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

Project acronym: **SurPRISE**

Collaborative Project

Grant Agreement No.: 285492

FP7 Call Topic: SEC-2011.6.5-2: The Relationship Between Human Privacy And Security

Start of project: February 2012

Duration: 36 Months

D 4.3 – Information material and documentary films

Lead Beneficiary: OU

Author: Kirstie Ball (OU)

Due Date: September 2013

Submission Date: October 2013

Dissemination Level: Public

Version: 1

This document was developed by the SurPRISE project (http://www.surprise-project.eu), co-funded within the Seventh Framework Program (FP7). SurPRISE re-examines the relationship between security and privacy. SurPRISE will provide new insights into the relation between surveillance, privacy and security, taking into account the European citizens' perspective as a central element. It will also explore options for less privacy infringing security technologies and for non-surveillance oriented security solutions, aiming at better informed debates of security policies.

The SurPRISE project is conducted by a consortium consisting of the following partners:

Institut für Technikfolgen-Abschätzung / Oesterreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM	
Instituto de Politicas y Bienes Publicos/ Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	CSIC	
Teknologirådet - The Danish Board of Technology Foundation, Denmark	DBT	
European University Institute, Italy	EUI	
Verein für Rechts-und Kriminalsoziologie, Austria	IRKS	
Median Opinion and Market Research Limited Company, Hungary	Median	
Teknologirådet - The Norwegian Board of Technology, Norway	NBT	
The Open University, United Kingdom	OU	
TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland	TA-SWISS	
Unabhängiges Landeszentrum für Datenschutz, 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.

Table of Contents

1. Introduction

This deliverable presents the information material to be used in the citizen summits. Two elements of information material are presented. The first, an information magazine, will be used to inform citizens about the context of the study as well as the different Surveillance-Oriented Security Technologies (SOSTs) which will be examined at the summits, before they arrive at the events. The magazine will be sent to citizens when they are recruited to the summits. The second, three films about different SOSTs, will be used during the summits themselves. The films will bring the debates around the SOSTs to life, and will be used to stimulate discussion during the summits. In the following pages, the development process for each element will be described.

2. Information magazine

The English version of the information magazine is presented in an appendix to this document. The structure and content of the magazine was conceived and drafted by Kirstie Ball of the Open University (OU). As the document was specifically designed to engage the public, existing expertise in accessible scientific writing, a style typically found in the Open University's teaching material, was deployed. The magazine explains the core concepts of the study: Surveillance, Privacy and Security, illustrating them with a short story and plenty of real world examples. It then goes on to describe the function, benefits, limitations and discussion points which surround the use of each technology. Resources from academic, legal and journalistic publications informed the content of the magazine. However the interviews which form the backbone of the films were also drawn upon. The content was proof-read and edited by a professional magazine editor at the Open University.

The document progressed through four rounds of internal review and three rounds of piloting with citizens, before its final content was defined. The document was then converted into a magazine by graphic designers from the Open University's Corporate Learning and Teaching team. The graphic design element of the magazine was subject to a similar review process. The text was made available for translation in June 2013 and the graphic design files were made available to partners, so that they could produce versions in their own language, in July 2013. The information material is currently in a final round of external view with the advisory board, no significant changes are anticipated.

3. Films

Three films were produced for use in the citizen summits. Production began in December 2012 where a tender was issued to a shortlist of film production companies drawn up in collaboration with the Broadcast Unit of the Open University. The tender was issued in January 2013 with a submission deadline of 18th February 2013. Four tenders were received and were independently evaluated by partners OU, ITA and DBT using a score sheet based on the criteria stipulated in the tender document. A decision was made on the 27th February 2013 to appoint the company Two Cats Can to produce the films and production began on the 1st March 2013. Two Cats Can are a small company with many years of producing television for the BBC and The Open University, including films which were to be used in a research setting.

