Surveillance, privacy and security

WHAT IS YOUR OPINION?

surprise
surveillance
privacy
security

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Contents

1 Welcome to SurPRISE

Welcome to SurPRISE: a Europe-wide research project. SurPRISE is a shortened version of 'Surveillance, Privacy and Security'. Its aim is to collect citizens' views on new security technologies. Many of these technologies relate to the surveillance of people and what they are doing. They are used by police or security personnel to monitor what is going on, to detect and avoid security problems. When you go to the airport and your baggage is checked by scanning machines, or when a closed-circuit television (CCTV) camera records activity on a street you are walking along, you are encountering surveillance-based security technologies. The aim of SurPRISE is to ensure that these technologies are effective, safe and respect human rights. To achieve this goal, SurPRISE needs your help.

We have invited you to take part in the SurPRISE Project because the European Commission wants to ask citizens what they think should be done to ensure that they are safe and feel secure. When you attend the SurPRISE citizen meeting, you can share your views on new security technologies with fellow citizens.

SurPRISE gathers citizens' views on new security technologies in nine European countries: in Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and in the UK.

This booklet provides basic information on the issues that will be discussed at the …….. (*INCLUDE THE NAME OF YOUR COUNTRY)* SurPRISE citizen meeting in ……. *(INCLUDE THE MONTH OF THE SMALL SCALE EVENT)* 2014. It provides information about the new security technologies that the SurPRISE project is studying. It also provides background information about surveillance, security and privacy in Europe.

Your participation in the citizen meeting is important exactly because you are not an expert. We have asked you to take part because you are an ordinary citizen whose everyday life is affected by the decisions made by European politicians and those in your own country.

Politicians determine security policy, but you as a citizen will have to live with the consequences of those decisions. This makes your opinion important.

Science informs us. It does not tell us what to do. The choice is ours. Have your say!

2 Summary

Plenty of people could not imagine life without their smartphones, debit cards or the internet. What they may not have thought about is that these technologies generate different kinds of electronic records. These records can indicate where we are in space and time, and sometimes can indicate what we are doing. For example, bank transactions, including those made on a debit card, can indicate the types of purchase we make and with whom we associate. This information is held in bank databases and we can see it on our bank statements.

Travel booking information held by airlines can indicate whether we are travelling to or from a risky part of the world. Mobile phone data indicates our location, to whom we talk and how often we do so. This information is held by mobile phone and internet service providers in their databases. European regulations mandate that this information be stored from between six months to two years. This makes it possible to identify, track and trace most people at different points in their lives.

Technologies, like the ones discussed above and the information they collect, can offer benefits to us and to others, too. Following high-profile terrorist attacks within Europe and elsewhere, governments have invested in advanced security technologies that use this kind of information. They have also amended existing laws and passed new ones to allow access to this information for security purposes. Although there are many 'official' intelligence sources, governments have realised that the activities of likely criminals and terrorists might be detectable in other ways. Like the majority of citizens, criminals and terrorists have bank accounts, possess national identity documents, use the internet and have mobile phones. They also use transport systems, public spaces and consume goods and services. Perhaps knowing more about these activities would hold the clue to finding criminals and terrorists. Many governments believe that by using new security technologies, not only will it be possible to arrest wrongdoers, it will also be possible to identify them before they cause harm. Because these technologies use information in this way, the SurPRISE project refers to them as 'surveillance-oriented security technologies'.

A surveillance-oriented security technology is:

a technology, which uses information gathered in different contexts about the general population and their activities to tackle a security problem.

These technologies analyse the information generated by citizens during their daily lives. They use information from, for example, mobile phones, the internet, and from 'smart' technologies like digitally-enabled CCTV to try to identify criminals and terrorists, sometimes before they do wrong.

In this information material, we will be examining five-of these technologies in depth:

- Smart CCTV: CCTV systems that go beyond simple monitoring of public spaces. Smart CCTV features digital cameras, which are linked together in a system that can recognise people's faces, analyse their behaviour and detect objects.
- 'Civil' drones: Civil drones are unmanned air vehicles (UAVs) for non-military use. They can be used for a broad range of surveillance activities. A drone can be equipped with a camera and additional sensor technologies, and they can be seen as mobile versions of CCTV cameras.
- Cyber surveillance using deep packet inspection: Using hardware devices and special software, all messages and information transmitted over the internet can be read, analysed and changed.
- Smartphone location tracking: By analysing location data from a mobile phone, information can be gleaned about the location and movements of the phone user over a period of time. A phone's location can be indicated using data from the mobile phone masts to which it has connected, and more exactly by global positioning systems (GPS) or wireless data.
- Biometrics: Biometrics refers to automated methods of recognizing individuals based on measurement of their physical or behavioural characteristics. The most common use of bio-

metrics is the biometric passport based on facial, fingerprint and/or iris recognition.

Each technology can improve security by identifying suspects and criminal or illegal activities. Some believe that they can also make life much more convenient. But each security technology has a set of drawbacks. For example, smart CCTV, or civil drones equipped with a camera, works only in certain conditions and can produce a lot of 'false alarms'. Deep packet inspection compromises the privacy of online communications. Smartphone location tracking is difficult to control because many apps transmit location information from the phone without the knowledge of the user. Data leaking from biometric databases might result in identity theft. A lack of control over the collection and use of information is an issue associated with all the technologies we examine.

The use of these technologies raises issues about human rights, privacy, regulation and trust. These technologies usually collect and share information about a person without their knowledge. Data about innocent people is inevitably captured and analysed, and in the case of some technologies, deliberately so. As such, they have the potential to invade privacy, which is a fundamental human right, protected in Europe. They can also lead to innocent people being mistakenly identified as harm-doers, with serious consequences for their lives.

In spite of the potential security improvements these technologies offer, some citizens are unsure how they feel if their information is used for security purposes. If everyone is more secure as a result, perhaps it is OK. However, if fundamental human rights are infringed, perhaps it can never be OK. People's opinions might also differ depending on what they believe about a number of other issues, for example:

- Do these technologies really improve security?
- How intrusive are they?
- Is there enough effective legal regulation?
- Are the technologies used in ways that comply with the law?
- Are the institutions using them trustworthy?
- How well regulated are the institutions that use the data?
- Are the institutions transparent and accountable for any privacy infringements committed in the name of security?
- Who watches the watchers?
- What are the alternatives and are they practical?

These are some of the questions we will be discussing during the citizen meeting.

Science education, consumer education and especially public controversies over science and technology surely contribute to a citizens' ability to take part in the debates and to exercise their democratic rights.

In the next few paragraphs, we will introduce some of the key terms and definitions before describing the five selected technologies we explain in more detail.

Please read on to know more about these issues.

3 Surveillance, privacy and security

3.1 Surveillance

When we think of 'surveillance', there are probably a few images that immediately come to mind: you may think about 'Big Brother' – both the reality television series and the character in George Orwell's novel, *1984*. As a result, you may associate surveillance with a creepy feeling of being watched by a powerful but unknown organisation or person.

When we refer to 'surveillance' in SurPRISE, we think of it as 'monitoring people in order to regulate or govern their behaviour' and it can be undertaken for different purposes. Surveillance might be done for security purposes. For example, the police might use CCTV or drones equipped with CCTV cameras to spot or to follow wrongdoers. Surveillance might also be employed for commercial purposes. For example, a search engine provider might analyse surfing behaviour using internet surveillance methods in order to improve its search machine. Surveillance can be used to prevent crime and catch criminals, but it is also used to provide people with products and services.

If surveillance is a normal part of society then you might well be wondering what is wrong with it. Reports in the news relating to 'the surveillance society' always seem to have a sinister edge to them. The point is that controlling a surveillance technology bestows great power. It is important that those who are in such positions, such as law enforcement agencies, data brokers or retailers, wield that power fairly and with due respect to civil liberties and the law.

Whether you think you have nothing to hide or nothing to fear really depends on who is doing the watching, why they are watching you, and how they perceive your actions. If you have no control or say in that process and the rules suddenly change against you – be that because of your ethnicity, religion, sexual orientation, gender or political views – what would you do? This is why excessive surveillance can have a negative impact on other human rights such as freedom of expression. In these circumstances, surveillance can also damage levels of social trust, as people are afraid to be themselves. A lot hangs in the balance when different forms of surveillance data are used in the context of security.

