a contact-less RFID chip.

The same personal information that can be found in the chip will be stored in a central database, and the corresponding biometric information will be stored anonymously in separate files.

[141] IDABC: FR: *Future French eID card to become compulsory* and FR: *Future French electronic ID card to include two biometrics*

Chapter 5 Data Storage

Data storage is the holding of data on an electromagnetic or optical medium, such as a hard disc, a magnetic tape, a CD or DVD etc. The data can be *accessed* using an adequate reading device and, depending on the technology, be *modified* or *deleted*.

5.1 Database systems

A database is defined as an organised collection of data. In principle, this may also include non-digital data, like lists and index cards, but in this report we will refer to organised data in digital form when we use this term.

Databases can be organised in different ways, but a common feature is that the data is organised into elements, that are then linked together. The most common type of database is the relational database. Here, different pieces of information (data elements) are linked together with one or more other data elements. For instance can *person* (name), be linked to one or more *addresses*, that again are linked to a *type describing the relation* – one address can be the home address and one the business address. Different persons can be linked together by *characteristics describing the nature of their relation* (father/son, friend, colleague etc).

This way of organising data makes it easier to link together information and retrieve it again when needed, and it makes it possible to search large amounts of data to find relevant information in a way that was impossible with manual filing. Databases are an integral part of almost every computer system, ranging from private CD archives via commercial customer- or product databases to public systems like health records or electronic case files. Important database systems used as part of European security are VIS (the Visa database), SIS (Database of the Schengen information system) and EURODAC (Database with information on asylum seekers, see chapter 3.5). This report will mainly focus on the latter systems and only touch on commercial databases where they are relevant in a security setting (see chapter 5.2.1).

5.1.1 Privacy challenges with databases

A major challenge when dealing with large sets of data relates to the quality of the data. It is important that all records are maintained in order to make determinations about an individual with sufficient accuracy, relevance, timeliness, and completeness. Other ways there is a risk that a government agency, airline or other will make decisions or single someone out based in inaccurate, incomplete or out of date records.[142] The fact that most of these processes are intransparent to the user makes it impossible for a person to check if data processed about him or her are correct.

Database systems are also vulnerable to so called *function creep*, that is the use of the data for something other that the original intention. An example of such function creep was seen

[142]United States Government Accountability Office (2005) *DATA MINING Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*

when the Norwegian data base of asylum seekers – which also contains biometric information like fingerprints – was opened to the police in criminal investigations.[143] The original intention of the data base was to help establish the identity of asylum seekers.

In the case of biometric information, it is often pointed out that storing such information in central databases pose a greater risk than storing it locally, for instance on a card with an integrated circuit. The reasons for this are both the risk of *function creep* mentioned above, but also that central databases are at a higher risk of breaches in security.[144]

5.2 Data Retention

By Data Retention we mean the capturing and storing of data for different purposes, such as billing, customer relationship management, etc. Privacy issues with Data Retention are associated with the storing of personal data that are not needed for a practical purpose, or the storing of such data for a longer period than necessary.

The types of data most commonly referred to when data retention is discussed, is data related to ICT, such as the traffic and location data of communications taking place over mobile phones, SMS, landline telephones, faxes, e-mails, chat rooms, the Internet, etc.

The retention of traffic and location data is controversial. Rules vary from country to country, both as to the amount of time data can be stored, and as to where the responsibility for the data and the cost of the data retention should be – with the authorities or with the telecommunications companies?

Other areas where data retention could be seen as a security measure and therefore required by law may be: Toll booth passing, airline traffic passenger lists, bank- and credit card transactions, library lending records etc.

System example: EU Directive on data retention[145]

The background for DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is the terror attacks in Madrid and London. These attacks have lead to local initiatives on data retention in the different Member States, and the directive seeks to harmonise the different practices.

It is also a result of the significant growth in the possibilities afforded by electronic communications. Data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

The directive applies to traffic and location data and to the related data necessary to identify the subscriber or registered user. The content of the communication will not be retained.

---

[143]The Norwegian Ministery of Local Government and Regional Development (2003) *Rundskriv H19/03: Ikrafttredelse av endringer i utlendingsloven og utlendingsforskriften*
[144]The Norwegian Board of Technology (2005) *Elektroniske spor og personvern*
[145] The information in this chapter is based on the text of the directive itself

The data that will be retained include:[146]

- The phone number or, in case of Internet use, user ID, plus name and address of the caller
- The destination of the call (phone number or user ID, plus name and address)
- The date, time and duration of the communication (start and end time, alternatively log-on and log-off times, plus IP-address for Internet communication)
- The type of communication (telephone service or Internet service)
- What equipment was used (IMSI and IMEI number of both caller and called party, date, time and cell ID for anonymous calls)
- The location of mobile communication equipment (Cell ID)

The directive stated that the data should be retained for periods of not less than six months and not more than two years from the date of the communication.

System example: DNA databases
A DNA-database is a centralized database for storing DNA-samples of individuals. The nature of the samples and the rules for what samples that can be registered and criteria for when a sample may be entered varies greatly from country to country.

Many types of DNA storage systems exist, but most are not presently used for identification purposes. These types of databases include research databases, blood banks and tissue storage facilities.[147]

We will here focus on systems that store samples of DNA in order to compare them with samples collected at crime scenes. Countries that currently have such databases include the United States, Germany, Britain, Norway, Finland, Belgium, Australia and Denmark.

The technology in this area is developing quickly. Where earlier DNA samples were only used for "fingerprint matching", it is now becoming feasible to generate the beginning of an actual profile (gender, ethnicity) from even the smallest sample of trace DNA.[148]

One important question when it comes to the establishing and use of DNA databases are related to how broad the sample base should be: Should only convicted felons be added, or should DNA samples be taken of everyone arrested? Should the samples be retained even if the case is dismissed or the person in question acquitted? Should there be a universal data base including all citizens?[149] In Europe we have seen how the threshold for inclusion is lowered again and again. In the Netherlands the criterion for mandatory giving up DNA was changed from suspects of crimes with 8-years sentences to suspects of crimes with 4-years sentences.[148] In Norway, a committee appointed by the Ministry of Justice and the Police suggested that anyone sentenced for a crime should have to give up DNA for the central

[146] See chapter **Feil! Fant ikke referansekilden.** for explanations of the technical terms related to telecommunications
[147] OECD Working Party on Information Security and Privacy (2004) *Biometric-based technologies*
[148] Van der Ploeg, I. (2005) *Biometric Identification Technologies: Ethical Implications of the Informization of the Body*
[149] Cole, S. A. *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*

DNA database. Previously only felons in cases of murder, violent crimes and serious crimes related to narcotics had to give up DNA.[150]

Another question is whether only a DNA "fingerprint" (only enough information to be used for identification) should be stored, or if the actual DNA sample should be retained, making further analysis in the future possible.