Although films are a central element of the citizen summit method, their efficacy as a stimulus in social scientific research is worth noting. The use of films, or 'video vignettes' are appropriate in settings where difficult situations, extreme emotions or questions of ethics or human rights are being considered. These are situations which might harm the research participant if they were exposed to such things in the real world[1]. They also help to bring abstract concepts, such as surveillance, privacy and security to life. In spite of their simulated nature, reactions to video vignettes compare favourably with observed reactions to similar phenomena when experienced first-hand[2]. An iterative, theory and research question driven approach was taken to their production, drawing largely on the work of Johnson (2000)[3]

Drawing primarily on the information magazine, and on its collective knowledge and experience, the consortium collaborated to design the shooting scripts of each film. Following Johnson (2000) issues highlighted by the research model, defined in D4.1, were included. In parallel, experts from industry, regulatory bodies, campaign organizations and academia were interviewed on camera about the uses, benefits and limitations of each SOST. Each interviewee was asked a schedule of questions derived from the research model. Twelve interviews of approximately an hour each were conducted.

The work package leader conducted a content analysis of each interview, distilling the possible content of each film and its respective subsections. The film makers then edited potential material from the raw interviews. Five separate rounds of editing took place, reducing the films from 1hr 45mins in length, down to 20 minutes and finally to the 6 minute versions which are to be used in the summits. When the edits were 20 minutes long, the scripts and raw interviews (without background images) were shared with the consortium who recommended which bits were to stay in and which were to be cut. The consortium also recommended a voice-over introduction rather than interviews which was provided by the work package leader. Once the final narrative had been defined, images were added and copyright clearances were obtained. Due to difficulties with obtaining BBC footage, iStockvideo provided the main moving image content. Collaboration with ADDPRIV FP7 partner Kingston University produced the Smart CCTV system images used in the Smart CCTV film. Four production meetings between the work package leader and film makers defined the near-final versions of the films which were piloted in the UK, Hungary and Denmark. It was decided by the consortium that voice over and subtitling be provided for each film in each relevant language. The production of the sound tracks which will be programmed onto the films by Two Cats Can has been subcontracted. The films are currently in a final round of external view with the advisory board and no further changes are anticipated. The following pages contain screen shots from the films.

---

[1] Caro F.G. et al (2012) Choosing among residential options: The results of a vignette experiment. *Research on Aging* 34 (1) 3 – 33

[2] Eifler, S. 2007. "Evaluating the Validity of Self-reported Deviant Behavior Using Vignette Analyses." *Quality & Quantity* 41:303-18.

[3] Johnson, B (2000) Using video vignettes to evaluate children's personal safety knowledge: methodological and ethical issues *Child Abuse and Neglect* 24 (6) 811 – 827

4. Sreenshots

4.1 Smart CCTV

Title page

Farooq Nazir, Benefits

Nick Pickles, Benefits

Smart CCTV system footage

James Orwell, Limitations

Gus Hosein, Limitations

Eva Schlehahn, Limitations

Final screen

4.2 Deep Packet Inspection

Title page

Michael Blakemore, Benefits

DPI Benefits

US based email services and DPI

Eva Schlehahn, Limitations

Tom Ilube, Discussion Points

Gus Hosein, Discussion Points

4.3 Phone Location Tracking

Title page

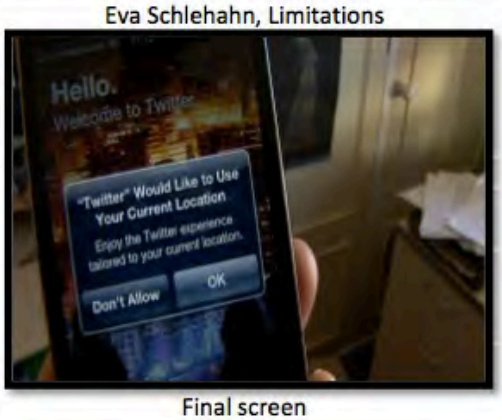
Gus Hosein, Benefits

Sally Dibb, Open University, Benefits

GPS Satellite and Smart Phone fade

Eva Schlehahn, Limitations

Martin Scheinin, Discussion points



Final screen

5. References

Caro F.G. et al (2012) Choosing among residential options: The results of a vignette experiment. *Research on Aging* 34 (1) 3 – 33

Eifler, S. 2007. "Evaluating the Validity of Self-reported Deviant Behavior Using Vignette Analyses." *Quality & Quantity* 41:303-18.

