Security and Privacy

Scenarios

Security and Privacy

Scenarios

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

Published: Oslo, June 2007
Cover: Enzo Finger Design AS
Print: ILAS Grafisk
Text: Christine Hafskjold
Illustrations: Åsne Flyen

Electronic version published at: www.teknologiradet.no

Table of contents **page**

Preface

This document is part of the PRISE-project. The aim of the project is to contribute to a secure future for Europe, in line with European citizen's civil rights and preferences, particularily the right to privacy. The project is conducted in co-operation with colleagues in Denmark (Teknologirådet), Germany (Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein) and Austria (Institute for Technology Assesment, ITA).

The Norwegian Board of Technology has been responsible for the development of the scenarios presented in this document, and for the mapping of the different technologies the scenarios build on. The objective is to visualise how the different technologies for surveillance and and security can be used in society, and to stimulate the public debate on this topic.

The Norwegian Board of Technology works with a wide range of projects, and for each project we involve resources that have specific competence on the subject in question. To ensure that the scenarios are credible and realistic, we recruited a group of experts from fields of expertise that are important in relation to security and privacy.The group has had the following members:

- Asle Fossberg, The National Police Computing and Material Service
- Marit Gjerde, The Norwegian Police University College
- Nina Græger, Norwegian Institute of International Affairs
- Thomas Olsen, Norwegian Research Center for Computers and Law
- Ove Skåra, The Norwegian Data Inspectorate

We would also like to thank Jordi Mas, Deputy Director of the Catalan Foundation for Research and Innovation for his contribution. The work has been co-ordinated by Project manager Christine Hafskjold of the Norwegian Board of Technology.

On behalf of the Norwegian Board of Technology, I would like to thank everybody who has contributed.

Tore Tennøe
Director, The Norwegian Board of Technology

Introduction

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 our scenarios we mainly focus on technologies or means (systems, legislation etc.) that are meant 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.

In the scenario text we introduce some facts about the different technologies, to help you understand how they work today and their potential for the future.

What is privacy?

Privacy is generally associated with the protection of the integrity, autonomy and private life of the individual. Basically, it's about people's right to choose how they want to live their life, and what things they want to keep private. Privacy is considered a basic human right, and the first regulation of privacy is article 12 in the Universal Declaration of Human Rights.

What makes the protection of privacy difficult is the fact that privacy is almost always competing against other goods in society, such as mobility, efficiency, security or convenience. For example; even if we know that carrying a mobile phone that is turned on makes it possible to trace where we are, most of us would not dream of leaving the phone at home! And most people prefer having an RFID token in their car, rather than waiting in line to pay with (anonymous) cash when driving onto a toll-road.

Research suggests that many people are not concerned about technologies that infringe their privacy because they feel they have nothing to hide. Experts fear that this will result in a loss in privacy for the society that can be difficult to regain once it is gone. And even the most law-abiding citizen may find himself in a situation where he wouldn't want to be watched or traced.

When it comes to security technologies and surveillance, critics claim that a lot of the measures that are implemented are not suited to combat terror, but only to reassure the public that "something is being done". This is because the measures can be circumvented or because the threat they address is too unlikely to justify the action taken against it. A much used example of this is the banning of anonymous calling cards in many countries. Critics of this ban claim that it only stops ordinary people who would like to be anonymous; the criminals have ways of circumventing it by registering with a fake identity or using stolen mobile phones.

Some of the anti-terror initiatives, in particular in the United States, are very privacy infringing, such as eavesdropping telephone calls, screening electronic communication without a warrant or analysing someone based on data collected from different sources without informing the person in question.

An important privacy principle is that a person should be informed when his or her personal data is stored and processed, and that it is possible to get access to the data and check that it is correct. Personal data should only be collected and stored if it is really necessary and it should be deleted when it is no longer needed for the original purpose.

How do you feel about security technology?