5.2.1 Commercial data retention

Basic technologies: *Communication technologies*
Data retention
Data bases
Data mining

Most commercial actors will retain as much data as possible about their customers, to be used for internal R&D purposes and as a marketing tool. To what extent they are allowed to use this for targeted marketing will vary from country to country. However, following the activities, specifically in the US after September 11th 2001, we have seen an increasing tendency where commercial data are used for security purposes.

The US Departments of Justice, Homeland Security, and State and the Social Security Administration reported in 2005 that they purchased personal information from so called information resellers for approximately $30 million. About 91 percent of that was for law enforcement (69 percent) or counterterrorism (22 percent).[151]

Information resellers are businesses who collect and aggregate personal information from multiple sources and make it available to their customers (see also chapter 0 for a description of Data Mining). The sources may be public records, publicly available information (for instance on the Internet) and information from proprietary sources such as private businesses.

There are also examples where law-enforcement agencies address businesses directly in order to get access to their customer data: In the USA the U.S. Department of Justice filed a motion in federal court seeking a court order that would compel Google to turn over a multi-stage random sample of one million URL's from Google's database, and a computer file with the text of each search string entered onto Google's search engine over a one-week period (absent any information identifying the person who entered such query).[152] Other search engines, like Yahoo and MSN has received the same request from the Department of Justice, and has complied.

Law enforcement authorities can in this way be granted access rights to data from businesses in order to conduct their investigations. In Germany, for example, the law

[150]The Norwegian Ministry of Justice and the Police (2005) *NOU 2005:19: Lov om DNA-register til bruk i strafferettspleien*
[151]United States Government Accountability Office (2006) *PERSONAL INFORMATION Agencies and Resellers Vary in Providing Privacy Protections*
[152]United States District court for the northern district of California, San Jose division (2006) *Gonzales vs. Google*

enforcement authorities are entitled to obtaining data controlled by legal entities to substantiate or rule out a concrete suspicion of a criminal act.[153]

It is possible to differentiate access to data from business entities based on the criterion of suspicion. Access to such data by law enforcement authorities can result from a concrete suspicion against a person suspected of a criminal act. Or law enforcement authorities seek to access information to investigate a potential and ubiquitous risk, for example of terrorist attacks. These investigations are not based on a concrete suspicion but are subject of law enforcement authorities' attempt to detect conspiracies to committing serious crimes. In this context the potential suspect is not known to the authorities. In order to conduct such an investigation law enforcement authorities seek to collect and analyze information on persons that fit a certain profile that indicate their capability and willingness to conduct such serious crimes. Data screening as a means of preventing terrorist attacks[154] does by definition include the screening of personal data from a large group of people. It is thus highly privacy relevant, especially as the data of innocent persons is processed.

If data collected by business entities is accessed by law enforcement authorities for the purpose of data screening the risks to privacy are apparent. Many business entities run customer relationship management (CRM) programs which include the creation of a customer profile. This profile contains accumulated information on customers' preferences and habits and by these means even originally irrelevant data gains unexpected significance. Linking such data available in several companies' data-warehouses possibly enables law enforcement authorities to obtain detailed information about citizens. Most people leave data traces in business environments very thoughtlessly. Due to the associated risk to the fundamental right of privacy access to such data for investigations based on no suspicion must follow very distinct and limited legal provisions.[155]

5.3 Border control systems

Basic technologies: *Database systems*
Biometrics
Communication technologies

This section looks at various systems used at borders in order to assess that individuals are who they say they are, and have the right to access the nation or region performing the control. These systems are normally based on the application of databases and biometric identification.

Because Machine readable travel documents (MRTDs) or *biometric passports,* are more connected to RFID and sensor technologies, issues related to this technology –including passport databases – are discussed in Chapter 4.6.

[153]Regulated in Article 161a of the German Code of Criminal Procedure.
[154]In Germany data screening (so called *Rasterfahndung*) was subject to a ruling by the Constitutional Court. For more information see PRISE report D 3.2 See also Achelpöhler, W. and Niehaus H. (2004) *Data Screening as a Means of Preventing Islamic Terrorist Attacks in Germany*
[155]For more details please see PRISE report D 3.2 Legal Report

System example: SIS II

The original Schengen agreement was made in 1985 between Belgium, France, Luxembourg, the Netherlands and Germany. The idea was (and is) to remove border control between the participating countries, and to compensate for this by controlling the outer boundaries of the Schengen area and increasing police co-operation between member countries.[156]

The SIS (Schengen Information System) is a common information system that allows national police authorities within Schengen to access and share information. The original system was introduced in 1995. SIS currently includes 13 EU members, plus Norway and Iceland, but is expected to expand. SIS II is an updated version of SIS, and it is planned implemented in 2007.

Through the system, the police authorities get information related to alerts on persons or objects. This information is used for cooperation in criminal matters, for the control for persons at the borders and for the issuing of visas and residence permits. There are six different categories of alerts in SIS II:[157]

1) alerts on persons who should be refused entry to the Schengen area;
2) alerts on persons wanted for arrest (in view of surrender or extradition);
   Information that can be entered into the system includes: the identity and nationality of the wanted person and information about the offence and judgement.

   The information may be accessed by police and border authorities, national judicial authorities and those responsible for public prosecutions, The European Police Office (Europol) and Eurojust.[158]

   The data will be kept in the system until the wanted person has been surrendered or extradited. The alerts for arrest and additional data will automatically be erased after 10 years.
3) alerts on persons to ensure protection or prevent threats;
   Alerts can be made on missing persons who needs to be placed under temporary police protection, either for their own protection or in order to prevent threats, and on missing minors.

   The information may be accessed by police and border authorities, and national judicial authorities and those responsible for public prosecutions.

   The alerts should be erased as soon as the person is placed under police protection. The alerts will automatically be erased after 10 years.
4) alerts on persons wanted for judicial procedure;
   Alerts can be issued on witnesses, persons summoned to appear before the national

---

[156]Rieker, P. and Knutsen, B. O. (2003) *EUs "nye" sikkerhetspolitikk: Bekjempelse av terrorisme og internasjonal kriminalitet*
[157]The following is mainly based on: European Commission Press Release MEMO/05/188, *Schengen: from SIS to SIS II* and Commission of the European Communities *Proposal for a council decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*
[158]The European Union's Judicial Cooperation Unit, http://eurojust.europa.eu/

court or who are to be served with a criminal judgement or have to serve a penalty. The information may be accessed by police and border authorities, and national judicial authorities and those responsible for public prosecutions, and Eurojust.

Alerts will be erased as soon as the whereabouts of the person concerned has been ascertained. The alerts will automatically be erased after 10 years.