3.2 Privacy and data protection: important issues?

One of the main issues is privacy and how the data that new security technologies generate and use is made secure. Although privacy can mean different things to different people, it is an important part of everyday life. There are a number of things that you might want to keep private at different times:

- what you are doing, thinking and feeling
- information about your intimate relationships, where you are, what you communicate to others either by post or email, your personal characteristics and your image
- your body: how much of it you reveal, whether you can keep it free from unwanted touch or body searches, and your control over others' access to your bodily materials such as your DNA or your fingerprints

Just think about it: would you be happy if a life insurance company had unlimited access to your medical records? Or if the police could listen to all your phone calls? Do you have curtains in your house? If your answer to the first two questions is 'no' and to the third, 'yes', then you are still concerned about privacy! You are not alone. Studies of young people using social media showed that they disclosed only very selective information about themselves due to privacy concerns. People still want to share information, but want to do so within established boundaries. For the individual, anything beyond these boundaries represents the areas of their life that they wish to keep free from outside interference: their private life.

In SurPRISE, we define privacy as:

the ability of an individual to be left alone, out of public view, and in control of information about oneself.

The right to privacy and the right to protection of personal data are fundamental rights in the European Union. Everyone needs a right to privacy: to be free to act, meet and discuss in a democratic society. People cannot exercise democratic freedoms if everything is known about their thoughts, intentions and actions.

New European data protection laws are going to insist that privacy be 'designed into' new technologies, so that they are less privacy invasive from the start. The businesses that make new technologies are going to be encouraged to consider privacy every step of the way. This new approach is called 'privacy by design'.

3.3 Security

On the SurPRISE project, we define security as:

the condition of being protected from or not exposed to danger; a feeling of safety or freedom from or absence of danger.

Security not only refers to the protection of physical things, such as buildings, information systems, national borders and so on, it also refers to human feelings of safety. In an ideal world, effective security measures would result in increased feelings of safety but this is not always the case.

It seems odd that because new security technologies have the potential to compromise privacy, they could end up making us feel *less*, rather than *more* secure. But, this might not be the same for everyone. As with privacy, security means very different things to different people. We each have our own perceptions about what we consider a security threat and what we would be prepared to do to protect the things that are important to us.

This is also true for those who govern security. They need to identify and deal with the most important threats. Any government will have limited economic, human and technical resources to devote to security, and so choices need to be made. For the European Union, the main security priorities are to:

- increase cyber security for citizens and businesses in the EU
- disrupt international crime networks
- prevent terrorism
- increase Europe's ability to recover from all kinds of crisis or disaster

Because Europe has decided to focus on recovery from all kinds of crisis or disaster, security now goes beyond the prevention of crime and terror. Europe is also concerned with threats to the environment, natural resources, infrastructures, economic activity and health. For policymakers, security has expanded into nearly all areas of public life. This approach has been adopted by many European states. But can the promise of security in all these areas ever be delivered? The security industry is now a major industry being developed in Europe to address this need. It features large defence companies and also lot of smaller companies. Recent developments in surveillance-oriented security technologies include:

- smart CCTV, which focuses on spotting known offenders and identifying suspicious behaviour
- cyber surveillance, which seeks to prevent damage being caused by viruses, hackers or identity thieves
- biometrics, which are deployed to prevent unwanted individuals entering a territory and to expedite the passage of those who are known to government as 'trusted travellers'
- aerial surveillance drones, which can spot dangerous activities from the air that could not be seen from the ground. This information can be used to direct security personnel to emerging trouble spots
- advanced passenger information systems, which seek to detect individuals before they travel, who could pose a threat
- location-tracking technologies, which seek to minimise harm to things on the move and to pinpoint suspects in physical space

4 Five security technologies

The five security technologies that the SurPRISE project is examining are:

- Smart CCTV
- Drones
- Cyber surveillance by deep packet inspection
- (Smart-) phone location tracking
- Biometrics

These security technologies are still being developed and policy about them can still be determined.

In the following sections in this booklet, we describe how each technology works, why it was developed, who uses it and how it is used. We also describe the security improvements they offer, and the privacy and other issues involved in the security technology's use.

It is important for this project, and the European Union, to understand what people think about security technologies and how acceptable they find them. This is why your opinion matters so much. You may already be strongly for or against some of these technologies. During the SurPRISE meeting, you will be given many opportunities to voice your opinion, but we would particularly like you to think about the following questions:

What makes a new security technology more or less acceptable to you?

Could it be:

- Knowing more about the technology and how it works?
- Knowing more about how different institutions are using the technology and the information it produces?
- Having effective legal regulation and control mechanisms?
- Being better informed about the kinds of threat we currently face, against which this technology is deployed?

Or maybe it depends on how intrusive you think the technology is. For example:

- Does it cause any embarrassment?
- Does it infringe fundamental rights?
- Does it disclose information to third parties without your knowledge, or impact on other aspects of your privacy?

Maybe it depends on how effective the technology is:

- Does it make life more convenient?
- Does it make you feel safer?
- Does it accurately identify suspects?

Or perhaps you only think about security technologies when you are aware that they are physically near you. This could be in an airport, when you are in the street, or when you use a mobile phone or the internet. The rest of the time it does not bother you. Perhaps you are OK with security technology now, but are concerned about its use in the future.

5 Smart CCTV

A 'traditional' CCTV system features cameras mounted on street furniture in public spaces or shops. The cameras are connected to a control room via telecommunications. In the control room, banks of television screens show trained operators the pictures captured by the cameras. The images are recorded, stored, and after a period of time are deleted. The system is 'closed' as the pictures are not broadcast anywhere other than to the control room. If operators see anything suspicious, they can contact security guards or police by phone or radio so that they can then intervene.

5.1 Why smart CCTV was developed

CCTV was originally developed to observe missile launches in the Second World War and to manage hazardous industrial processes at a distance. It was first sold as a security technology in the USA in the 1950s. Police started to use it from the 1960s. In 2013, CCTV systems in Boston were crucial in identifying those responsible for the Boston Marathon bombing.

The smart variant of CCTV has been designed to address the long-standing problem that CCTV has faced from the beginning. This is the fact that there are too many cameras and too few pairs of eyes to keep track of what is going on. In contrast to a 'traditional' CCTV system, a smart CCTV system uses networked digital cameras linked to systems that can analyse the digital images. Software analyses what is going on in the image. If it is something unusual, an alarm sounds and the CCTV operator's attention is drawn to the image. A record is also kept of the alarm. Images related to that alarm are then stored on a computer and can be retrieved and shared easily.

Smart CCTV software can do a number of things. It is most frequently used to:

- identify objects in an image, such as a vehicle, by reading its registration plate and comparing it with information in a database
- identify a person's face when the face appears against a plain, uncluttered background. To identify the person, that picture is compared with images held in a database of known individuals
- identify an unattended bag but only if that bag is left in an empty space

Although smart CCTV cannot currently do the following things reliably, software is being developed which:

- identifies people in a crowd by tracking their clothing
- identifies suspicious behaviour, or behaviour that is unusual in the scene being observed, such as loitering. Behaviours in the images are compared with known patterns of behaviour stored in a database.

However, not all smart CCTV systems are the same. How 'smart' a system is depends on how well its software analyses the image and what happens to the image once it has been shared. Systems are installed for different purposes, so a smart CCTV system might not be able to do all the things discussed above. The owner of a system might not need it to do some of those things.

5.2 How smart CCTV is used

Smart CCTV systems are commercial products sold by security and defence technology companies. Numerous systems are available already. Currently, transport authorities, such as highway, airport, port or rail authorities, local authorities and police are the main institutional users of smart CCTV.

For example, in Budapest at the end of 2012, the police started to use smart CCTV cameras to observe bus lanes. The police can lawfully use the images to punish those who drive in designated bus lanes.

The European Union has funded 16 separate projects to develop the algorithms and functions of smart CCTV systems. Currently, more complex uses, such as recognising suspicious behaviours or faces in crowds are still being developed and improved. Their use is not widespread, and new systems are being tested all the time. For example, transport authorities in Rome, London, Paris, Brussels, Milan and Prague have recently participated in trials of an intelligent pedestrian surveillance system that uses smart CCTV. This system alerts operators to suspicious packages, abnormal movements by passengers and unusual behaviour. It is not in operational use as it is still being tested at the time of writing.