Johnson, B (2000) Using video vignettes to evaluate children's personal safety knowledge: methodological and ethical issues *Child Abuse and Neglect* 24 (6) 811 – 827

6. Appendix : Information Magazine

Surveillance, Privacy and Security

WHAT'S YOUR VIEW?

surprise
surveillance
privacy
security

SEVENTH FRAMEWORK PROGRAMME

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 rely on the surveillance of people and what they are doing. They are used by police or security personnel to monitor what is going on to make sure that nothing is wrong. 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 we need 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 feel safe and feel secure. When you attend the SurPRISE citizen summit you can share your views on new security technologies with fellow citizens. SurPRISE will gather citizens' views on new security technologies and share them with the European Commission.

Citizen summits are taking place in nine European countries: as well as in the UK, citizens in Austria, Denmark, Germany, Hungary, Italy, Norway, Spain and Switzerland are taking part. The results of the summits will be delivered to the European Union in June 2014 and will be made publicly available to the media, government and citizens.

This booklet provides basic information on the issues that will be discussed at the British SurPRISE summit in March 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.

We know that reading this booklet will be challenging. You don't have to understand every word written in it before you turn up at the citizen summit. We're not going to be testing how much you know and we're not trying to make you an expert! The aim of the booklet is to give you an idea of what issues will be discussed at the citizen summit and to start you thinking about your personal views when it comes to surveillance, privacy and security. Your participation in the citizen summit is important exactly because you are not an expert. We have asked you to take part because you are an ordinary European citizen whose everyday life is affected by the decisions made by European politicians and those in your own country.

SurPRISE will provide representatives and other decision-makers with your opinions: the views of the citizens. Security technologies relate to human rights, issues of justice and fairness, the development of civil society and of trustworthy and effective institutions. This is why debates should involve the general public, not just policymakers, industries, experts and charities. 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!

1.1 How to read this booklet

This booklet has five main sections. The first is a general introduction to surveillance, security and privacy in Europe and how everyday citizens are affected by the issues that arise. Three further sections outline the three security technologies we will be discussing at the citizen summit. Each section describes why the technology was developed, how it is used, the security improvements it offers and its limitations. We have included an information box within each technology section that explains how the security technology works. The fifth section briefly discusses some alternatives to security technologies.

If you don't want to read the whole document, we have provided a summary of the main points.

2 Summary

SurPRISE aims to understand the range of views that European citizens hold about new security technologies. As European governments have become more concerned about terrorism, organised crime and cybercrime, they have invested in the development of new security technologies.

Many of 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.

Because these technologies use personal information, we call them '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.

In the SurPRISE citizen summit we will be examining three 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 identify people, analyse their behaviour and detect objects.
- **Cyber surveillance using deep packet inspection:** Using hardware devices and special software, messages transmitted over the internet can be read in case their contents (e.g. words and images) contain references to serious crimes such as terrorism or holocaust denial, or use computers to commit serious crime such as the distribution of child pornography.
- **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 by global positioning systems (GPS) or wireless data, and data from the mobile phone masts to which it has connected.

Each technology improves security by identifying suspects and criminal or illegal activities. They can also make life much more convenient. But each security technology has a set of drawbacks. For example, smart CCTV works only in certain conditions and can produce a lot of 'false alarms'. Deep packet inspection completely destroys 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. A lack of control over the collection and use of information is an issue associated with all the technologies we examine.

In spite of the 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. But maybe people's opinions also differ depending on what they believe about a number of other issues, for example:

- Do the technologies actually work?
- How intrusive are they?
- Are the institutions using them trustworthy?
- Is there enough effective legal regulation?
- What are the alternatives and are they practical?