5) alerts on persons and objects for discreet surveillance or specific checks;
To prevent threats to public security, alerts can be made on persons or vehicles, boats, aircrafts or containers in order for them to be put under discreet surveillance or specific checks. This can be done when there is clear evidence that the person concerned intends to commit or is committing numerous and extremely serious criminal offences, or where an overall assessment gives reason to suppose that the person will commit such offences in the future.

Information on persons entered into the system include: Name and possible aliases, date and place of birth, sex and nationality, photographs, fingerprints and physical characteristics, whether the person is armed, violent or has escaped and details on the alert, including links to other alerts.

The information may be accessed by police and border authorities, and national judicial authorities and those responsible for public prosecutions, and Europol.

Alerts on persons will automatically be erased after 3 years.

6) alerts on objects for seizure or use as evidence in criminal proceedings

Currently, the SIS database holds over 13 million records, of which 1/10 are related to "wanted persons".[159]

Some of the most important new features of SIS II will be central storage of European Arrest Warrant and extradition information, and the storage of biometric data like fingerprints and photographs. This is a major change compared to today's situation where information is only exchanged bilaterally. The new system will also contain the possibility of entering information on persons whose identity has been abused in order to avoid further inconveniences caused by misidentifications. This is subject to the consent of the individual in question.[160]

SIRENE
In order to ensure the exchange of all supplementary information that may be needed between police and other authorities, each Member State have to establish a SIRENE

[159] Article 29 Data Protection Working Party (2005) *Opinion 6/2005 on the Proposal for a Regulation of the European Parliament and of the Council (COM (2005) 236 final) and a Council Decision (COM (2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for Regulation of the European Parliament and of the council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final)*

[160] Commission of the European Communities (2005) *Proposal for a council decision on the establishment, operation and use of the second generation Schengen information system (SIS II)*

authority (Supplementary Information Request at the National Entry). SIRENE is made up of representatives from the national and local police, customs and the judiciary.[161] The SIRENE office shall also verify the quality of the information entered into the SIS II.

System example: VIS
VIS (Visa Information System) will be a system for exchanging visa data between Member States. Today all member countries administrate their own visa systems. Citizens from 134 countries require a visa to enter the EU. Until now it has been possible for an applicant that has been turned down at one consulate to proceed to the next (so called "visa shopping").

An important objective for the new system is to prevent this. Information on previous applications and reasons for rejection will be centrally available. Other objectives include the ability to check that the carrier and the holder of the visa are the same person, and to assist in the identification and documentation of undocumented illegal immigrants.[162]

The following data will be included in the system:

- alphanumeric data on the applicant and on visas requested, issued, refused, annulled, revoked or extended;
- photographs;
- fingerprint data;
- links to other applications or databases where the subject might be registered, such as SIS.

The VIS will be based on a common technical platform with SIS II. It will be composed of a central structure and national interfaces. These interfaces will be supplemented with links to consulates and border checkpoints. The data will be collected by the consulates in the different member states and then transferred to the central database, where it will be accessible to all member states. The system capability is estimated – in particular as regards biometric data – to be able to contain the data concerning about 20 million of visa applications annually, which would result into 70 million of fingerprints data to be stored in the system over a 5 year term.[163]

The ARTICLE 29 Data Protection Working Party points out that: *...there have to be particularly rigorous checks if these biometric data are to be stored in a centralised database, as this would substantially increase the risk of the data being used in a manner that was disproportionate to or incompatible with the original purpose for which they were collected.*

It is stated in the proposal for regulation that the data should not be kept longer than necessary. The appropriate period is set to five years, in order to be able to take data on previous visa applications into account when assessing new visa applications. After the five

[161]From www.oasis.gov.ie
[162]Proposal for a regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between members on short stay-visas
[163]Article 29 Data Protection Working Party (2005) *Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas*

year period, the data should be deleted. The data can be deleted earlier if there are grounds for this.

5.4 The exchange of passenger information in international travel

There are different types of systems that are based on the exchange of passenger information in international travel:[164]

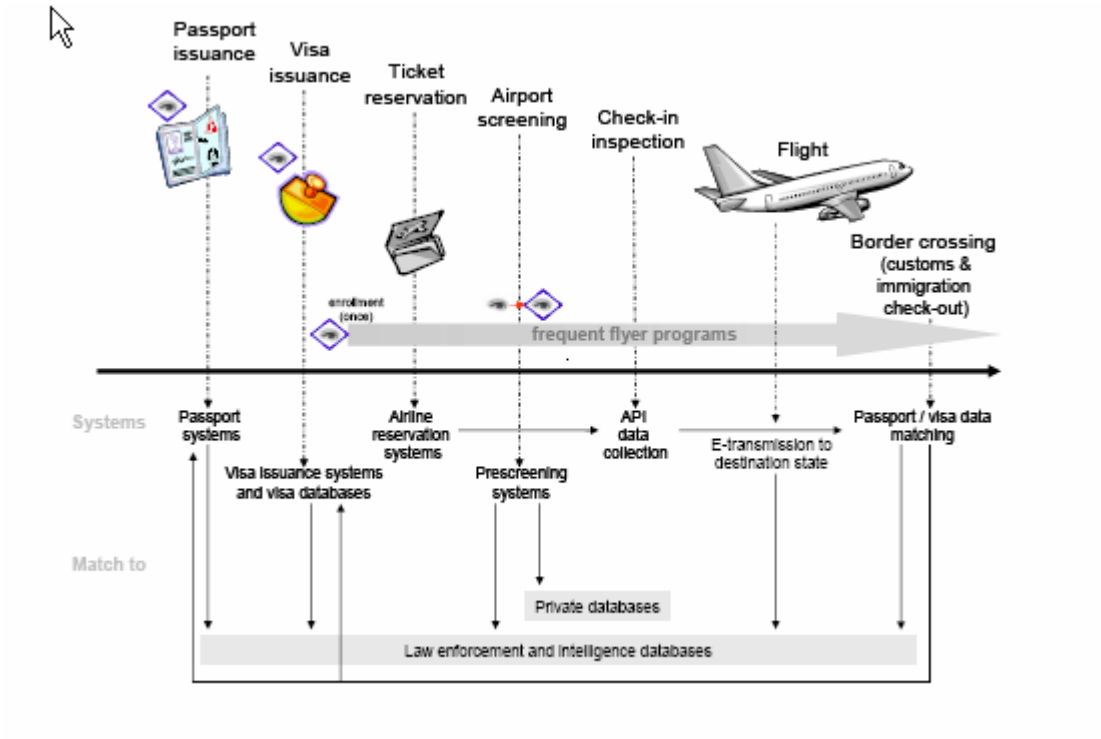

Figure3: Categories of systems on a chronologic axis (OECD)

5.4.1 Airport screening

Airport screening (or pre-screening) systems enable the authority in charge of airport security (*e.g.* for access to aircrafts and boarding zones) to rationalize the screening of passengers. Instead of randomly selecting passengers for deeper inspection, pre-screening systems use profiling to select the passenger where a deeper inspection is required. Pre-screening systems generally process:

1) Data related to the identity of the passenger as provided by airline reservation systems or via machine readable travel documents.
2) Data stored in different databases to which the passenger's identity is matched. This may include law enforcement and private marketing databases.