Perhaps the most widespread use of smart CCTV is for automatic number plate recognition. With a digital image of a car number plate, information can be compared with government car owner databases, insurance databases and police databases. The owner of the car and the car's registered address can be easily identified, and the ANPR camera can pinpoint a specific individual in time and space. The system can be used to identify stolen vehicles, vehicles that are being driven without tax or insurance, or vehicles that are speeding.

One question is whether these different types of crime or misconduct warrant the same level of surveillance. Should smart CCTV be used for all types of misdemeanours or just saved for the most dangerous of criminal offences? There are varying views on this matter throughout Europe. In Germany, for example, in 2008 the constitutional court restricted ANPR use in police work on privacy grounds. The court insisted that police forces were only to retain digital data gathered by ANPR cameras if immediate database checks were done and acted upon. ANPR is also used to enforce road tolls, but once again this attracted criticism, as other, less surveillance-oriented means were available to enforce the tolls.

How smart CCTV works

Using 'intelligent algorithms', a computer linked to a smart CCTV system learns to recognise specific types of public behaviour. These are known as 'trigger events', e.g. a person holding a gun or standing still in a moving crowd. An algorithm is a set of calculations that sorts through the data contained in the digital image. An intelligent algorithm is one that learns what to look for as it analyses more and more data.

Intelligent algorithms in smart CCTV systems are designed to replicate how the human eye and brain work. The software breaks down an image into tiny parts, known as 'pixels'. You may recognise the term 'pixel' if you have a digital camera or a smartphone. If a digital camera has '8 megapixels', each image it captures is made up of 8 million pixels.

The algorithm is then able to calculate the degree of movement for each pixel in the image. This allows the software to identify the active areas in each scene. From this, it learns to recognise the patterns of movement in an image. The system can then identify and classify events according to the patterns it already knows about. For instance, software can distinguish between passive spectators and fans jumping up and down at a football game.

5.3 Security improvements

Smart CCTV can improve security in the following ways.

Security problems are easier to spot as they arise:

- The system identifies anything unusual and alerts the CCTV operator with an alarm. This makes it easier for the operator to interpret the images.
- The alarms make it easier for the operator to make faster, more efficient decisions about whether or not to take action to combat a security problem.
- The algorithms in the system can sometimes pick up details that an operator could miss. This is because they can deal with very high volumes of information.

Fear of crime and of intrusiveness will be reduced:

- When the security technology works effectively, people are reassured because they know that anything unusual that is happening around them will be spotted quickly by a smart CCTV system.
- Digital smart CCTV cameras can see in much greater detail than traditional CCTV cameras. This means that fewer cameras are needed to monitor a space. As a result, smart CCTV surveillance can feel less intrusive because fewer cameras are present.
- Privacy can be enhanced as sensitive areas of images, such as views into private property, can be 'blacked out' so the operator does not see them.

5.4 Issues

Several drawbacks to smart CCTV need to be considered.

The smart CCTV algorithms currently in use have a number of problems and weaknesses. These weaknesses can result in a 'false alarm', which incorrectly identifies a security incident. This could mean confusing someone who is innocent with someone who is a suspect. The current weaknesses are:

- Only certain kinds of object, such as a car number plate or an unattended bag in an empty space, can be reliably spotted.
- The cameras are less able to identify what is going on in a crowd.
- Covert crimes, such as pickpocketing or shoplifting, are difficult to identify.
- The algorithms are open to bias because they are programmed by humans to identify what they consider to be 'abnormal'. There is a danger that systems may, either deliberately or accidentally, be programmed to target minorities in discriminatory way.
- If, in the future, a potential criminal knows that smart CCTV is being used, they can avoid being tracked simply by changing their clothes, as the algorithms work by recognising the clothes suspects are wearing.
- The high level of false alarms that are sent to human operators could result in them losing confidence in the system and ignoring what it tells them.

Smart CCTV cameras are more powerful as well as smaller:

- They can capture more information and so potentially they are more privacy invasive. This is because the activities of innocent people are more likely to be captured and analysed.
- Cameras are less easy to spot, making it more difficult for people to know that they are under smart CCTV surveillance. As a result, it is less easy for people to challenge or avoid surveillance.
- It may affect freedom of expression as well as the dignity of the person if their behaviour in public spaces is being monitored by this combination of software and people.

Human beings are still required to operate the systems. This means that:

- A human is required to interpret the images and confirm there is a real alert. While the system may identify unusual behaviour, it does not explain why that behaviour is taking place.
- Institutions need to be very closely regulated on the types of search being undertaken and safeguard against the misuse of data.

6 Drones

A drone is the flying element of an unmanned aircraft system (UAS). It is flown by a pilot via a ground control system, or autonomously through the use of an on-board computer. Drones are also known as Remotely Piloted Aircraft (ROA), Remotely Piloted Vehicles (RPV) or Unmanned Aerial Vehicles (UAV). The use of drones gained greater public attention after the United States increasingly started using drones in its war against terrorism in Afghanistan, Pakistan, Yemen and Somalia following the September 11 terrorist attacks. Recently, many European states are rearming their military forces with drones.

Drones are not only used by the military in a war-like context, but also by law enforcement agencies for reconnaissance and surveillance to ensure civilian security. These non-military 'civil' drones are increasingly being used as flying cameras that monitor public spaces in order to prevent or detect a wide range of security threats. Civil drones are also used for non-security related purposes, such as cartography, real-estate photography or as toys. Another important aspect is that this technology allows for surveillance of areas that are too dangerous for humans to move in, such as after an avalanche, earthquake or nuclear accident. For example, drones were used after the Fukushima accident to monitor the state of the plant and to control the radiation level.

As the SurPRISE project explores the capabilities of existent and emerging surveillance-oriented security technologies as measures to foster security, here we focus primarily on civil drones that are used for security purposes.

6.1 Why drones were developed

Drones were initially designed for purposes of military reconnaissance and targeted strikes with weaponry. The technology of remotely controlling an unmanned aerial vehicle was first employed during World War I. The first vehicle was conceived by Prof. A. M. Low in the UK in 1916. And it was designed both for defence against the Zeppelins controlled from the ground, and as a flying bomb for which control from an accompanying manned aircraft was considered.

Although drones are today most commonly associated with military actions, UAVs are increasingly used by civilian government agencies, businesses, and private individuals.

Within the EU, the use of 'light' drones that weigh less than 150 kilograms, and the use of all types of drones for security or military purposes, are regulated by the member states. The regulation of the use of larger drones for commercial purposes is currently being investigated by the European Commission, which aims to start integrating drones in the EU's civilian airspace by 2016. By 2028, drones should be fully integrated in the EU's civilian airspace.

Current research aims at making drones even less dependent on human supervision in the future, thereby crossing the boundary into robotics. Drones are being equipped with sensors that will enable them to fly autonomously in an urban space. New methods are also being developed for the mass-production of micro drones. The technological capabilities of drones are developing quickly, as construction and deployment costs are becoming increasingly cheaper.

Drones may be linked up to a variety of different add-on equipment, which enables surveillance as well as intervention. The nature of the add-on depends on the size and payload capability of the individual vehicle.

6.2 How drones are used

Drones can efficiently complement existing infrastructure (manned aircraft or satellites) being used by public agencies to support crisis management, law enforcement, border control, traffic monitoring or fire-fighting operations.

In a security context, law enforcement agencies have used drones in the EU predominantly to monitor crowds at large-scale public events such as music festivals, demonstrations and sporting events in order to detect unusual events or sudden crowd movements. They can also be used for crime scene investigations. Their use in border control is also a possibility that will be exploited in the EU more in the near future. Drones have also been used to detect drug cultivation and to support police activities.

Surveillance drones used to monitor public spaces have a huge comparative advantage. They can monitor a much larger space, are mobile, and their use at a height of 50 to 200 metres allows for a different perspective compared to the more static public CCTV cameras.

Drones can be used for a vast amount of commercial applications. They can be used to support precision agriculture and fisheries, power/gas line monitoring, infrastructure inspection, communications and broadcast services, wireless communication relay and satellite augmentation systems, natural resources monitoring, media/entertainment, digital mapping, land and wildlife management, or air quality management and control.

Despite these impressive perspectives, various technical issues related to drones still remain unresolved. These issues are related to, for example, limited capabilities regarding flight altitude, speed and duration, as well as the refuelling drones during flight. Drones are also very vulnerable to inclement weather conditions, like heavy clouds, wind, and rain. Moreover, drones producing data through advanced equipment, such as CCTV cameras or sensors, cause workload and trigger problems related to insufficient bandwidth. CCTV footage can often be blurry due to the movement of a drone.