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

If you would like to know more about these issues, please read on.

3 Just an ordinary day…

Just south of Budapest, Aisha joins European Route E-75 to Budapest International Airport. She recalls the first time she used this route. Then, she paid the road toll on the spot: now, the toll is automatically charged to her bank account. Her car's registration plate is read by automatic number plate recognition (ANPR) cameras and the road toll system does the rest. Previously Aisha didn't notice the overhead cameras. Now she sees them and wonders how the information connects to her bank.

Aisha parks her car and boards the shuttle bus to the terminal. There, she checks in to her flight using a self-service check-in machine. She places her passport on the machine and it matches her name to her booking details. As Aisha receives her boarding pass, she realises that information about her is stored somewhere in there as well.

As she approaches airport security Aisha begins to think more about her information and where it goes. She watches carefully as the Hungarian immigration inspector scans her passport through another machine. She is waved through and heads for the security check.

Once through security Aisha flops down her hand luggage in the coffee shop. She orders a coffee, but again pauses before handing her debit card to the cashier. 'Very handy plastic' she thinks, 'but who records that transaction and why?'

While Aisha waits for her coffee to cool she pulls out her smartphone to check for messages. As the screen flickers into life, the location displayed on the phone's home screen immediately changes from 'Kecskemét', where Aisha lives, to 'Ferihegy'. 'How did it know that? There must be a really obvious explanation, but I can't think of one' she ponders.

Aisha just has time to send an email to a work colleague before it is time to board the plane. As she switches her phone to flight mode, she wonders what will happen to the email on its way through the internet.

Aisha's trip is not unusual. These represent familiar events in the life of any traveller. The technologies offer benefits to Aisha by making travel more convenient and efficient. But they also raise some questions in her mind: 'Who uses my personal information and what does it mean for me that they are "in the system"?'

Many of the technologies Aisha encounters also feature outside the world of the airport. Plenty of people could not imagine life without their smartphones, debit cards or the internet! In fact, many daily activities generate the kinds of electronic record of which Aisha becomes aware. Perhaps you have the same questions in your mind as she does. 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 can indicate 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 billing databases. Because of this it is possible to identify, track and trace most people at different points in their lives. It is perhaps this which causes Aisha to be concerned, but she is also torn because of the benefits these technologies offer.

Technologies like the ones discussed above and the information they collect can offer benefits 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 deploying new security technologies not only it will be possible to arrest wrongdoers, it will also be possible to identify them before they commit harm. Because the 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.

If Aisha were to consider that her information could be used in this way would she still be torn? If it meant better security for her and everyone else, perhaps it would be something she could accept. However, the use of these technologies raises issues about human rights, privacy, regulation and trust. These technologies sometimes collect and share information about a person without their knowledge. Data about innocent people are inevitably captured and analysed, and in the case of some technologies, deliberately so. As such they have the potential to invade privacy, which in Europe is a fundamental human right.

A number of other questions arise:

- Are the institutions using the data trustworthy?
- How well regulated are the institutions who use the data?
- Are the technologies used in ways that comply with the law?
- Are the institutions transparent and accountable for any privacy infringements done in the name of security?
- Do these technologies really improve security?

These are some of the questions we will be examining at the citizen summit.

In the next few paragraphs we will introduce some of the key terms and definitions before describing the three technologies that we will look at during the summit.

3.1 Surveillance, privacy and security

3.1.1 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 to spot wrongdoers in local streets. Surveillance can also be for commercial purposes. For example, a supermarket might use loyalty cards to understand what different groups of customers prefer to buy. This then influences what special offers are made to

those customers in future. Surveillance can be used to prevent crime and catch criminals, but it is also used to provide people with products and services. In fact, it's one of the main principles behind how modern society is organised and run.

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 to be in control of a surveillance technology bestows great power. It is important that those who are in such positions, such as law enforcement agencies 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.

3.1.2 Privacy and data protection: important issues?

One of the main issues that hangs in the balance is privacy and the protection of the data that new security technologies generate and use. 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, 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.