Scenarios to inspire debate

We will now present you with the stories of two people: Carla and Peter. We will follow them in their encounters with different security technologies and means, and share their thoughts and ideas on these issues. In order to make the scenarios general, we have avoided using specific countries, cities or airports as examples. Instead, we have tried to show how different countries – and security authorities – have chosen different approaches to implementing security technology. The scenarios are placed some time into the future, in order to show the use of some security technologies or legislation that are not adopted yet.

We hope that these stories will inspire you to reflect on security and privacy, and how you feel about these two values.

Carla is 62. She has worked as a teacher all her life, but she is now considering early retirement. Everything is getting so technical these days! And the children seem noisier than before. Maybe she is getting old? This week, however, she will not worry about that. It's the beginning of the summer holiday, and she is visiting her son in a neighbouring country.

Carla gets on the underground to go to the central train station. She has "charged" her *Universal ticket* and uses this to pay for her journey by holding it in front of the reader at the bar. The ticket is a plastic card that contains a small chip. The chip keeps track of how many journeys she has left in her card. Carla has chosen a so-called anonymous ticket. She knows this means that the money is lost should she loose her ticket, and its also a bit extra hassle as she has to have the separate card. The regular *universal ticket* is of course embedded into the holder's *mobile unit*. You just have to carry the unit on you or in your purse, and verify with your fingerprint when you pass the bar.

Carla can't help it, she finds using finger-printing to identify herself unpleasant. She notices, of course, that the young today don't seem bothered by it at all, but to her it will always be associated with criminals and arrests. "It's bad enough that you have to give up your fingerprint and show your ID card when you want to travel abroad", she thinks. She definitely does not want to do it more often than she has to!

Biometrics

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 (e.g. computers). The most commonly used biometrics are fingerprints and facial characteristics.

In most cases, the biometric image is stored in the form of a *template*, which is a digital representation of the biometric. The template is created using an algorithm. For privacy reasons, it is recommended to only store the template, and discard the original image. However, in international law-enforcement systems, like biometric passports, and facial recognition systems, the original image is often retained.

We can distinguish between *identification* which is finding out who a person is by comparing his or her sample to all the templates that are stored in a system, and *authentication*, where the sample person is compared to his or her stored template, in order to verify that the person is who he or she claims to be.

The process of comparing the biometric from a person against a previously stored template is called matching. The matching results in a score. If the person is accepted or rejected is then based on whether this score exceeds a given threshold. One challenge with biometric systems is finding the right balance between how often you can accept that the system identifies the wrong person (*False positive*) and how often it fails to accept an enrolled person (*False negative*).

One of the major advantages with biometrics is that they are so strongly linked to a person. Biometric authentication provides better access control, and identity theft becomes a lot more challenging when personal data are linked exclusively to the right person. But this is also the greatest liability of biometric systems. Once a set of biometric data has been compromised (stolen), it is compromised forever.

Peter is 32. He works as a sales representative for a car dealership. This morning he is getting up early to go to a car show in Central Europe. He gets up, takes a quick shower, grabs his bag, gets into his car and heads for the airport. He's late as usual, but as he has registered for the *fast lane*, he should be OK. The fast lane lets you skip all the hassle with check in where passengers are checked against profiles of criminals, passports are checked, and of course there's the rigorous security check. With the fast lane you go through a particularly thorough registration process once – and let the airport store all your data. In return, you can bypass ordinary check in, and just authenticate yourself using biometric technologies at the entrance.

He sends a thought to his colleague who, in Peter's mind, has a fixation on privacy. He claims there is too much surveillance in the society as it is, and now he won't even accept cookies to his computer! He even uninstalled the Google toolbar - nobody does that! If it were true that American agencies use those data to map networks and scan for suspicious profiles, surely that would be common knowledge? Right now he's probably been up a couple of hours, and is already standing in

line for check in and security. Well – he asked for it! Peter just hopes his colleague will get through security in time for them to go over their presentation one last time before boarding.