How drones work

Drones come in a wide variety of formats, and they can carry a virtually unlimited amount of 'payloads', i.e. the things that are attached to the drone, such as cameras, sensors or missiles. Drones are usually remotely controlled by one or more operators on the ground that control and monitor the activities of the vehicle and its payload. It is possible to control a drone with a smartphone or a tablet. In some cases, it may be possible to pre-program a drone for a specific flight route within its range. However, compared to remote piloting, the autonomous programming of such drones is still in its infancy and the focus of current research. The communication between a drone and its operator may occur in various forms, though, for longer distances, a satellite link may be needed to support the transmission of data from the vehicle and to relay commands back.

A UAV system typically consists of these elements:
- Unmanned aircraft (UAV)
- Ground control unit, eventually mobile
- Data link, eventually with satellite support
- Additional equipment.

The size and equipment of drones vary greatly and depends on the purposes for which they are used. Drones can, for example, be equipped with CCTV, sensors, panoptic equipment, radars, Wi-Fi and other communications interception technology, chemical or radiation detection, and armoury. Since much research focuses on the development of micro or nano-drones that are able to imitate the movement of insects or birds, it can be anticipated that the surveillance capability of drones will be almost unlimited in the future, although the permitted deployment scenarios are still rather limited due to legal restrictions.

6.3 Security improvements

1. Drones make it easier to spot security problems

   - Drones can monitor large and/or inaccessible areas. For example, in a search and rescue context, drones can be used for the surveillance of large inaccessible areas such as dense forests. Drones can also monitor large border areas in order to detect unauthorized entries and to combat human trafficking.
   - Drones are mobile. They can not only detect and register suspicious objects and individuals, but also further track these as they move in public spaces. Unlike human teams that follow individuals or objects, drones do not get tired and are less visible, so they are able to track objects and individuals for a long period of time.
   - Drones are less visible than CCTV cameras. As a result, they are harder to detect by potential wrongdoers.

2. Fear of crime and of intrusiveness will be reduced:

   - When people know that a specific area is being monitored by a drone, they might feel reassured because they know that anything unusual that is happening around them will be spotted quickly by the drone.

6.4 Issues

1. Drones are less visible than static CCTV cameras or sensors, thus they have the capacity to indiscriminately record and store information, making them a potentially more privacy invasive tool.

   - The capacities of drones transcend those of (smart) CCTV cameras since drones can collect information from private places that individuals have tried to prevent from being seen by constructing walls, fences or other objects. As a result, drones can record images of private properties that are not visible to static CCTV cameras.
   - Similarly to the great majority of surveillance technologies, drones also have the capacity to indiscriminately record and store information, they are more likely to capture and analyse the public and private activities of innocent people. This can create a chilling effect.
   - In comparison with CCTV cameras, drones are even less easy to spot, making it more difficult for people to know that they are being monitored. Their intrinsically mobile character makes it hard to find out who exactly is operating the drone. As a result, it is less easy for people to challenge or avoid surveillance.
   - This difficulty can trigger a permanent feeling of uncertainty in the individuals being observed, causing more or less subtle changes in their behaviour to avoid unwanted and negative attention. This aforementioned 'chilling effect' becomes even stronger once drones will be equipped more with so-called 'smart CCTV' features, like behavioural/anomaly pattern recognition functionalities, which may severely affect the exercising of basic rights like freedom of expression and freedom of association in public spaces.
   - The use of drones in combination together with ground-based static CCTV and location trackers deploys a much more comprehensive surveillance of citizens, making detailed movement, behaviour, and social profiling possible.

2. Drones equipped with data recording devices such as CCTV or sensors may be vulnerable to hacking from external parties due to lack of encryption and the exploitation of communication disruption towards the base or pilot.
3. There are also public safety issues related to the use of drones in inhabited spaces

   - Drones have still a much greater accident rate than manned aircraft because they are more susceptible to weather conditions (wind, rain). This increases the risk to individuals on the ground.

7 Cyber surveillance by deep packet inspection

Internet service providers, telecoms network operators and telecommunications companies have always been able to monitor their networks. Knowing who is communicating with whom, which websites are being visited and which services are used, inform the customer billing, network management and marketing activities of these companies. However, a technique called 'deep packet inspection' (DPI) enables companies, intelligence services and governments to access the content of communications sent via the internet. To draw an analogy, DPI is equivalent to the postal service opening all letters, reading them and sometimes changing, deleting or not delivering them.

DPI is capable of monitoring every aspect of digital communication. This ranges from the information you read online, the websites you visit, the videos you watch and your search terms, whom you communicate with via email, instant messaging or

How deep packet inspection works

When you send or receive information over the internet, it goes through a very complex process and passes through numerous computers.

Computers connected through the World Wide Web break the information that you send and receive into smaller chunks called 'packets'. This is so the information can travel easily across the internet. When the packets arrive at their destination, they are joined together, like a jigsaw puzzle, to make the message. Each packet has a label on it called a 'header': this describes what the packet is, who it is from and where it is going, just like a letter sent through a postal network. Inside the packet is the content of the message, which is called the 'payload'.

Each packet has several layers, each containing different information about the message. The layers sit inside each other, a bit like a Russian doll. Internet service providers do need to inspect some of the message's packets in order that it can be delivered. Most of the time they need to look only at the headers (the outside of the envelope) rather than at the payload (the inside of the envelope) to ensure a message is delivered. This is called 'shallow packet inspection'. Deep packet inspection, by contrast, involves inspecting all the packets of a message and looking not only at the headers but at the payloads as well.

Packets are inspected using computer algorithms that scan messages for particular kinds of data. In the discussion of smart CCTV, we described algorithms as sets of calculations that sort through and analyse data. They are used in DPI as well, but in a different way.

In DPI, an algorithm will be programmed to look for particular 'keywords', similarly to when you search for information in a web browser. The kinds of data that are searched for depend on who is doing the searching and why they are doing it. The keywords used may relate to criminal or suspicious activities, to a new computer virus that is circulating, or even to whether a certain product has been bought.

social media. DPI applications can open and analyse messages as they travel, identifying those that may pose particular risks. You do not have to be a suspect to be affected by DPI – DPI intercepts and reads every message that travels over the network of an internet service provider.

7.1 Why deep packet inspection was developed

DPI was originally developed to detect viruses and malware that would damage computer networks. Nowadays, by using DPI to analyse the content of messages as they travel, not only can viruses be stopped, but malicious, dangerous or criminal activity that takes place via the internet can also be identified.

All the equipment that houses the technology that performs deep packet inspection is owned by internet companies. Those companies can control how the internet works locally, regionally, nationally or internationally. These companies want to use the technology for their own ends, but they can also make money out of it by selling their innovation to others. Other companies, such as defence corporations, have also developed DPI technology and want to do the same. There is now a market for DPI technology.

7.2 How deep packet inspection is used

In Europe, DPI can only be used legally in very limited ways. Under existing laws, it can be used to 'filter' internet traffic, sifting through it for viruses and malware. In addition, it can help internet companies to manage traffic flow on their networks. But DPI technology is also capable of analysing all the content of online communications. When used in this way, it can detect very specific crimes, such as the distribution of child pornography. But this is legally controversial as there is no specific law regulating this 'detailed' use of DPI. This is because the European laws on communications technologies were drawn up at a time when DPI did not exist. The European Court of Justice and the European Data Protection Supervisor have interpreted these laws to say that they only relate to the limited 'filtering' of online communications. New laws need to be developed, which will enable the more detailed use of DPI to be properly regulated.

As a result, DPI cannot legally be used to monitor general communications, to detect illegal copyright infringement, to block politically sensitive content or to target advertising, although, as a technology, it is capable of doing all of these things. European laws protect the confidentiality of communications. DPI would also breach the European Convention on Human Rights because it comprises warrantless, mass, untargeted surveillance: it can read every bit of information that is sent and received between computers.

The picture is very different in the USA, where it is unregulated and many companies use it to target advertising. If you have a Gmail™ or Yahoo™ email address, the message will almost certainly travel via the USA and be subject to DPI. It appears that DPI was used in connection with the United States' National Security Agency (NSA) and the United Kingdom's General Communications Headquarters (GCHQ) mass surveillance programmes revealed in the summer of 2013.