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 due to privacy concerns they disclosed only very selective information about themselves. People still want to share information, but want to do so within an established boundary, and it is this boundary that indicates where privacy begins.

> 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 is a fundamental human right in Europe. Everyone needs their 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'.

3.1.3 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 isn't 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 true for those who govern security as well. 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 companies, such as Airbus, BEA Systems and Finmeccanica, and a lot of smaller companies too. Recent developments in surveillance-oriented security technologies include:

> smart CCTV, which focuses on spotting known offenders and identifying suspicious behaviour before a crime has been committed

> 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'

> 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 Three new security technologies

The three security technologies we'll be discussing during the citizen summit are:

> **Smart CCTV**

> **Cyber surveillance by deep packet inspection**

> **Smartphone location tracking**

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 how 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 summit you will be given many opportunities to voice your opinion, but in particular we would 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?

> 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 your civil liberties?

> 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 in your opinion?

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 doesn't bother you. Perhaps you are OK with security technology now, but are concerned about its use in the future.

5 Smart CCTV

Earlier in this booklet, we described how Aisha, on her trip to the airport, wondered how the cameras that collected her road toll worked. The cameras were automatic number plate recognition or ANPR cameras. ANPR cameras are an example of a new security technology called 'smart CCTV'.

Most Europeans are familiar with the idea of a CCTV system. 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. It was then adopted by police in the USA and the UK in the 1960s. Use of CCTV grew steadily throughout Europe in the 1990s, with the UK leading the way and France and the Netherlands close behind. It never seems to be far from the news. In 2013 CCTV systems in Boston were crucial in identifying those responsible for the Boston marathon bombing.

Smart 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

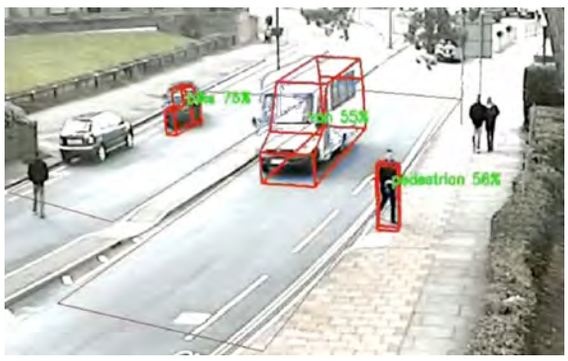
> identify a person's face when the face appears against a plain, uncluttered background. To identify the person that picture is compared with images held in a database of known individuals

> 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.



Not all smart CCTV systems are the same, however. 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.

How smart CCTV works

Smart CCTV records and analyses events in a scene as they happen. It alerts the operator to anything that is out of the ordinary. 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 '3megapixels', each image it captures is made up of 3 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.

Smart CCTV can also compile stored images that are relevant. It can begin collating footage from a particular camera and from nearby cameras from the minutes before a crime began unfolding. For example, because the software can be programmed to recognise particular clothing, smart CCTV cameras can follow a person suspected of criminal activity so police could track a criminal after the fact. It cannot yet do this in real time, however.

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.

In Budapest at the end of 2012, the police started to use smart CCTV cameras for observing bus lanes. The police can use the images lawfully as long as passengers are not filmed and the public are fully informed. Facial recognition cameras have been in place at Zürich Airport since 2003. At the time, it was the first ever use of facial recognition in the context of border controls. This system is now permanently installed.

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.

There are varying views on smart CCTV 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. In Britain ANPR has also been used to enforce road tolls in London, but by contrast it is now integrated into both national and local policing strategies. Since 2010, 5000 ANPR cameras have been installed in the UK, with the police national data centre reading between 10 and 14 million ANPR records each day.

Controversy around smart CCTV: ANPR in Birmingham, UK

In 2011, the British police in Birmingham, UK had to remove ANPR cameras from three areas of the city that had a high Muslim population. The cameras were funded under an anti-terrorism programme called 'Project Champion' but the cameras were promoted to the public on safety grounds. Community leaders and local members of parliament strongly objected to the cameras and community relations were damaged. Two hundred cameras were installed but were never switched on. Sixty-four of the cameras were covert and were put up without public consultation. The cameras were either destroyed or used by other UK police forces. The project's failure and the loss of the cameras cost the police £300,000 (€351,414).