- o -

Carla arrives at the central station. As in the underground, there are cameras everywhere. Screens and loudspeakers on the walls repeat security warnings till nobody notices them anymore. "– Don't leave your bags unattended." "– Your image will be checked against the database of known terrorists." There was a debate about that last one a few years ago. Many countries don't signpost that they capture images and check against different databases, and it was suggested that they shouldn't have to do it here either. But the government was very clear on the principle that people should know when and where they are being checked. "That's particularly important when you have no way of noticing it yourself. You can't really know anymore if your picture is taken", Carla reflects. She has heard that there are countries where they also screen people's e-mails and phone conversations for words and phrases that are suspicious – but surely that must only be rumours!.

Carla feels her head spin with all the noise and heads for the *silent zone*. She has to show her ID to get in, but once inside, she relaxes. "No cameras, no mobile phones, no wireless zone, no noisy warnings! There really should be more such technology-free zones", she thinks.

It's not that she's not used to the cameras. After all, they've been around for most of her adult life, but don't they seem more intrusive lately? After they started using both facial and pattern recognition software she seems to feel more observed and evaluated than before: "Am I making a terrorist-like movement now?" Imagine how embarrassing it would be to do something that might cause her to be stopped and checked by the anti-terror police! To be fair, she has never actually been stopped, but she can't help thinking about it when there are cameras around.

And, like most people, she knows someone that has actually been suspected of being a terrorist. When the technology was in its early phase there were a lot of problems with the facial recognition software. And because the politicians didn't want the scandal of someone on

Closed Circuit Television (CCTV)

CCTV surveillance with *active cameras* is when an operator watches the monitor and can control the camera (turn, zoom) to follow an individual or a situation that develops. 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 in a database.

Passive cameras: These 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.

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, but it is a concern that such images also can be manipulated more easily.

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 authentication. 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 therefore normally used to verify that a person is not on a list of for instance known criminals or terrorists.

the watch list actually fooling the system, the result was a lot of so called *false positives*.

A colleague of hers, whose parents are from Iran, got mistaken for a terrorist. He found it very humiliating, and she doesn't blame him. Like he said: "When you have been arrested by anti-terror police dressed in bullet-proof vests and you look like me, people look at you differently afterwards – even if you are let off with an apology". Carla knows that he stayed away from the most camera-dense areas for a while after that, especially when he had his children with him.

Lately more and more people have been questioning both the legitimacy and efficiency of the cameras. In some areas of the city they are now starting tests where instead of surveillance cameras they install better and brighter street lights. Apparently with good results!

- o -

Working at a car dealership, Peter always has the latest model car. The one he is driving right now has all the newest technology: Galileo satellite connection with navigation system, automatic emergency call through the eCall-system and a bunch of other Vehicle Safety Systems. Peter isn't even sure what all of them do. The eCall system is now standard in all new cars, and it is supposed to call the emergency number automatically if the car is in an accident. Because it is connected to the Galileo system, it has the exact position of the car.

Locating technology

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

For more accurate positioning, satellite based systems are used:

GPS is short for *Global Positioning System*, a worldwide satellite navigational system formed by 24 satellites orbiting 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.

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 2012. It will be more accurate than the GPS system, and it will have greater penetration.

Over the last years there have been suggestions to use the technology for other purposes as well. After an attempted terrorist attack in Berlin, the terrorists stole a car and fled through Germany. It then turned out that the system could also be used to track the car, and even stop it! The car was an expensive model with the latest in anti-theft technology, and it could actually be stopped remotely via satellite. The terrorists were stopped and arrested, and after this the EU member states agreed that the systems could also be used by the police for tracking criminals and suspected terrorists.

After a research report on how many lives could be saved in traffic if the speed limits were respected by motorists, it was suggested that the Vehicle Security Systems should integrate a module that could check the speed limit on a given stretch of road and match it against the speedometer. The original suggestion was that a chip in the engine should make sure that no car could drive above the speed limit, but this was met with heavy

eCall

The eCall device contains sensors that are activated after an accident. It calls the emergency number and communicates information about the accident, including the time, precise location, direction and identification of the car.