How DPI can be detected, limited or controlled is something of a grey area. Regulation is trying to catch up with what the technology is capable of doing. It is very difficult to know the extent to

which DPI takes place. Any message you send or receive can travel all over the world before it arrives. It may have been subject to DPI conducted by an internet service provider or by a government security service in any number of countries. It is almost impossible to tell. Without regulation, a 'Wild West' situation exists, where companies and governments alike may be exploiting this regulatory grey area.

What we can say is that, worldwide, many different institutions make use of DPI. Internet service providers, marketing companies, the police and security agencies of national governments have made use of it at different times. There are a few reported uses of DPI apart from the vast surveillance activities by US security agencies revealed by the American computer professional, Edward Snowden last year: some are commercial and others relate to public and national safety.

7.2.1 Commercial uses

- *Network security and management:* Messages are inspected to make sure they do not contain viruses and large person-to-person file sharing is often filtered
- *Behavioural advertising:* Data are gathered from messages about a person's product preferences. This is not permitted in Europe but is welcomed by some consumers in the USA, where it is allowed. It enables them to access products and services that are suitable for their needs.
- *Digital rights management:* Messages are inspected to identify illegal file sharing and copyright infringement.

7.2.2 Public and national security uses

Government surveillance of criminal activity: Deep packet inspection is proposed as an investigative tool in relation to very specific crimes, although this is legally controversial. This includes crimes:

- committed against computer systems, or committed using a computer (e.g. the distribution of child pornography)
- where racist information has been shared, or where racist threats have been made
- where terrorism has been incited or organised
- where information is shared that approves of genocide or crimes against humanity.

Censorship: It has been speculated that DPI has been used to mislead political opponents in repressive regimes all over the world. US defence company, NARUS, a subsidiary of Boeing, sold DPI to Libya, which used it to crush dissent during the Arab Spring. By contrast, in the wake of the Arab Spring, the UK limited the sale of DPI technology to Egypt, Bahrain and Libya by revoking export licences. Although the supplier of the technology being used is unclear, Iran is using DPI not only to eavesdrop on and censor what information citizens can access online, but also to alter online content for the purposes of disinformation. China uses DPI in a similar manner. Questions remain as to whether internet censorship also goes on within Europe.

7.3 Security improvements

Deep packet inspection can improve information security and the fight against crime by identifying and blocking harmful, damaging or criminal messages described in section 7.2.2.

Although DPI cannot prevent the serious crimes, to which these messages relate, it allows their detection and can provide evidence in an investigation. By contrast, it *can* prevent the spread of computer viruses and other forms of cybercrime.

7.4 Issues

Deep packet inspection raises the following serious issues:

4. DPI is all-seeing.
    - It can analyse all messages and the sensitive data they may contain as they travel, which means that electronic communications are no longer private under DPI.
    - Knowing that communications are no longer private could result in a serious 'chilling effect', where people are afraid to communicate openly and express themselves freely.
    - The use of DPI needs to be very tightly regulated because of its huge power.

5. Technological capability is changing faster than regulation.

   - There are no clear legal rules as to what DPI can and cannot be used for.
   - In practice, DPI's use depends on the ethics of who is using it. It can be used for anything from the detection of computer viruses to political oppression.
   - In countries where a national government and national communications providers have a close relationship, information could be shared in a way that gives the state access to all electronic communications made by citizens.

6. It is difficult to pinpoint exactly who is using DPI and where they are doing so.

   - Legal regulations would need to be the same throughout the world. For some time, data protection authorities worldwide have been calling for an international minimum standard of privacy.
   - A 'DPI regulator' would need to be a truly international body with sufficient power to punish offenders.

7. The effectiveness of DPI is questionable:

   - As computers identify potentially problematic messages, there is an issue of incorrect interpretation and innocent people becoming suspects.
   - Some experts have challenged the effectiveness of DPI in finding illegal material.

8 Smartphone location tracking

The smart mobile phone has almost eclipsed the Swiss army knife as the perfect, all-in-one tool and toy. There are roughly 5 billion mobile phone connections worldwide. On average, there are just under 1.3 phones per person throughout Europe. That's a huge number when you consider that pocket-sized phones were not available until the early 1990s.

8.1 Why smartphone location tracking was developed

Smartphones are a relatively recent development. Their enormous popularity stems from the fact that they are able to do many different things as well as be a regular mobile phone. In fact, smartphones are more like small pocket computers that happen to be able to make phone calls. Like a desktop or a laptop computer, each type of smartphone has its own operating system, which can enable email, messaging and web browsing. Smartphones can run software applications, which can deliver services such as games, mapping and online news. They also feature digital and video cameras, portable media players and have bigger, colourful screens, which can be operated by touch.

Mobile phones have a history that dates back to the Second World War. A basic mobile phone is essentially a wireless radio that can send and receive messages. The first wireless radios, 'walkie-talkies', were introduced to help soldiers stay in contact on the front line. In the 1970s and 1980s, innovations in microprocessors saw the first handsets emerge. The original mobile phone handset was the size and weight of a brick and the battery lasted only 20 minutes. How times have changed! From the 1980s onwards, a growing network of mobile phone masts improved phone signals both locally and over longer distances.

Phone masts are very important for the location of mobile phones. A phone mast covers a set geographical area. In order to connect to the network, make calls and send texts, all mobile phones must register at the nearest phone mast. The mast to which it is connected always records a phone's location. If the person using the phone moves into the range of a different phone mast, the phone registers there instead. So the movement of a person carrying a phone is tracked by the telecommunications provider. Current regulations in the European Union require operators to store this data for at least six and up to 24 months. Although the respective EU directive was rejected by the European Court of Justice in April 2014, national regulations have not yet been changed.

Smartphones can be located in other ways, too. The person using the phone can set it up so that the mobile phone establishes its location using global positioning satellites and by connecting to wireless networks.

This has led to a huge growth in the provision of 'location-based services' for smartphones. These are usually available as applications ('apps') that can be installed on the phone. An app is a piece of software that can perform a specific function or service. Location-based apps can enable a user to find information about nearby restaurants, or shops, or which of their friends are close by. Location-based gaming is now available too. Location-based services will probably grow in use in the coming years.

Location-based services offer a lot to the smartphone user. However, for some privacy advocates, the level of information that can be revealed by smartphone location tracking is a worry. For example, when German Green politician Malte Spitz got hold of the records for six months of his mobile phone's location data, they looked like a meaningless stream of numbers and letters. But when Malte had a statistician look at the data, a detailed picture of his life emerged. In conjunction with *Die Zeit* newspaper, Malte produced an animation detailing exactly where he had been over the course of half a year. Malte became worried because of the level of detail that could be revealed about him, particularly if the location information was com-

bined with information from social media such as Twitter or Facebook.

In a recent US Supreme Court case, the judge observed that GPS data was able to disclose 'indisputably private' trips, such as 'trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment centre, the strip club, the criminal defence attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on'.

8.2 How smartphone location tracking is used

There are both commercial and security uses of smartphone location data.

8.2.1 Commercial uses

- Phone bill administration: Mobile phone companies need location data as well as the phone's identification number to generate a phone bill.
- Targeted marketing: Software houses that produce apps, such as Twitter, Angry Birds or FourSquare, gather location and other contact data from phones and sell it to advertisers. Advertisers then use the data to design the adverts for products sold in the spaces they know different kinds of consumer use. Angry Birds, for example, has been downloaded one billion

How smartphone location tracking works

Both regular and 'smart' mobile phones can be location tracked. There are three ways to track a mobile phone: through mobile phone masts, global positioning systems or wireless networks. The first applies to all mobile phones, whereas the second and third apply only to smartphones.

Mobile phone masts: All phones register with the nearest mobile phone mast so that calls, texts and emails can be sent and received over the mobile network. Each phone contains a unique reference number, which links the phone to an account with the mobile phone company and, therefore, to the user. This information is also needed to generate phone bills. If security services or law enforcement agencies are trying to track the movements of a particular person at a particular time, they can request phone mast data from mobile phone companies. The phone mast records indicate whether the person's phone was within the range of a particular mast. When this is done for all masts – as it is the case in the EU – the phone's location can be traced and the movements of its owner revealed.

GPS: Smartphones contain mapping software and applications that rely on global positioning data to work. When the GPS feature in a smartphone is switched on, the phone works out its position on the planet by calculating how far away it is from the nearest GPS satellites overhead in space. When the feature is switched off, the phone cannot locate itself using GPS. However this feature can be activated remotely without notifying the user, e.g. if they have an app installed on their phone, which enables it to be located if it is lost or stolen. Apps providers gather this location data and some sell it on for marketing purposes.