5.3 Security improvements

Smart CCTV can improve security in the following ways.

1. 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.
2. 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.

1. The smart CCTV algorithms currently in use have a number of 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, the public know 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.

2. 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. To counteract this, smart CCTV should always be deployed in a limited way to counteract a very specific threat.

   > 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 the surveillance.

   > It may affect freedom of expression if the public realise that their behaviour in public spaces is being monitored by this combination of software and people.

3. 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 have to be very careful whom they recruit to work with the systems and train them well. They need to very closely regulate the types of search being undertaken and safeguard against the misuse of data.

4. Records are created about what has happened at many places and times. That information could be used for purposes which were never intended and may have little or nothing to do with security.

There needs to be transparency as to why smart CCTV systems are in place. People should be entitled to contact the manager of the system to ask about its use. They need to feel that the camera is there for a good reason and they need to be confident in its use.

Chris Tomlinson, Independent Security Consultant

6 Cyber surveillance by deep packet inspection

As she was sitting in the airport coffee shop, Aisha wondered what would happen to the email she sent to her colleague as it travelled through the internet. It may well have encountered a cyber-surveillance technique called '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 read 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, to whom you communicate with via email, instant messaging or social media. DPI applications work by detecting and shaping how messages travel on a network. They open and analyse messages as they travel, identifying those that may pose particular risks. You don't 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.

6.1 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.

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's from and where it's 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', similar 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.

Deep packet inspection takes place in 'routers'. A router is a computer that directs messages around the different networks that make up the internet. 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. It is the companies who own the routers who have pioneered the technology that does deep packet inspection. Of course the 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 a now a market for DPI technology.

6.2 How deep packet inspection is used

In Europe DPI can help internet companies prevent software viruses and malware damaging their networks. Its use to detect very specific crimes, such as the distribution of child pornography, is possible but it's also legally controversial. This is because the European law on communications interception was drawn up at a time when DPI did not exist. This law allows the 'filtering' of internet traffic. While DPI does 'filter' internet traffic, sifting through it for illegal content, it goes much further than that by analysing all the content of online communications. At the moment a judge may order that DPI can take place as long as it is appropriate

for the kind of crime being investigated.

Deep packet inspection is not allowed to take place in Europe if communications data are used by companies to target advertising or by governments to block politically sensitive content. DPI may not be used indiscriminately as European data protection law prohibits the surveillance of communications without the sender's or receiver's consent. 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.

How DPI can be detected, limited or controlled is something of a grey area. Regulation is desperately 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. DPI generates further information, which can be shared between internet service providers and governments, and it is difficult to know what happens to the results of DPI searches. 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 five reported uses of DPI: three are commercial and two relate to public and national safety.

6.2.1 Commercial uses

- **Network security:** Messages are inspected to make sure they do not contain errors or viruses.
- **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 and copyright infringement.

Controversy with deep packet inspection: Phorm and consumer data in the UK

In 2008, a US company called Phorm attempted to launch a system in the UK with telecoms providers British Telecom, Virgin Media and TalkTalk. Phorm used DPI to intercept users' web surfing habits as they surfed. It then analysed the data before selling it to advertisers. The service providers told users that the measures combatted cybercrime but did not reveal that they were using the information for advertising. British Telecom conducted stealth trials of the technology and made over 18 million interceptions. British consumers found out about it and protested because data had been processed without their consent. Eventually Phorm technology was dropped by all the service providers. The European Commission then began legal action against the British government for permitting the service to operate. The case was closed in January 2012, after the UK amended its laws to include a sanction on unlawful interception of communications.

6.2.2 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 (and may be unlawful). 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 goes on within Europe too.