[164]OECD Working Party on Information Security and Privacy (2004) *Background material on biometrics and enhanced network systems for the security of international travel*

3) Various criterions to determine why one individual may proceed through normal check-in, deeper check-in or may be rejected for check-in.

Advance Passenger Information

Advance Passenger Information (API) systems aim at enabling the customs and/or immigration officials to organise their clearance process in advance of the arrival of the flight. Depending on the country, API systems allow for processing of API data before boarding. Such systems process the information collected by the airline company during the check-in process. This information, called Passenger manifest, may be automatically collected from machine-readable travel documents (passports, visas, or other documents).

The information is electronically transmitted from the airline to the competent agency. The collected data is checked against lookout databases and may itself feed other systems, for instance for tracking or profiling purposes.

In addition to the API data, the US requires the airlines to transfer data extracted from the Passenger Name Record (PNR). The Passenger Name Record (PNR) are the files created by the airlines when a passenger books a journey. They are stored in the airlines' reservation and departure control databases. PNR allows different actors, like travel agents, computer reservation systems (CRS), carriers and the handling agents at the airports to recognise each passenger and have access to all relevant information related to his or her journey. This can be departure and return flights, connecting flights, special services required on board the flight (kosher or vegetarian meals, if assistance is required, etc).[165]

Advance Passenger Processing

Advance Passenger Processing (APP) is a method for collecting API which allows for the transfer and process of the passenger's information before boarding. A screening process returns a board/no board status flag. APP allows airlines to check passengers at check-in. It allows for the collection of passenger data and transmission of the data to the destination's border agencies prior to arrival. APP electronically notifies the airline and confirms the existence of a valid visa for those passengers who need it. The whole process is done in real time.

Most focus on API systems has been on the exchange of PNR data from airlines serving the European market to the US. The previous agreement between the EU and the US on the exchange of PNR data expired on September 30th 2006. It was replaced by a new agreement, stating that the US Department of Homeland Security can access PNR data from the air carrier's reservation systems. The data will then be handled according to US laws and constitutional requirements.[166]

Passenger data is also of interest to European authorities: In the UK the police have access to personal online details of all passengers travelling in and out of Britain.[167] The intention is to extend the system to include domestic flights as well. Also Denmark has suggested that the

[165]European Commission Airline passenger data transfers from the EU to the United States (Passenger Name Record)
[166]The European Union (2006) *AGREEMENT between the European Union and the United Stats of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security*
[167]Bunyan, T. (2005) *While Europe sleeps...*

police should be given access to Airlines' information on all passengers travelling to or from Denmark for mandatory screening.

A new French immigration act includes the creation of a fingerprint/facial image database for resident card applicants and illegal immigrants as well as for visa applicants to allow for verification at ports of entry.[168]

The Article 29 Data Protection Working Party has pointed out that bodies such as the International Civil Aviation Organisation (ICAO), the World Customs Organisation (WCO) and the International Air Transport Association (IATA) have developed clearcut definitions of API data in order to achieve harmonised standards and uniform practices. The agreed guidelines state that API data consist of the data that can be found in the machine readable zone of travel documents. PNR data exceed this by far.[169]

[168]OECD Working Party on Information Security and Privacy (2004) *Background material on biometrics and enhanced network systems for the security of international travel*

[169]Article 29 Data Protection Working Party (2006) *Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data*

Chapter 6 Analysis and Decision support

The area of analysis and decision support is closely related to that of databases. It is the ever increasing amount of data in both commercial and government databases that have made the analysis of such data both a prosperous business and part of some nations' security strategies.[170]

6.1 Privacy challenges with analysis and Decision support

It is widely recognised that when different pieces of data about a person can be put together, it reveals more about that person than the information items viewed separately. An important privacy principle related to databases containing information about persons, is therefore that only the data necessary to fulfil the purpose of the system should be collected, and that it should be deleted when it is no longer needed (the principle of purpose).

Lately, we have seen a trend where governments have wanted to connect database systems for purposes that are different from the original purpose of the database system. The intentions of such a strategy may be increased efficiency (for instance in the UK[171]) or security (like the proposal for enhanced interoperability between SIS II, VIS and EURODAC[172]).

Data mining is the most used technique for analysis and decision support. The challenges related to data mining are much the same as for data bases (see chapter 5.1). Aggregation of data lead to more information about individuals, and in most cases of data mining, the data subject does not know that data is being aggregated about him or her – far less which databases are connected.

The issue of data quality is a challenge with all databases. When data is collected from a number of different sources – some public, some commercial – assuring quality becomes even more difficult.

6.2 Data Mining

Data mining is a label for technologies which find useful patterns and rules within large amounts of data. As an indirect consequence these technologies foster the creation of large data pools (data warehouses) which could not have been analysed effectively with traditional methods.[173] With the use of mathematical, or rather statistical techniques, it

[170] See for instance Chapter 6.2 on Total Information Awareness.
[171] OPM (2005) *Research into the use of personal data sets held by public sector bodies*
[172] Article 29 Data Protection Working Party (2004) *Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)*
[173] EPTA (2006) *ICT and Privacy in Europe – A report on different aspects of privacy based on studies made by EPTA members in 7 European countries*

becomes possible to search massive quantities of data for patterns of correlations that produce a new type of knowledge.[174]

The power of data mining technology for security purposes lies in its potential to bring to light non-obvious investigation targets or identify terrorist threats through inferences drawn on decentralized data sets spread around the Web, around the world. Many see the possibilities that this technology offers as necessary to keep up with new security threats, but it also puts an unprecedented level of intrusive power in the hands of those who have access to it.[175]

Data mining generally incorporates three processes:[176]

- *data input*:
  In this phase data are collected in a central data warehouse, validated, and formatted for use in data mining.
- *data analysis*
  In this phase data are typically searched through a query. The two most common types of queries are pattern-based queries and subject-based queries. Pattern-based queries search for data elements that match or depart from a predetermined pattern (e.g., unusual claim patterns in an insurance program). Subject-based queries search for any available information on a predetermined subject using a specific identifier. This could be personal information such as an individual identifier (e.g., an ID number or the name of a person)
- *results output*

The Following figure illustrates the process:

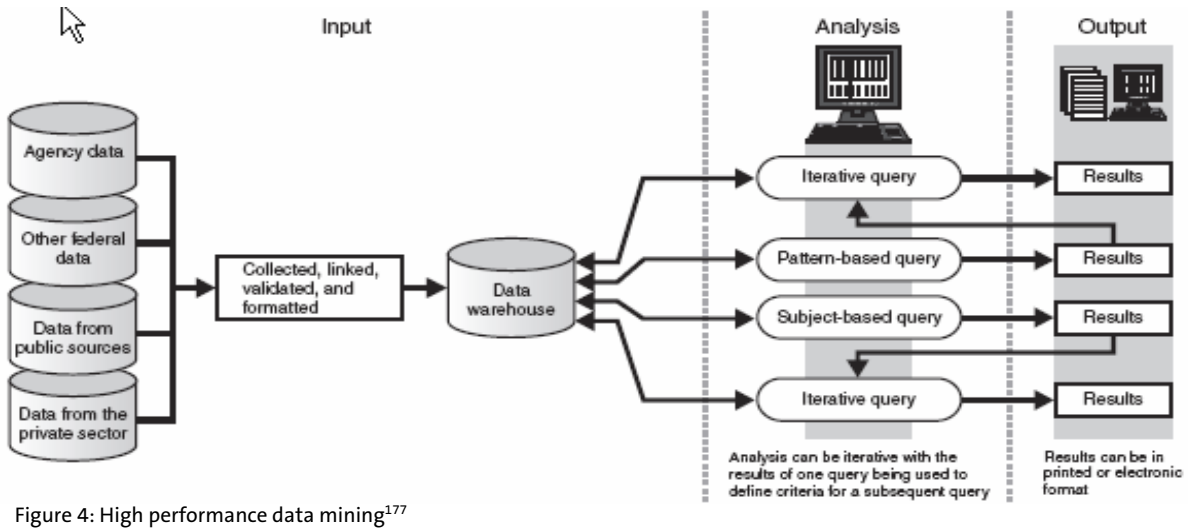

Figure 4: High performance data mining[177]

[174]Hildebrandt and Backhouse (2005) *D 7.2 Descriptive analysis and inventory of profiling practices*
[175]Weitzner et al. (2006) *Transparent Accountable Data Mining. New Strategies for Privacy Protection*
[176]United States Government Accountability Office (2005) *DATA MINING Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*

System example: FBI Foreign Terrorist Tracking Task Force[177]
Following the terrorist attacks of September 11, 2001, data mining has been used increasingly as a tool to help detect terrorist threats through the collection and analysis of public and private sector data. The data mining effort of the FBI Foreign Terrorist Tracking Task Force is aimed at helping federal law enforcement and intelligence agencies locate foreign terrorists and their supporters in the United States.

Reports from the system range from lists of individuals who might meet a certain profile to detailed information on a certain suspect. Such reports typically contain personal information. Reports are shared with field investigators, field offices, and other federal investigators.

These systems use information that the agency collects directly, as well as information provided by other agencies, such as the Social Security Administration, and private sector sources, such as credit card companies. The system uses 30 government sources, 11 commercial sources and 4 international sources, including lost property reported to Interpol and intelligence data.

System example: Predicting behaviour[178]
In a study in 2004-2005 100 MIT staff and students were equipped with special mobile phones. Their call logs, blue-tooth devices in proximity, communication and device usage behaviour were captured. In total approximately 450 000 hours of data were collected (MIT Reality Mining dataset).

By using this data, the researchers have identified some building blocks in individual's behaviour (named *eigenbehaviours)*, and use this to make their analysis. They claim that given the behaviour during the first half of the day, they can predict the remaining behaviours of the day with an accuracy of 79%. This technique can also be used to characterise the behaviour of groups, and to identify how affiliated an individual is to a group. The idea behind the study is that if you can characterise people quickly, match them to similar people and predict their behaviour in the near future, you can build interfaces that can guess the user's preferences, social connections and daily plans.

6.3 Search technology

Search technology has developed enormously over the last years, and some now claim that searching unstructured text soon will replace database technology as the best technology for retrieving connections and patterns of information.

More and more information, both on individuals and businesses are now available on the Internet and in different public and private database systems connected to the Internet. A search engine will systematically go through (crawl) the Internet and index (either make a copy of or register the most important keywords) the pages it finds.[179]

---

[177]United States Government Accountability Office (2005) *DATA MINING Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*
[178]Based on Eagle and Pentland (2006) *Eigenbehaviours: Indentifying Structure in Routine*
[179]Battelle, J. (2005) *The Search – How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*

Combining information from a range of sources can help identify suspicious profiles. Using search technologies, it is possible to set up automatic searches that go through different databases and publicly available sources continuously, searching for patterns that have been observed in previous criminal activities.

One technology that is predicted to improve the search for terrorists on the Internet is *the semantic web*. The semantic web is about *data* rather than *documents.* Much of the motivation is about being able to access information that is today locked away in different proprietary databases. In order to make this work, information items need to be "tagged" the same way by everybody. The idea is to provide a common framework that allows data to be shared and reused across applications, enterprises, and community boundaries. The work on this a collaborative effort led by W3C with participation from a large number of researchers and industrial partners.[180] Various e-government initiatives represent similar efforts. The United Kingdom has developed an Integrated Public Sector Vocabulary.[181]

The US National Security Agency (NSA) has been known to use phone logs to build basic picture of someone's contact network. Clusters of people in highly connected groups become apparent, as do people with few connections who appear to be the intermediaries between such groups. The idea is to see by how many links or "degrees" separate people from, say, a member of a blacklisted organisation.

By adding online social networking data to its phone analyses, the NSA could connect people at deeper levels, through shared activities, such as taking flying lessons.[182] In many cases there exists implicit and/or explicit information in the form of social networks, such as those on the Web. For example, the LinkedIn.com social network comprises a large number of people from information technology areas, MySpace.com, Friendster and Hi5 contain large amounts of social network data (as of August 2006 MySpace had 100 million members).[183] The semantic web is a way of enabling the connection of information from all such sites to look for networks. Research into this area is funded by the NSA.[182]

Rich media search is another important aspect of search as a security technology. All media is eventually converted to raw text or text that describes the content in meta-tags or properties. An advanced search platform will have the ability to identify associative patterns through on the- fly regression analysis and then use these patterns to trigger events or warnings. Rich media search can be improved by integrating speech recognition to transcribe spoken words (from videos and recorded speech) into text which is subsequently indexed by the search engine.[184]

System Example: Total Information Awareness

Total Information Awareness (TIA) was a program with the US Defence Advanced Research Projects Agency (DARPA). The TIA program contained three categories of tools - language

[180]World Wide Web Consotium (W3C): *Sematic web*, http://www.w3.org/2001/sw/
[181]www.esd.org.uk/standards/ipsv
[182]Marks, P. (2006) *Pentagon sets its sights on social networking websites*
[183]Aleman-Meza et al.. (2006) *Semantic Analysis on Social Networks: Experiences in Addressing the Problem of Conflict of Interest Detection*
[184]FAST Search Best Practices TM (2006) *Searching Rich Media*

translation, data search and pattern recognition, and advanced collaborative and decision support tools.[185]

The goal of TIA was to predict terrorist attacks before they happen. The system was intended to scan private and public databases, as well as the Internet, for transactions that might be associated with a terrorist attack. The US Congress stopped the funding of TIA in September 2003.