The device will not be permanently connected to a mobile communications network, it will only connect after it has been triggered. There is however concern that this could change, about the transmitting of additional data (for instance for insurance companies), and about possible unauthorised access to databases where eCall data is stored. From September 2009, all new cars in the participating countries will be equipped with eCall.

protesting, both from the car industry and the car-owners associations. At the moment, the system is set up so that every time a car drives above the speed limit, a call is made to the central fine registry, and the fine is automatically deducted from the car owner's bank account.

Peter pushes the accelerator. All road stretches have still not been updated in the system, and he has downloaded an overview of which it is to his navigation system. He gets an alert every time he passes a sign that is hooked up to the system – meaning that he "has to" keep within the speed limit. "It's good that surveillance can work the other way as well", he thinks.

Automatic Number Plate Recognition (ANPR)
ANPR systems read number plates picked up by CCTV and match them against a database. Systems for number plate recognition are in use in several countries. They are mostly related to toll booth passing or speed cameras, but they are also used to identify stolen vehicles.

Peter arrives at the airport. The licence plate of his car is already in the system, and his car is registered automatically as he drives into the car park. It's the same technology that is being used in the cities to identify stolen vehicles. He actually thought such a system would be superfluous after the eCall connected to Galileo was implemented, but apparently the more organised gangs know how to disable the system. And he knows that some countries even demand that the driver should be able to disable the eCall-system himself. Those kinds of requirements always make it more difficult for the car industry! And why is it that the criminals always seem to be one step ahead of the technology?

He parks the car, gets out and heads for the terminal and the fast lane check-in entrance. He places his finger on the sensor and looks straight into the camera. A green light flashes and the door opens.

Even if the sensors are a lot better than they used to be, some people still have trouble using fingerprinting: His grandfather, for instance. Even though he is a very fit 80-year old, he is getting more isolated. You have to use your fingerprint with the ID everywhere these days, and he's uncomfortable with all the hassle that you have to go through when the sensor can't read your prints. So he stays at home mostly.

Peter sometimes goes to the library to borrow *real* books for him. It amuses him to think of what his library profile must look like. If it's ever analysed in search of suspicious individuals, the intelligence service might wonder why a man in his thirties borrows books like "Dating for seniors" and "Our friends the birds".

A few years ago, after a major terrorist attack was prevented in the US, it was actually suggested that security agencies should be allowed to search all possible databases. And that was not only for suspected criminals or terrorist. They wanted to analyse all material in library databases, electricity and gas consumption patterns, traffic data for telephone and internet, travel data and shopping habits.

Function creep
Database systems are 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 when the Norwegian data base of asylum seekers – which also contains biometric information like fingerprints – was opened to the police in criminal investigations. The original intention of the data base was to help establish the identity of asylum-seekers.

By searching for suspicious patterns, they wanted to identify possible terrorists.

His colleague, Alex, had been outraged, and Peter had tried to argue with him: Surely they wouldn't be asking for this unless they had good reasons? Surely the authorities should do whatever they could to catch terrorists? Alex was not convinced, and had argued that at least they could do the analysis on anonymous data: "If they find something suspicious, they can get a court order to have the identity revealed. There's no legitimate reason why they should know everything about everybody!"

Peter hadn't really been much interested in debating the subject further, but his colleague had been on and on about it in every lunch break, and in the end he had signed a petition against the proposal. "But I don't really see the point", he said. "Surely this is only a problem for those with something to hide?" On the other hand, he caught himself wondering if it's been registered somewhere that he signed that petition...

Total Information Awareness (TIA)

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

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, but many of the programs within the system live on under different names.

Carla sits in the silent zone, reading her book for a while, and then heads for the security gate.

The security gate at the international train terminal came as a result of increased demand for control, not only in airports, but also other places where many people are congregated. She knows that in some countries there are even security checks at the entrances of shopping malls and sports arenas. A bomber was caught at a shopping mall near where her son lives a couple of years ago. Apparently they had just started using scanning equipment at the entrance, and the bomber didn't know. Even so, she is glad that it hasn't gone that far in her country. So far, only air and train terminals have security with passenger scanning.