6.3 Security improvements

Deep packet inspection can improve security by identifying and blocking harmful, damaging or criminal messages; for example:

- messages that distribute child pornography
- messages that contain hate-speech or hate-crime
- messages that contain viruses or other forms of cybercrime
- messages that relate to the perpetration of serious organised crime or terrorism.

6.4 Issues

Deep packet inspection raises the following serious issues:

1. DPI is all-seeing.
   - It can analyse all messages and the sensitive data they may contain as they travel, which means that under DPI electronic communications are no longer private.
   - 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.
   - There is currently no accountability or recourse if DPI is misused.
   - As computers identify only potentially problematic messages there is an issue of incorrect interpretation and innocent people becoming suspects.
   - DPI's use needs to be very tightly regulated because of its huge power.

2. 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 efficient running of computer networks 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.

3. 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.

   > A 'DPI regulator' would need to be a truly international body with sufficient power to punish offenders.

Many of the companies that use DPI are located outside Europe but analyse data about European citizens. Because of this they cannot be told not to do it.

Eva Schlehahn, Independent Privacy Protection Authority, Schleswig Holstein

7 Smartphone location tracking

When Aisha turned on her smartphone, she noticed that the home screen indicated that its location had changed. She was sure that there would be an obvious explanation behind it. In fact, all kinds of mobile phone need to know their location in order to work. Smartphones take this to a whole new level.

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 weren't available until the early 1990s.

7.1 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. You may remember in the mid-1990s that many more masts started appearing. There was a lot of public debate about the position of the unsightly phone masts and health concerns over increased radiation levels.

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. A phone's location is always recorded by the mast to which it is connected. 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 can be tracked by the telecommunications provider. 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 are probably the one smartphone feature that will grow in use in the coming years.

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 enables the creation of a phone use package that suits the user's needs and the generation of a phone bill. 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 a number of different masts, 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. 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.

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 tried to get hold of the records for six months of his mobile phone's location data, he had to take the phone company to court to get the information. When he first received the data, it 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'd 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 combined with information from social media such as Twitter or Facebook.

In a recent US Supreme Court case, United States v. Jones, 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'.

7.2 How smartphone location tracking is used

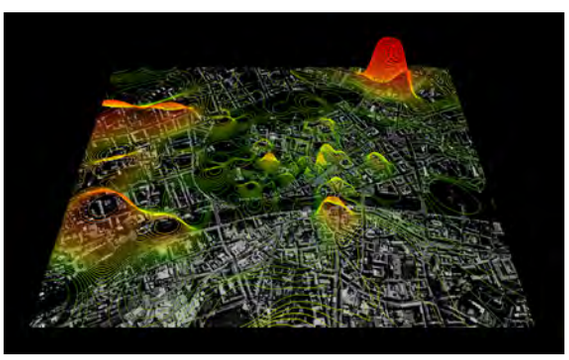
There are both commercial and security uses of smartphone location data.

7.2.1 Commercial uses

> **Phone bill administration:** Mobile phone companies need location data as well as the phone's identification number to generate a phone bill. The companies also use the data to design phone usage tariffs to suit the needs of different customers.

> **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 times worldwide. Users were surprised to find that its Finnish developers, Rovio Entertainment Ltd, routinely collected and sold the location data of players. Fifty per cent of all apps collect location data even when the app doesn't 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.



7.2.2 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 data protection 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. Using *Silent SMS*, a service provider can text message (SMS) a mobile phone without the knowledge of its owner and can then download information from mobile phone masts that will reveal the phone's location.

> **Tracking family members:** Individuals may also benefit from location-based services. Many parents will be familiar with individual mobile-phone-tracking products, which enable them to see where their children are at all times, for example.

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.

7.3 Security improvements

Smartphone location tracking improves security in a number of ways:

1. It enables those in risky situations to be found and helped.

2. It enables vulnerable adults or children to be monitored by their families.

3. 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.

7.4 Issues

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

1. 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.

2. Some apps collect location data even if the app does not need it to run. In the absence of strong public pressure, companies are unlikely to give consumers better control of location data.