[185]US Department of Defence (2003) *Total Information Awareness (TIA)*

References

Books and articles

Achelpöhler, W. og Niehaus, H. (2004) Data Screening as a Means of Preventing Islamic Terrorist Attacks in Germany. *German Law Journal,* **Vol. 05 (**No. 05), pp. 495-513

Agre, P. E. (2003) *Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places.* University of California, Los Angeles

Albrecht, A. (2003) *Privacy Best Practices in Deployment of Biometric Systems.*

Aleman-Meza et al. (2006): *Semantic Analysis on Social Networks: Experiences in Addressing the Problem of Conflict of Interest Detection.* Edinburgh: WWW 2006

Article 29 Data Protection Working Party (2003) *Working document on biometrics.* Brüssel

Article 29 Data Protection Working Party (2004) *Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS).* Brüssel

Article 29 Data Protection Working Party (2005) *Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas.* Brüssel

Article 29 Data Protection Working Party (2005) *Opinion 6/2005 on the Proposal for a Regulation of the European Parliament and of the Council (COM (2005) 236 final) and a Council Decision (COM (2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for Regulation of the European Parliament and of the council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final).* Brüssel

Article 29 Data Protection Working Party (2005) *Working document on data protection issues related to RFID technology.* Brüssel

Article 29 Data Protection Working Party (2006) *Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data.* Brüssel

Article 29 Data Protection Working Party (2006) *Working document on data protection and privacy implications in eCall initiative.* Brüssel

Battelle, J. (2005) *The Search – How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture.* London: Nicholas Brealey Publishing

Berg et al. (2004) *Autonomous sensor systems. Communication needs for independent sensors.* Kjeller: Forsvarets forskningsinstitutt

Bolkcom, C. (2005) *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance*, *CRS Report for Congress,* oppdatert 7. februar 2005. Washington: The Library of Congress

Bunyan, T. (2005) While Europe sleeps... *ELCN Essays* (no. 11)

Cabinet Office, eGovernment Unit (2006) *IPSV-Integrated Public Sector Vocabulary, version 2.00.*

Campbell, D. (1999) Interception Capabilities 2000, i: Holdsworth D. (red.) (1999) *Development of surveillance technology and risk of abuse of economic information (An appraisal of technologies for political control)*, Luxembourg: European Parliament, Directorate General for Research, Directorate A, The STOA Programme

Cole, S. A. Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate i: Lazer D. (red.) (2004) *DNA and the Criminal Justice System: The Technology of Justice,* MIT Press, pp. 63-89

Commission of the European Communities (2005) *Proposal for a council decision on the establishment, operation and use of the second generation Schengen information system (SIS II).* Brüssel

Committee on the Judiciary, The United States Senate (2001) *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age. Testimony of James X Dempsey (pp 47-61).* Washington: US Government Printing Office

Council of the European Union (2005) *NOTE from Presidency to Strategic Committee on Immigration, Frontiers and Asylum: Minimum common standards for national identity cards.* Brüssel: DG Justice and Home Affairs

D-G Energy and Transport [accessed: 22.02.2007] *Galileo – Satellite Navigation System.*

Eagle og Pentland (2006) *Eigenbehaviours:* Identifying Structure in Routine, submitted to: *Ubicomp '06*. September 17-21. Orange County. CA

EPIC (2005) *Carnivore page.* http://www.epic.org/privacy/carnivore/

EPIC (2005) Unmanned Planes Offer New Opportunities for Clandestine Government Tracking, *Spotlight on Surveillance* (August 2005).

ESSTRT (2005) *Extract from ESSTRT Deliverable D1-6 "Responses to Terrorist Threats"*

European Commission (2003) *Airline passenger data transfers from the EU to the United States (Passenger Name Record).* Brüssel
http://ec.europa.eu/comm/external_relations/us/intro/pnrmem03_53.htm

European Commission, Information Society and Media (2006) *eCall – saving lives through in-vehicle communication technology.* Brüssel

European Commission, Justice and Home Affairs (2006) *EU – Passport Specification Biometrics Deployment of EU-Passports* Working Document (EN) – 28/06/2006.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2005) *Proposal for a regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between members on short stay-visas.* Brussels

European Parliamentary Technology Assessment Network (2006) *ICT and Privacy in Europe – Experiences from technology assessment of ICT and Privacy in seven different European countries.* Oslo: The Norwegian Board of Technology

FAST Search Best Practices TM (2006) Searching Rich Media, *Search 360* (februar 2006).

Finkenzeller, K. (2003) *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* 2. utgave. München: Carl Hanser Verlag

Gasson et al. (red.)(2005) *D 3.2, A study on PKI and biometrics.* FIDIS consortium

German Federal Office for Information Security (2005) *Common Criteria Protection Profile. Machine Readable Travel Document with „ICAO Application", Basic Access Control* Version 1.0. Bonn: BSI

German Federal Office for Information Security (2005) *Digitale Sicherheitsmerkmale im elektronischen Reisepass.* Bonn: BSI

German Federal Office for Information Security (2005) *Security Aspects and Prospective Applications of RFID Systems.* Bonn: BSI

Hegghammer, T. (2006) *Terrorisme og ny kommunikasjonsteknologi.* Kjeller: The Norwegian Defence Research Establishment

Heinrich, C. (2005) *RFID and beyond. Growing your business through real world awareness.* Indianapolis: Wiley Publishing

Hellevik, O. (1995) *Sosiologisk metode,* Oslo: Universitetsforlaget

Hempel og Töpfer (2004) *CCTV in Europe.* Berlin: Technische Universität Berlin

Henderson, Bruce og Burton (2001) Matching faces of Robbers captured on Video*, Applied Cognitive Psychology* **15**, pp. 445-464,

Hildebrandt og Backhouse (2005) *D 7.2 Descriptive analysis and inventory of profiling practices.* FIDIS consortium

ICAO (2004) Annex 1 Use of Contactless Integrated Circuits In Machine Readable Travel Documents*, Biometrics Deployment of Machine Readable Travel Documents, Technical Report* v.2.0 Version 4.0. International Civil Aviation Organization (ICAO)

ICAO (2004) *Machine Readable Travel Documents Development of a Logical Data Structure – LDS – for Optional Capacity Expansion Technologies*, Version 1.7. International Civil Aviation Organization (ICAO)

ICAO (2006) *ICAO MRTD Report* **Volume 1** (Number 1). Montreal: International Civil Aviation Organization (ICAO)

ICAO TAGMRTD/NTWG (2004): *Biometrics Deployment of Machine Readable Travel Documents, Technical Report* v.2.0. International Civil Aviation Organization (ICAO)