She's not too worried about shopping malls herself – after all there haven't been any threats to her country as far as she knows. But she's seen statistics showing that more people are going back to shopping in the smaller shops in the town and city centres, and that the malls are claiming that they are loosing revenue because they aren't allowed to put up scanning equipment like *naked machines*.

Carla takes out her passport and walks up to the iris scanner. She knows that some countries still use fingerprints in their IDs and passports, but she feels that using iris is more secure. The reader compares her iris to the template stored in her passport. She used to be worried about that, but her son, who works in the IT industry, has assured her that it is completely safe now. "The original encryption in the first passport was quite weak", he said, "but with the encryption used now, a supercomputer would have to use thousands of years to break the encryption! And also; in the early passports, they stored the actual image of the face and fingerprints or iris. Now they only store a *template* – a digital

representation of the most important feature of the iris and face. Even if somebody should break the encryption, they would not be able to recreate the face or the iris to impersonate the passport holder."

She has also been reassured that the reader only stores her iris template long enough to compare it to the one on her card, and that it is not stored in a central database. She is not so sure what happens when her passport is checked at another border. Are the data deleted after the matching there as well?

She remembers there was a scandal a few years ago with a central fingerprint database – was it in the US? A lot of fingerprints were stolen by an employee and sold to international criminals. Thousands of people had their identity stolen and experienced all sorts of problems – from being "black listed" at borders to having their bank accounts emptied. It was particularly difficult because it took such a long time before the government actually would admit to loosing the data. And in the mean time nobody would believe that their identities were stolen – or indeed that it was possible to use somebody's fingerprints to steal their identity!

Carla knows better, though. Last summer a friend of her son's got his ID stolen, just before he and his family were going on vacation. He was afraid they would have to cancel everything because he would be

Radio Frequency Identification (RFID)
RFID is a concept for automatic identification using radio waves. Tiny integrated circuits (tags) containing information are attached to documents or integrated in products. A *reader* can be used to read the information on the tags within range.

RFID tags come as both *active* and *passive* chips. Active tags - like tokens for toll booth passing - contain a battery and will therefore be bigger than passive tags, but they can contain more information and work over longer distances. Passive tags do not contain a battery, but get their energy from the radio signal from the reader. A typical application of passive tags is the new European passport.

Most tags will communicate with any reader, but there are also tags that require the reader to provide a password or some other credential.

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

The chip contains mandatory and optional data In addition there is a photograph of the user as a visual link between the holder and the passport.

The International Civil Aviation Organization (ICAO) has chosen to use a chip that can be read at a distance (like an RFID tag). ICAO has chosen *face* as the primary biometric to be used in passports. *Finger* and *iris* are recommended as secondary biometrics. The EU has chosen to use only finger as the secondary biometric.

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).

To address these concerns a scheme for "basic access control" (BAC) has been developed. Under BAC the inspection system uses a "key" derived from numeric data elements in the Machine readable zone (the barcode) to "unlock" the chip so that the system can read it. BAC has been criticised for not being secure enough, and security experts have managed to break the encryption in only a short amount of time.

"black listed", but apparently the Schengen information system that is used in many European countries registers people who have had their identity stolen. Because of this, he and his family could travel as planned, and he was never accused of being a criminal or a terrorist, although his ID was probably checked more thoroughly than the average traveller's.

After the ID check, Carla has to send her luggage through the scanner, before going through what used to be referred to as the *naked machine*. She is relieved that the actual naked machine never was bought for the airports and international train terminals in her homeland. The security authorities evaluated different machines, but decided that it was just as secure to have the kind of machine where items hidden under the clothing is projected onto a neutral image of a person.

Even at 62, Carla is self-conscious about her body, and she is glad the young men at the security gate does not get to see her naked. She needs to remove her shoes, but apart from that she experiences no problems and is soon seated comfortably on the train.

- o -

Peter crosses the airport hall over to Security. Of course – even the fast lane customers have to pass through some form of security, but they have their own gate, and they are all professional at this. No-one in *this* lane is wearing metal belt buckles, or is amateurish enough to leave loose change in their pockets. And it's been years since shoes made for the business segment contained metal. He sucks in his stomach and passes through the *naked machine*. "Why do they always have to keep such a low temperature in this room?" he thinks, and blushes as he notices that one of the security guards is a woman roughly his own age. Even so, he is pleased that the airport uses the *real* naked machine. It just feels safer, somehow.