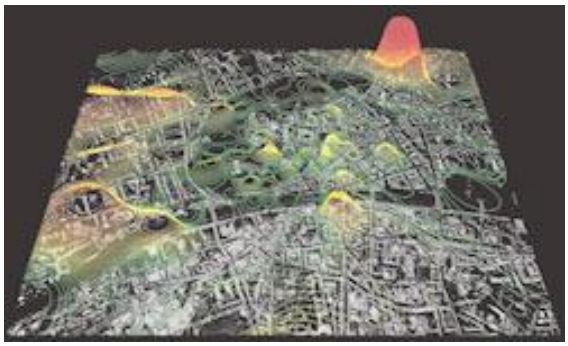
If security services and law enforcement agencies are tracking a particular person, they can request GPS data from phone companies.

Wireless: Smartphones can connect to wireless networks that operate over a designated area. Connecting to a wireless network locates the phone within the boundaries of a wireless network. Once again, turning off this feature of the phone will mean that the phone cannot be location tracked in this way. Typically, a Wi-Fi access point will have a range of 20 metres indoors, but a greater range outdoors.

Other 'smart' mobile personal devices, such as iPads, tablets and notebooks, can be tracked in the same way.

times worldwide. Users were surprised to find that its Finnish developers, Rovio Entertainment Ltd, routinely collected and sold the location data of players. Fifty percent of all apps collect location data even when the app does not need the information to run.

- Urban planning: Location data can be used to map the use of city spaces. As there are more phone masts in urban spaces when compared with rural areas, phones can be tracked much more closely. This rather spooky-looking image is a map of mobile phone use in Graz, Austria. Researchers at the Massachusetts Institute of Technology tracked mobile phones anonymously to build up a picture of how people moved around the city of Graz. Their aim is to inform urban and transport planners about how the city is used.



8.2.2 Public and national security uses

- Finding lost and injured people: In the USA and Canada, a service called E-911 legally mandates the use of GPS in all mobile phones so that they (and their users) can be located in the event of an emergency. In Europe, around 180 million emergency calls are made every year. Sixty to seventy per cent of these originate from mobile phones. The phone reveals its location data to the European-wide emergency number 112. Unlike Americans and Canadians, Europeans are not required to have GPS switched on at all times in their phone.
- Tracing the movements of criminal suspects: Security and law enforcement services are able to access location-based data by submitting data requests to mobile phone companies. Currently, any such request in Europe will be governed by law. Upon receiving such a request, companies will be required to hand over to the security services any data pertaining to a suspect. Security services have other phone-tracking methods too, which can be applied to specifically targeted individuals.
- Tracking family members: Individuals may also benefit from location-based services. Many parents will be familiar with individual mobile-phone-tracking products, for example, which enable them to see where their children are at all times.

Controversy in smartphone location tracking

Following the 'Occupy' protests in New York, Twitter was forced to give location data to the US government so that it could identify the protesters. Recently, Twitter launched a new service called 'Please Don't Stalk Me'. This allows users to fake the location data attached to their tweets. The 'Please Don't Stalk Me' app lets users pinpoint any place on the planet, via Google Maps, and embed that spoofed location data in their tweets. Other apps, such as 'My Fake Location', 'Fake GPS Location' and 'GPS Cheat' do the same thing.

8.3 Security improvements

Smartphone location tracking improves security in a number of ways:

- It enables those in risky situations to be found and helped.
- It enables vulnerable adults or children to be monitored by their families.
- Police and law enforcement agencies can use location data to place individuals at the scene of a crime or to rule them out as suspects. They can also track and trace suspects in ongoing investigations.

8.4 Issues

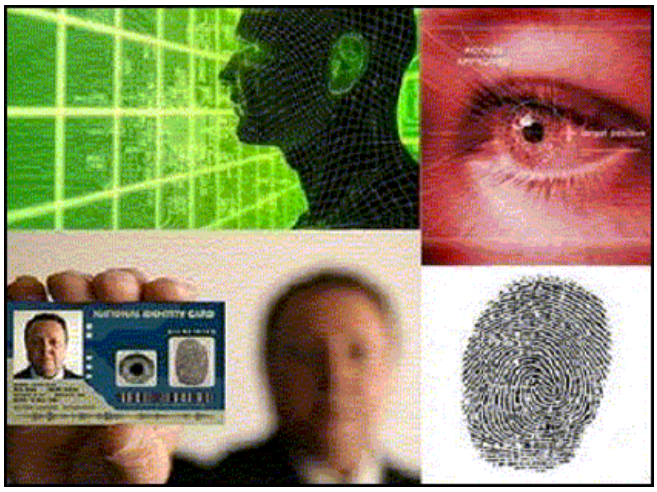
Smartphone location tracking raises the following issues connected with privacy, regulation and human rights:

- Users do not have complete control over the information disclosed by smartphones. This is particularly difficult for more vulnerable users, such as protected witnesses, who may not want to share location data but would still like the benefit of a mobile phone. Some phones, such as Apple iPhones, automatically store location data in the phone and this feature cannot be turned off.
- Many apps collect location data even if the app does not need these data to run.

- Many app developers are located outside Europe so they are not bound by its data protection regulations. Therefore it is difficult for the EU to insist that apps should be privacy-friendly. However, a recent amendment to the ePrivacy directive insists that users must be able to consent to data being processed from their smartphone apps, no matter where in the world the app provider is based.
- In a manner similar to deep packet inspection, in countries where a national government and mobile phone providers have a close relationship, information could be shared in a way that gives the state access to the location data of all citizens.
- As location data have been used to identify protesters, their use has a potential 'chilling effect' as individuals may become wary of protesting and exercising their democratic rights.

9 Biometrics

'Biometrics' can refer to either systems that use measurable physiological characteristics of a person, such as fingerprints, DNA, retinal patterns, facial structure, body odours, or the analysis of unique personal behaviour traits, such as gait and voice analysis and keystrokes, in order to recognise the identity, verify the claimed identity of an individual or categorize an individual.



Some countries capture their citizens' fingerprints and other biometric 'identifiers', and store these in national identity cards or in a database. At this point, a person's characteristics are enrolled and stored into a biometric system. At later stages, the biometric information of the person is compared with the information stored at the time of enrolment to verify that person's identity. Significant advances in the field of computer processing have resulted in automated biometric systems, allowing, for instance, mass identity checks within seconds.

9.1 Why biometrics were developed

In the 19th century, the development of national justice systems required a more formalised way of identifying people. These systems sought to treat first-time offenders more leniently and recidivist offenders more harshly. As a result, a formal system was needed that recorded offenses along with measured identity traits of the offender. In France, Alphonse Bertillon developed 'Bertillonage' or anthropometries, a method of identifying individuals based on detailed records of their body measurements such as height or arm length, physical descriptions and photographs. In the 1890s, a more promising approach emerged, when Sir Francis Galton was able to develop a method to retrieve records to identify criminals on the basis of fingerprints, which was a more individualized identifier compared to Bertillon's measurements. In the 20th century, other biometric identifiers were discovered as potential identifiers. In 1936, Frank Burch proposed the concept of using iris patterns as a method to recognize an individual, and facial and speaker recognition techniques were developed in the 1960s.

9.2 How biometrics are used

Biometrics have traditionally been used by law enforcement authorities to identify known and unknown criminals or to authenticate access to secure locations, government buildings, business premises etc.

In the 21st century, biometrics are increasingly used in a border security context. Biometric data is captured from visitors requiring a visa to visit a particular country. Upon arrival, these biometrics are checked against a database in order to verify, for instance, whether a traveller has previously been determined inadmissible, is a known security risk or has previously overstayed the terms of a visa. For instance, the EU also collects 10 fingerprints and a digital photograph of those persons who are applying for an EU visa. This biometric data is stored in the VIS-database (Visa Information System). Similarly, the EU has established EURODAC, a large database of fingerprints of applicants for asylum and undocumented migrants found within the EU. The database helps the effective application of the Dublin convention on handling claims for asylum.

In a military setting, the US military has employed handheld devices in battlefields in Afghanistan and Iraq that allowed them to routinely subject people they encountered to iris or other biometric scans. Persons of interest are subsequently placed on a 'Biometric Enabled Watchlist' that allows soldiers in the field to verify the identity of a terrorist suspect, or to reveal that a local national has ties to an

insurgent network, leading to denial of his employment at a U.S. military installation overseas. So far, the database contains 209,000 records on individuals all over the globe.