Institute for Prospective Technological Studies (IPTS) (2005) *Biometrics at the Frontiers: Assessing the impact on Society.* European Communities

Jain, Bolle og Pankanti (1999) *Personal Identification in Networked society.* Norwell, Massachusetts: Kluwer Academic Publisher

Kinnegig, T. A. F. (2004): *PKI for Machine Readable Travel Documents offering ICC read-only access* v 1.1. International Civil Aviation Organization (ICAO)

Lyon, Hardenberg (2001) Warum Neugeborene mehr wissen als Grosse manchmahl ahnen, *GEO* (7), s. 27-42, Hamburg

McMunn, Mary K. (2006) Machine Readable Travel Documents with biometric enhancement: The ICAO Standard, *ICAO MRTD Report* **Volume 1 (**Number 1). Montreal: International Civil Aviation Organization (ICAO)

Meints og Hansen (2006) *D 3.6 Study on ID Documents.* FIDIS consortium

Ministry of Foreign Affairs of Denmark (2004) *En verden i forandring - nye trusler, nye svar. Redegørelse fra regeringen om indsatsen mod terrorisme.* Copenhagen: Ministry of Foreign Affairs of Denmark

Naylor og Attwood (2003) *Annotated Digital Video for Intelligent Surveillance and Optimised Retrieval.* The ADVISOR Consortium

Norris, McCahill og Woods (2004) *Editorial. The Growth of CCTV: A global perspective in the international diffusion of video surveillance in publicly accessible space*. Surveillance & Society

The Norwegian Board of Technology (2005): *Elektroniske spor og personvern.* Oslo: The Norwegian Board of Technology

The Norwegian Ministry of Justice and the Police (2005): *NOU 2005:19. Lov om DNA-register til bruk i strafferettspleien.* Oslo: Statens Forvaltningstjeneste Informasjonsforvaltning

The Norwegian Ministry of Justice and the Police (2005): *Ot.prp. nr. 60 (2004-2005): Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet).* Oslo: The Norwegian Ministry of Justice and the Police

The Norwegian Ministery of Local Government and Regional Development (2003): *Rundskriv H19/03*: *Ikrafttredelse av endringer i utlendingsloven og utlendingsforskriften*. Oslo: The Norwegian Ministery of Local Government and Regional Development

OECD Working Party on Information Security and Privacy (2004) *Background material on biometrics and enhanced network systems for the security of international travel*. Paris: OECD

OECD Working Party on Information Security and Privacy (2004) *Biometric-based technologies*. Paris: OECD

Office for Public Management (OPM) (2005) *Research into the use of personal data sets held by public sector bodies*. Final report for Council for Science and Technology (draft). London: OPM

Parliamentary Office for Science and Technology (POST) (2002) *Postnote number 175: CCTV*. London: POST

Ratha, Connell og Bolle (2001) Enhancing security and privacy in biometrics-based authentication systems, *IBM Systems Journal* **Vol 40** (no 3)

Rejman-Greene, M. (red.) (2003): *Biovision Roadmap* issue 1.1. Ipswich: BIOVISION

Rieback et al. (2006) *Is Your Cat Infected with a Computer Virus?* Amsterdam

Rieker, P. og Knutsen, B. O. (2003) *EUs "nye" sikkerhetspolitikk: Bekjempelse av terrorisme og internasjonal kriminalitet*. Oslo: Forsvarets forskningsinstitutt og Norsk utenrikspolitisk institutt

Riksaasen, T. (1993/94) *Telematikknett*. Trondheim: NTNU

Safety Support (2006) *eCall: Saving a life every four hours!*

Sarma, Weis, Engels (2003): RFID Systems and Security and Privacy Implications, i: B.S. Kaliski Jr. et al. (Red.) (2003) *CHES 2002* pp. 454-469. Berlin: Springer-Verlag

Temporary Committee on the ECHELON Interception System *(2001) Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098 (INI))*. Brüssel: European Parliament

Texas A&M Research Foundation *Employee's guide to security responsibilities. Bugs and Other Eavesdropping Devices* http://rf-web.tamu.edu/security/SECGUIDE/Home.htm

Thalheim et al. (2002) Body Check, *c't* (11/2002), pp. 114

The European Union (2006) AGREEMENT between the European Union and the United Stats of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, *Official Journal of the European Union* **Vol 69** (No 131), pp. 41543

The European Union (2006) DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal of the European Union*

The House of Lords (1998) *Fifth report of the House of Lords Science and Technology Select Committee.* London: Science and Technology Committee Publications

UK Home Affairs Committee Publication: *Home Affairs – Fourth Report* 2003-04 (ID Cards)

United States District court for the northern district of California, San Jose division (2006) *Gonzales vs. Google*, *No. CV 06-8006MISC JW.*

United States Government Accountability Office (2005) *DATA MINING Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain.,* Washington: GAO

United States Government Accountability Office (2006) *PERSONAL INFORMATION Agencies and Resellers Vary in Providing Privacy Protections. Statement of Linda D. Koontz, director, before the Subcommittee on Commercial and Administrative Law and the Subcommittee on the constitution, Committee on the Judiciary, House of Representatives*, April 4 2006. Washington: GAO

US Department of Defense (2003): *Total Information Awareness (TIA)* Update February 2003. http://www.defenselink.mil/Releases/Release.aspx?ReleaseID=3625

US Department of Defense (2006): *Dictionary of Military and Associated Terms*, *Joint Publication 1-02*, As amended through 08 August 2006. DoD

Van der Ploeg, I. (2005): *Biometric Identification Technologies: Ethical Implications of the Informization of the Body*, draft March 2005. BITE project

Weitzner et.al (2006): *Transparent Accountable Data Mining. New Strategies for Privacy Protection*. Cambridge, MA: MIT CSAIL

Wilson, D. H. (2005): *How to survive a robot uprising. Tips on defending yourself against the coming rebellion*, London: Bloomsbury Publishing Plc

Wood, D. M. (red.) (2006) *A Report on the Surveillance Society.* Surveillance Studies Network For the Information Commissioner

Wright, S. (1998): *An appraisal of the Technologies of Political Control.* Luxembourg: European Parliament, Directorate General for Research, Directorate B, The STOA Programme

News articles

BBC News (2007) World's tiniest RFID tag unveiled, *BBC News,* February 23rd 2007 http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6389581.stm

European Commission Press Release (2005) *MEMO/05/188, Schengen: from SIS to SIS II.* Brüssel, June 1st 2005

FOX News (2005) FBI Ditches Carnivore Surveillance System. *FOX News* January 8th 2005, http://www.foxnews.com/story/0,2933,144809,00.html

Gadher, D. (2004) Plane passengers shocked by their X-ray scans*, The Sunday Times*, November 7th 2004 http://www.timesonline.co.uk/article/0,,2087-1348172,00.html

Halvorsen, F. (2006) SAS får benytte fingeravtrykk*, Teknisk Ukeblad*, April 29th 2006 http://www.tu.no/nyheter/ikt/article51090.ece

Heise Online (2006) ePass-Hack im niederländischen TV demonstriert, *Heise Online* http://www.heise.de/newsticker/meldung/69127 .