Peter notices an addition to the security that he hasn't seen before. After the naked machine there's a second "gate" that some of the passengers are asked to

go through. He vaguely remembers hearing something about a new security feature being tested at this airport. It supposedly registers features like body heat, sweat, heart rate... Stuff that can be a sign of diseases like SARS or Avian flu, or indicate that a person is nervous. Some of the test subjects are escorted into inter view rooms nearby. He's glad he wasn't singled out for the test, even if he is healthy and has a clear conscience. "But to put it up in the *fast lane*? Don't they know the people who use that are busy?"

He heads to the gate and takes a seat. Maybe he should call Yasmin and let her know that he is coming? She works for the car manufacturer his dealership represents, and he met her at the last car show he attended. They hit it off right away, and he would really like to see her again. On the other hand he's reluctant to call her on his mobile. He knows that Yasmin's brother is very active in a youth group in his Mosque, and that Yasmin probably is on some kind of watch list as part of her brother's "network". He wishes he'd bought some anonymous calling cards the last time he was in Asia. It's no longer legal to sell such cards in Europe.

He doesn't want to use an internet service either. Who knows what the airport networks keeps logs of? He's not even sure how the rules are these days. Does the

Passenger scanning (*Naked machines*)
Technologies such as *backscatter X-rays or Terahertz radiation* has better penetration in materials than optics. This means that it can be used for detection and imaging of items concealed by clothing.

A "naked machine" utilises this type of technology 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. This type of airport security has been tested at Heathrow (Terminal 4) since 2004. Other applications take the images of concealed objects and project them onto a sexless mannequin.

police have direct access to these kinds of data, or do they need a warrant? He suddenly wishes that he'd paid better attention in the privacy debate. He'll definitely ask his colleague when he gets on the plane.

The last time he had dinner with Yasmin she mentioned that she was sure that her e-mail was being scanned, and she asked him to use an encryption program if he wanted to write to her. "An un-encrypted e-mail is like a postcard", she explained. "Anyone who gets access to it can read it – didn't you know that?"

He actually thought that he would write to her, but he discovered that the mail program they use at work does not have built-in encryption, and he never got around to installing another one. He hopes she is not mad at him for ignoring her all this time. "I'll explain it when we meet", he thinks.

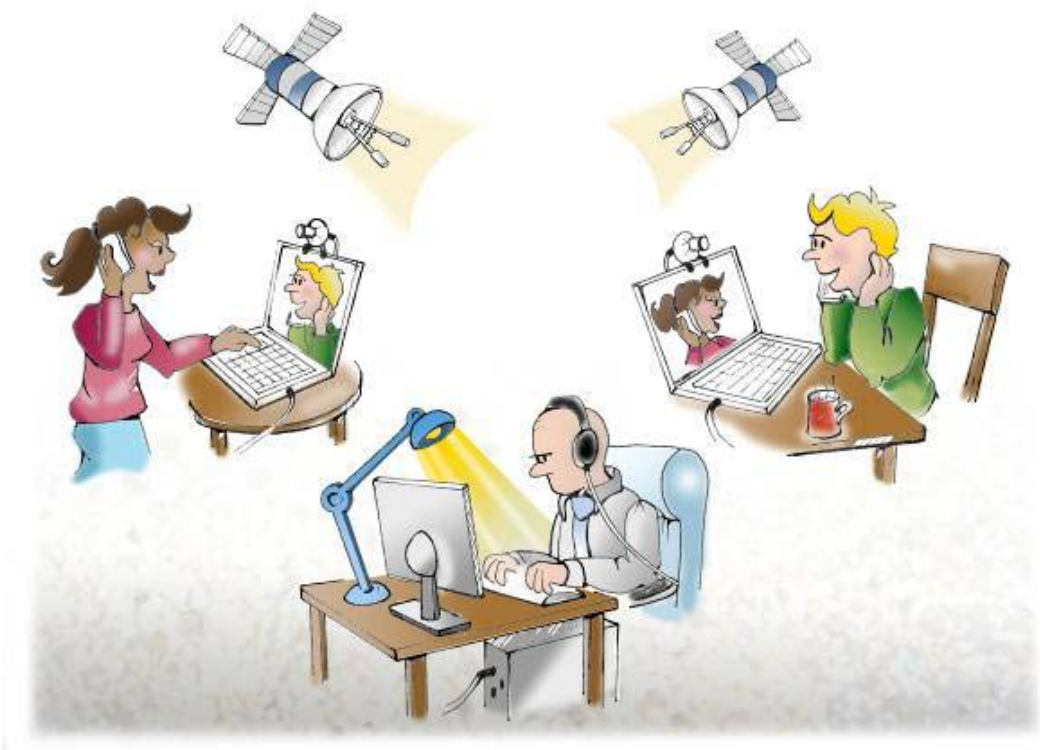
It's time to board the plane. He approaches the gate, places his finger on the