While biometrics may have been originally developed to identify individuals for security purposes, throughout the 20th century, they have been increasingly used to develop commercial access control mechanisms. Their advantage is, that unlike keys and passwords, the personal traits are extremely difficult to lose or forget. They can also be very difficult to copy. For this reason, many people consider them to be safer and more secure than keys or passwords. For example, Apple's new iPhones have now a fingerprint sensor, which is able to make a scan of the user's finger. Facebook uses facial recognition tools to automatically suggest the identity of a person in a picture. Its research project, DeepFace, can say with 97.25% accuracy whether two pictures contain the same face. Banks are developing voice biometrics to allow customers to access a credit card and make payments on their mobile just by saying a passphrase. Companies use laptops, which include fingerprint readers for biometric access control. Advertising displays in public streets may even show different advertisements depending on the individual that is looking at then, based on their age or gender.

However, biometrics are increasingly used not only as identifying tools but for behaviour analysis. A number of fitness applications use real-time biometrics, such as heart rate and respiration rate to give tailored fitness recommendations to the users of the app. In a security context, new biometric processing capabilities are coupled with an existing system (e.g. facial recognition into CCTV), which results in new surveillance capabilities. In this context it is important to note that new biometric systems have the potential to collect infor-

How biometric identification works

The first step is a biometric sample from the individual, such as a fingerprint or iris scan, typically by means of a picture. The data can be stored either as a picture, or as a template, which is a digital representation of the biometric created using an algorithm. To safeguard the highest level of privacy, it would be recommended to store the template only, and discard the original image.

The biometric data, either the picture or the template, can be stored in various locations, for instance in the operations centre where the enrolment took place (e.g. in a reader) for later use, and on a device carried by the individual (e.g. on a smart card). It could also be sent and stored in a centralised database accessible by one or more biometric systems.

When a biometric system is accessed, the system will ask the person to submit the biometric characteristics. The system will then compare the picture or the template of the submitted sample with the biometric data of the person recorded in the system.

If the biometric 'matching' process is successful, the system recognizes and accepts the person. If the match does not succeed, the person is not recognised and consequently is 'rejected'. The picture or the template created when the biometrics are first recorded will seldom be identical to the picture or the template of the biometric features that will later be presented. The relevant feature often changes slightly or is submitted in a manner slightly different than during the enrolment. Inevitably, there will be a certain degree of probability in the match.

Biometrics can be used in crime prevention as well, especially when it uses the analysis of personal behaviour traits, and the aim is not the identification of a particular individual but its categorization. The face recognition and behaviour analysis functions of the smart CCTV cameras can be regarded as biometric functions of the surveillance cameras.

mation from a distance or in motion without the need of cooperation or action required from the individual. Such systems might trigger an alarm, for instance when a CCTV camera identifies a known criminal whose image has been placed in a police database.

9.3 Security improvements

Biometrics can improve security in the following ways:

- Identification by biometric identifiers has been used for more than 100 years in law enforcement for both verification and identification tasks. Systems analysing the face of a person as well as systems that analyse the DNA of a person can contribute very efficiently to the fight against crime and efficiently reveal the identity of an unknown person suspected of a serious crime.
- The collection of biometrics can be used to increase the security of specific sensitive data processing activities. It can help for instance to ensure that only authorized persons at a particular telephone operator have access to traffic data (and location data) which must be retained for law enforcement purposes.

9.4 Issues

Several drawbacks need to be considered:

1. Biometric data is not infallible.
    - It can be said that two digital captures of a biometric trait will never be exactly the same. Differences in the type of equipment used at the time of enrolment, or differences in the environment (light, temperature) may lead to false acceptance and reject rates: a biometric system can incorrectly identify an individual or will fail to reject an impostor (false acceptance rate). A false reject occurs when an individual is not matched to his/her own existing biometric template.
    - Also, a person's biometric features may change during their lifetime, e.g. by aging, surgery or an accident. A biometric system might not recognize them any longer.
    - Falsifications of biometric data is possible, which results in an increased possibility of identity theft.
    - At the current state of the technology, it is still easy to trick, for example, a face recognition biometric system through simple changes in the appearance, like different hairstyles, beards, make-up, glasses, contact lenses, etc.
2. In the past, the use of biometrics was expensive and time-consuming. As a result of these constraints, the impact on an individual's data protection rights was limited. This has changed, which might lead to genetic discrimination and a gradual loss of privacy if no adequate safeguards are implemented. For example, equipping video surveillance systems and smartphones with facial recognition systems based on social network databases could put an end to the anonymity and untraced movement of individuals.
3. In most cases, the enrolment requires the personal involvement of the individual, e.g. in the case of fingerprinting, and therefore may provide a suitable opportunity to provide information and fair processing notification. However, it is also possible to enrol individuals without their knowledge or consent e.g. using CCTV systems with embedded facial recognition functionality. This has serious consequences on their capacity to exercise free consent or simply get information about the processing.
4. Biometrics as unalterable characteristics may also be problematic once the enrolment was already compromised, potentially leading to false stigmatization of an individual.

10 Is surveillance-based technology the only answer?

You might well be wondering whether security technologies are the only solution to security problems. At times it seems that tracking and identifying suspects within the general population is what security is all about. Surveillance-oriented security technologies work under the assumption that an extended surveillance system monitoring as many people as accurately as possible is the best way to detect potential threatening actions and to identify potential criminals after the crime has been committed, or, alternatively, even before it has actually been committed. Whenever such technologies are implemented, security is sought almost exclusively through enhanced surveillance.

This is partly the case but it is not the whole story. While security technologies are used to find criminals and terrorists and second-guess their next moves, there exist different strategies that aim at enhancing security through other means. In this chapter, we are going to look at approaches that can be considered as alternative security measures.

Security is an ambiguous social term that can be perceived in different ways. Conditions that are associated with societal stability, social certainty or reliability are highly connected with the discerned level of security.

10.1 Alternative security measures: the global level

The European security priorities that we looked at earlier seemed to suggest that security is something that features in all areas of life. They concern the 'classic' security issues such as crime and terrorism. From what we have seen in the previous pages, it is possible to use new security technologies to find the people who are involved in such activities. But there are underlying issues that cause these security problems to arise in the first place, such as poverty, national or international conflicts, or political and religious differences. Security technologies are not able to address these root causes.

European security priorities also refer to crises or disasters as security problems. These disasters could involve food or water shortages, financial crises, the spread of disease, or natural disasters: things that challenge overall human security. Once we are thinking of security in terms of "overall human security" we might want to have a brief look at some global societal challenges:

Security initiatives aiming to increase security levels in relation to natural or manmade disasters can, to some extent, be proposed and implemented. Such initiatives are most often rooted in long-term comprehensive approaches. The promotion of fair global systems of trade, aid and debt relief, for instance, tries to address not only economic matters but also environmental issues related to overexploitation of natural resources, pollution and serious alterations of environmental and climatic cycles. These are ultimately security issues. By the same token, policies aiming to improve local and national disaster responses, or policies improving communication and information infrastructures, and food and water supplies are also alternative ways to advance living conditions, hence pursue enhanced security levels in relevant areas.

Different ways to understand security and, thus, different ways to promote security have been developed not only at global level. Hence, we would like to draw your attention to your local environment to envisage a number of further approaches that are trying to enhance security.

In a nutshell: national and international solutions

- Promoting fair global systems of trade, aid and debt relief.
- Promote economic and social policies for more equal distribution of incomes and employment
- Improving disaster response infrastructures and resource.
- Using sustainable and alternative energy sources more effectively.

- Improving communication and information infrastructures, and food and water supplies in those parts of the world that need it.

10.2 Alternative security measures: the local level

There are different and alternative ways of understanding and pursuing higher levels of security on a local level. For example, security can be pursued through the implementation of technologies that do not involve surveillance. Metal detectors, motion-sensitive lights, volumetric alarms, general warning devices, or even emergency public telephones are all technologies aiming to increase security without introducing surveillance or data retrieval. They seek to enhance people's ability to react and intervene to protect themselves and their property. Alternatively, technologies like metal detectors help public authorities to detect potential dangers by focusing on the source of threat (the metal object) rather than on the characteristics of the individual potentially constituting a threat. Their effectiveness may be very high but limited to the specific moment and place in which they operate. Yet they do not constitute a threat in terms of privacy or surveillance.