3. 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 is based.

4. 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.

5. 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.

Smartphone location tracking empowers people as much as it surveils people. It can deliver a lot of services and can improve social relationships … but the location data sharing preferences aren't always that obvious or that easy to manipulate.

Gus Hosein, Privacy International

8 Is 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. This is partly the case but it is not the whole story.

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 again, security technologies are less effective at addressing these longer-term, more complex security problems.

So, while security technologies are used to find criminals and terrorists and second-guess their next moves, there are other solutions too.

8.1 Local solutions

> Promoting a safer built environment, through improved street lighting, emergency public telephones and an improved police presence

> Establishing better local community relations with police, through community crime prevention measures

> Having faith-based or other community groups manage problems locally so that social trust is increased

> Having transparent and accountable local governance and policing

> Having plenty of employment, training and mentoring opportunities for those who are vulnerable to becoming involved in crime.

8.2 National or international solutions

> Promoting fair global systems of trade, aid and debt relief

> Improving disaster response infrastructures and resources

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

> Using sustainable and alternative energy sources more effectively.

9 Over to you…

We hope that you aren't feeling too overwhelmed with information at this point! The good news is that you have now reached the end of the booklet and you can take some time to think and reflect on the issues we've raised.

We have outlined the three security technologies we will be discussing at the citizen summit. 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. Maybe you think that security isn't really a problem and we shouldn't worry too much about it.

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

Perhaps you feel that the technologies don't 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 how 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 isn't 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 summit 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**.

About this document

This information booklet has been produced to inform citizens taking part in the SurPRISE Project citizen summits. 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.

The SurPRISE Project is co-funded within the Seventh Framework Program (FP7). SurPRISE re-examines the relationship between security and privacy. SurPRISE will provide new insights into the relation between surveillance, privacy and security, taking into account the European citizens' perspective as a central element. It will also explore options for less privacy infringing security technologies and for non-surveillance oriented security solutions, aiming at better informed debates of security policies.

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.

> **Author:** Dr Kirstie Ball, The Open University

> **Scientific Advisory Board:** Dr Monica Areñas, Professor Colin Bennett, Dr Gloria González Fuster, Dr Ben Hayes, Dr Majtényi László, Mr Jean Marc Suchier, Ms Nina Tranø, Prof Ole Wæver

> **Layout:** Mr Peter Devine, Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University; Mr Jaro Sterbik-Lamina, Institute of Technology Assessment, Austrian Academy of Sciences

> **Images:** Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University.
Page 17 © iStockPhoto.com / EdStock, page 28 © iStockPhoto.com / dpmike, page 29 © iStockPhoto.com / alexsl, page 30 Senseable City Lab, Massachusetts Institute of Technology.

> **SurPRISE sponsors:** European Commission Framework 7 Programme, project no. 285492

> **This publication is available on:** http://surprise-project.eu

> **How this document was produced:** This information booklet was written by Kirstie Ball in close cooperation with the Danish Board of Technology Foundation, the SurPRISE consortium and its Advisory Board. The booklet underwent four rounds of internal review, one round of external review and was then pilot tested with groups in Denmark, Hungary and the UK.

Project Partners

> Institut für Technikfolgen-Abschätzung/Österreichische Akademie der Wissenschaften, Coordinator, Austria (ITA/OEAW)

> Agencia de Protección de Datos de la Comunidad de Madrid*, Spain (APDCM)

> Instituto de Politicas y Bienes Publicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain (CSIC)

> Teknologirådet - The Danish Board of Technology Foundation, Denmark (DBT)

> European University Institute, Italy (EUI)

> Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)

> Median Opinion and Market Research Limited Company, Hungary (Median)

> Teknologirådet - The Norwegian Board of Technology, Norway (NBT)

> The Open University, United Kingdom (OU)

> TA-SWISS/Akademien der Wissenschaften Schweiz, Switzerland (TA-SWISS)

> Unabhängiges Landeszentrum für 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.

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

SEVENTH FRAMEWORK
PROGRAMME