IDABC: FR: Future French eID card to become compulsory, *eGovernment news*, April 14th 2005. http://europa.eu.int/idabc/en/document/4100

IDABC: FR: Future French electronic ID card to include two biometrics, *eGovernment news*, September 3rd 2004 http://ec.europa.eu/idabc/en/document/3249/335

Love, D. (2004): Progressive's Black Box: Is Big Brother Good for the Industry*, Insurance Journal*, December 6th 2004. http://www.insurancejournal.com/magazines/southeast/2004/12/06/features/50322.htm

Marks, P. (2006): Pentagon sets its sights on social networking websites*, New Scientist*, June 2006 http://www.newscientisttech.com/channel/tech/mg19025556.200-pentagon-sets-its-sights-on-social-networking-websites.html

McCullagh, D. (2007): FBI turns to broad new wiretap method, *CNET News*, January 30th 2007, http://news.com.com/FBI+turns+to+broad+new+wiretap+method/2100-7348_3-6154457.html

The Norwegian Data Inspectorate (2007) *Statens Vegvesen holdt tilbake viktig AutoPASS-informasjon.* March 1st 2007

Petrie, E. (2002): Iceland places trust in face scanning*, BBC News*, January 24th 2002 http://news.bbc.co.uk/1/hi/sci/tech/1780150.stm

Reichgott, M. (2005): Chicago Pairing Surveillance Cameras with Gunshot Recognition Systems, *Security Info Watch.com* http://www.securityinfowatch.com/online/CCTV--and--Surveillance/Chicago-Pairing-Surveillance-Cameras-with-Gunshot-Recognition-Systems/4628SIW427

RFID Journal (2003): Hitachi Unveils Smallest RFID Chip *RFID Journal,* http://www.rfidjournal.com/article/view/337/1/

Strande M. (2006) Ingen finger-id på norske flyplasser*, Teknisk Ukeblad,* October 3rd 2006 http://www.tu.no/data/article60056.ece

Sweetman, B. (2005): Mini UAVs – the next small thing? *Jane's International Defence Review*, May 11th 2005

Tendler, S. (2005): "Smart" CCTV could fight terrorist threat in stations*, The Times*, November 15th 2005 http://www.timesonline.co.uk/article/0,,2-1872083,00.html

The Royal Society *Superhuman vision – seeing with terahertz* http://www.royalsoc.ac.uk/exhibit.asp?id=4661&tip=1

The Sunday Times (2006): Word on the street ... They're listening, *The Sunday Times*, November 26th , 2006 http://www.timesonline.co.uk/article/0%2C%2C2087-2471987%2C00.html

Wessel, R. (2006) Airport monitoring system combines RFID with video*, RFID Journal.* September 18th 2006 http://www.rfidjournal.com/article/articleprint/2658/-1/1

Appendix A – Interviews and Interview guide

About the interviews

In the preparation and during the course of the work on this document, experts from innovation centres and opinion-makers have been interviewed. The interviews were conducted in an informal way, based on a previously designed guide. This opens up the possibility that the interviewer may come about information during the interview that was not thought about previously, but that nevertheless invites further discussion.[186]

Because of the informal nature of the interviews, one interviewee could also suggest other experts that may be able to contribute and therefore should be interviewed. The following persons were interviewed as part of this Work package:

Magnar Aukrust
Magnar Aukrust is Deputy Director General at The Norwegian Ministery of Justice and the Police, The Police Department. He works particularly with international police co-operation, biometric passports and national ID card. Mr. Aukrust has been the member of a number of public councils related to the military and the police.

Christophe Birkeland, PhD
Christophe Birkeland, is the Director of NorCERT, part of The Norwegian National Security Authority.

Heidi Mork Lomell, PhD
Heidi Mork Lomell conducts her research at the Department of Criminology, University of Oslo. She has done research on the use of CCTV and on public opinion on CCTV as part of the Urbaneye project, which was supported by the European Commission. Lomell is currently part of the project For whom the bell curves, where she does research on the use of criminal statistics in police work.

Svein Y. Willassen,
Svein Y. Willassen is currently writing his Ph.D thesis on digital evidense at the Norwegian University of Science and Technology. Previous to that he has been a special investigator at the National Computer Crime Center in Norway. Willassen has participated in international work, such as composing the Interpol Computer Crime Manual and producing guidelines for digital evidence analysis in the International Organization on Computer Evidence.

Ove Skåra
Ove Skåra is Chief Information Officer at The Norwegian Data Inspectorate.

Hanne P. Guldbrandsen
Hanne P. Guldbrandsen is a Senior Advisor at The Norwegian Data Inspectorate, Legal department. She is also a member of the *Article 29 Data Protection Working Party*.

---

[186] Hellevik, Ottar (1995): *Sosiologisk metode,* Universitetsforlaget

Isabel Münch
Isabel Münch is Section chief for *IT-Grundschutz* at the German Federal Office for Information Security.

This document will also be presented to and commented by a workshop with European experts to be held in Copenhagen in January 2007.

Interview guide

The interview should start with a brief introduction to PRISE and PASR, and our criteria for relevant security technologies should be introduced.

The interviewee should be informed that all information from the project will be published in an *unrestricted* report.

Background information on the interviewee
In addition to the interviewees name and organisation, interesting information could be:

- What is his or her professional background?
- What area of security technology does he or she work in?
- Is he or she involved in any projects (national or international) that could be relevant for PRISE?
- Is he or she involved in any official committees etc. that could be relevant for PRISE?

Technologies and technological development
These are some keywords to ensure that as much relevant information as possible comes out of the interview. It is, however, essential that interesting subjects brought up by the interviewee is pursued.

1) Within the given technology area, what security technologies exist today that are relevant to the PRISE project?
2) How is the technology/system used in practice (if relevant)?
3) Who uses or will use the technology?
4) Why has it been deployed/researched/planned?
5) How does the interviewee see the future development within his/her field of expertise?
6) In what way can the technology be used to identify individuals or reveal additional information about identified individuals?
    - Is information stored in a database?
    - If so, what information is stored?
    - Who has access to it? Under what circumstances?
    - Is the information exchanged? How?

Final questions
It is important to make sure that there is room for some finishing requests at the end of the interview:

7) Can the interviewee supply us with any documentation that could be relevant to the project?
8) Are there any other experts that we have not contacted that could have information of relevance to the project? International resources are of particular interest.
9) Is it OK if we call back with follow-up questions or if we need to clarify something?