Data retention

A database is defined as an organised collection of data. 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.

Lately, we have seen a trend where governments have wanted to use database systems for purposes that are different from the original purpose, like security. The types of data most commonly referred to when data retention is discussed, is data related to ICT, such as communication data from phone, mobile phone and Internet traffic.

The EU has passed a directive on the retention of such data Data related to *who* is communicating, *where* and *when* will be stored, but not the content. The data can be stored for up to 2 years.



sensor and boards as one of the first passengers. There is still plenty of room for hand luggage. He sends a thought to his colleague who is probably still standing in line for the security check, before he leans back and closes his eyes.

- o -

"Mom's on her way," Carla's son says to his wife after having received a message on his mobile. "She should be here in three hours time". His mother doesn't know it, but the new mobile unit she got for Christmas is connected to a service called *Kid-watch*. The technology is a new version of the trackers you could see in old spy-movies, where surveillers could see their suspects as little dots on a map. The main difference is that by using the built in Galileo technology in the mobile unit, he can follow his mom's movements on a map even when he's sitting in his own living-room in another country.

He tries not to look at it much though – it feels a bit too much like prying into her private life, but he has put in some triggers that will sound alarms if she is immobile for a long time inside her house, or if she is not home at night. After all, she is getting older, and he can't look after her the way he feels he should when he's living in another country.

His phone rings: "Hi, it's mom. I'm on my way now – should be at the station in about three hours"...

Eavesdropping
Different applications can be used 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 suspect's telephone or on the telephones of persons he or she is expected to contact.

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. An example of this is the Echelon network, which is run by an alliance between the USA, UK, Canada, Australia and New Zealand. The system was initially set up to monitor communication in or to the Soviet Union and Eastern Europe. Patterns of communication can be analysed, and content can be scanned for interesting keywords.

Privacy enhancing technologies
Technologies that contribute directly to preserve privacy are known as Privacy enhancing technologies (PETs).

Anonymisation is one such PET. There are services that can enable anonymous electronic communication for regular users. Such technology hides the connection between the user and the traces he or she leaves behind, and can therefore prevent unwanted identification. Traditional cash payment and unregistered (anonymous) calling cards are means that provide for anonymity.

Identity management is also a form of PET: In some cases you don't want to identify yourself, but use a pseudonym (for instance in forums on the internet). In order to make it more difficult to match data, it can be a good idea to have different user names (which do not reveal your identity) and passwords for different purposes. Identity management systems assist people in keeping track of their different user names. In some cases, the service in question may only need to verify a specific attribute – like age or credit limit. In such cases the *identity provider* (e.g. your bank, telecom provider or employer) can act as a trusted third party and guarantee that attribute, without revealing your identity.

Encryption is about distorting content to make it unreadable to others. Because all electronic communication is vulnerable to eavesdropping or manipulation, it is in many cases crucial that the communication is taking place on encrypted lines, or that the content being transmitted is encrypted.