Attempts to prevent crime and increase security in the public space can also be made through urban management and planning. Structural alterations to promote a safer built environment, e.g. in reducing 'danger zones' (streets, squares, parks that were difficult to observe), can help to increase the level of perceived security in the public sphere in the first place and, at the same time, help citizens to be more aware of their surrounding environment and of the dangers that may arise.

In a nutshell: approaches that are not based on surveillance and data collection

- Crime prevention through urban planning and environmental design.
- Implementation of technologies that do not involve surveillance.

It is also possible to introduce security measures that pursue enhanced levels of security through surveillance but do not necessarily involve security technologies that lead to massive data gathering and storage. A typical example would be to strengthen police activities such as stepping up local police patrols. Traditional police activities, in effect, also pursue increased security levels through non-technological surveillance. Additionally, schemes such as 'neighbourhood watch' may also be implemented, which work through a redistribution of patrolling activities among the neighbours of residential areas, who check suspicious activities in the vicinity and report them to the local police. Identity checks through the use of precompiled lists of guests in order to regulate access of people into public or private places executed by doormen or security personnel are also examples of security measures that rely on surveillance in order to increase security but do not involve technologies or massive data retrieval.

In a nutshell: approaches to step up surveillance that are not based on technology

- Strengthening traditional police activities.
- Implementing neighbourhood watch programs and the like.
- Employing human gatekeepers i.e. security personnel or doormen.

Finally, there exist ways of addressing security, which pursue higher levels of security not so much through the repression of criminal activities or through threatening deterrence, but rather through a long-term, comprehensive approach capable of addressing the underlying social and economic causes of violence, crime, religious hatred, racism or social discrimination. Once again, security technologies are less effective at addressing these longer-term, more complex human security problems.

Following this broader understanding of security, different policy measures have been proposed, such as establishing better local community relations with the police or involving faith-based or other community groups to manage problems locally in order to increase social trust and cohesion. Increasing the level of social and economic support through active employment policies, training and mentoring opportunities for those who are vulnerable to becoming involved in crime are also, ultimately, security options. Volunteer groups for the

rehabilitation of people with alcohol or drug addiction, the implementation of welcome centres for migrants or the establishment of often self-organised social centres are also examples of local measures to increase social cohesion while at the same time improving levels of security in a given area.

The basic idea of these security approaches is two-fold; on the one hand, it is about active participation by those who are concerned (= the local citizens) in solving conflict, and on the other, it also aims to (re)integrate miscreants or offenders through social community work rather than disciplinary punishment.

Active educational policies oriented towards integration, self-management and respect of mutual diversity may contribute to reduce social, cultural and economic tensions and to improve the sense of belonging to local and national communities indirectly contributing, therefore, to increased security levels.

In a nutshell: approaches that are directed towards societal conditions and mitigation in the long term

- Investing in social means, measures and personnel.
- Fostering active participation of citizens in solving local issues and conflict.
- Establishing better community relations within various stakeholder groups.
- Increasing (economic) support service for employment policies, training opportunities and the like.
- Implementation of welcome centres, neighbourhood centres, social centres.

We have briefly introduced alternative approaches and concepts in this chapter but you might have some other and different ideas of your own as to how security could be improved. Or perhaps you think that Europe's security focus should move away from crime and terror and focus on other priorities.

11 Over to you…

You have now reached the end of the booklet and you can take some time to think and reflect on the issues raised by this magazine.

We have outlined the five security technologies we will be discussing at the citizen meetings. We have explained how they work, how they are used, the security improvements they offer and the issues that arise. We have also explained the context in which these technologies developed: in a Europe that is very concerned about security and where security is part of everyday life. Issues of surveillance and privacy are also prominent because of the amount of personal data that is now used in the security context. Finally, we looked at alternative, non-technological approaches to ensuring security in society.

It is now up to you to consider your opinion on these issues. If these technologies were deployed routinely for security purposes, how acceptable would they be? You might feel that each, in its own way, is effective in increasing security and could potentially reduce crime. But you might also feel that alternative, non-technological solutions might be better. Perhaps you think that more traditional methods featuring trained security personnel or police, rather than extensive information surveillance, should be used. Maybe you think that security is not really a problem and we should not worry too much about it.

Similarly, maybe you feel confident that these technologies are in safe hands because they are employed by government departments that are publicly accountable. Or perhaps you have your doubts as to whether those authorities are able to use such security technologies competently, ethically and with the interests of everyone in society at heart.

Perhaps you feel that the technologies do not really affect you: after all, they are aimed at others who have done wrong and are used in spaces or places that you do not go to. However, you might feel that everyone should be concerned about the issue because of the amount of data the technologies process and because they make everyone a potential suspect. Maybe you are comfortable with the way in which security technologies are used now but concerned about how they may be used in the future.

Whatever you believe, trading a little privacy for some extra security is not a simple decision for everyone. SurPRISE aims to understand the range of views that people hold about new security technologies.

We look forward to seeing you at the citizen meeting in the next few weeks. If you would like to find out more about the project and its partners, please visit the SurPRISE website at http://surprise-project.eu or {include here your national website if you have materials uploaded on it in national language}

‘Privacy related problems are as much political and policy issues as they are legal and technological ones.’

Colin J. Bennett, professor and security expert at Department of Political Science,
University of Victoria, Canada

About this document

This information booklet has been produced to inform citizens taking part in the SurPRISE Project citizen meetings. The publication is provided by the Institute of Technology Assessment (Austrian Academy of Sciences, Strohgasse 45/5, A-1030 Vienna) to all partners in the SurPRISE consortium. Read more about the project and the partners on the SurPRISE website: http://surprise-project.eu/.

The information contained in this booklet comes from reports written by SurPRISE project members, which in turn have drawn upon research and reports written by scientists, policymakers and technologists from all over the world.

This magazine is an extended and re-edited version of the information magazine written by Dr Kirstie Ball (The Open University) in 2013 for the large scale citizen summits held in nine countries in the first three months of 2014.

- Authors: Dr Kirstie Ball, The Open University; Maria Grazia Porcedda and Mathias Vermeulen, EUI; Elvira Santiago and Vincenzo Pavone, CSIC; Regina Berglez, IRKS; Eva Schlehahn, ULD; Márta Szénay, Medián
- Scientific Advisory Board: Dr Monica Areñas Ramiro, Mr Robin Bayley, Professor Colin Bennett, Dr Gloria González Fuster, Dr Ben Hayes, Dr. Majtényi László, Mr Jean Marc Suchier, Ms Nina Tranø, Prof Ole Wæver
- Layout: by Zsolt Bartha, Medián, based on the first magazine prepared by Mr Peter Devine, Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University
- Images: Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University.
  page 11: Vision Systems, http://www. vision-systems.co.nz/assets/Video-Analytics1.jpg
  page 14 Mat Wellington, “Police Use QuadCopter – UK” March 23rd 2011, http://multirotor-news.com/2011/03/23/
  page 21 © iStockPhoto.com / alexsl,
  page 23 Senseable City Lab, Massachusetts Institute of Technology
  page 25 © KIVI NIRIA DV, 2011
- The SurPRISE project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492
- This publication is available on: http://surprise-project.eu

Project Partners

- Institut fur Technikfolgen-Abschatzung/Osterreichische Akademie der Wissenschaften,
- Coordinator, Austria (ITA/OEAW)
- Agencia de Proteccion de Datos de la Comunidad de Madrid*, Spain (APDCM)
- Instituto de Politicas y Bienes Publicos/Agencia Estatal Consejo Superior de Investigaciones
- Cientificas, Spain (CSIC)
- Teknologiradet - The Danish Board of Technology Foundation, Denmark (DBT)
- European University Institute, Italy (EUI)
- Verein fur Rechts-und Kriminalsoziologie, Austria (IRKS)
- Median Opinion and Market Research Limited Company, Hungary (Median)
- Teknologiradet - The Norwegian Board of Technology, Norway (NBT)
- The Open University, United Kingdom (OU)
- TA-SWISS/Akademien der Wissenschaften Schweiz, Switzerland (TA-SWISS)
- Unabhangiges Landeszentrum fur Datenschutz, Schleswig-Holstein/Germany (ULD)

* APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe.

surprise
surveillance
privacy
security