Scalable Measures for Automated Recognition Technologies

Rapports

Informations projet

SMART

N° de convention de subvention: 261727

Site Web du projet

Projet clôturé

Date de début
1 Juin 2011

Date de fin
31 Mai 2014

Financé au titre de
Specific Programme "Cooperation": Security

Coût total
€ 4 191 066,60

Contribution de l'UE
€ 3 456 017,35

Coordonné par
UNIVERSITA TA MALTA
Malta

Final Report Summary - SMART (Scalable Measures for Automated Recognition Technologies)

Executive Summary:
The SMART project examines the social and legal consequences of adoption of automated, 'smart surveillance' systems by public bodies. Smart surveillance is technology that moves beyond reactive investigations to more pro-active responses in order to automatically respond to security incidents and threats as they happen. Smart surveillance technologies involve computerised on-line and off-line data processing to provide the collection of intelligence and/or security decision-making support.

Automated recognition of individuals and/or pre-determined traits or risk factors/criteria lies at the basis, indeed is the very raison d'être, of smart surveillance systems. Yet current EU regulations, and specifically

those on information sharing between police and security forces, explicitly prohibit automated decision-taking regarding individuals unless “authorised by a law which also lays down measures to safeguard the data subject’s legitimate interests” (Article 7, Council Framework Decision (CFD)2008/977/JHA). Where are these laws, what can these measures be and what else should the laws contain? Can the laws be technology-neutral but sector specific, thus permitting a measured approach to the appropriateness of smart surveillance technologies in key security applications? Can they be extended to all security applications of smart surveillance, even those not covered by CFD 2008/977/JHA or the proposed directive set to replace it?

This project examines these and other questions through a comprehensive approach which combines a technical review of key application areas by sector with a review of existing pertinent legislation to then produce a set of guidelines and a model law compliant with CFD 2008/977/JHA and EU Directive 95/46/EC and the proposed successor legislation. The project first focuses on a status quo analysis of technology currently deployed today in five key research areas: (i) border control (ii) crowd-control & counter terrorism (iii) mobile devices (iv) e-government and (v) cyberspace. This analysis is supplemented by a concurrent overview of the legal context within Europe, on a national and European level as well as a synopsis of the technological architecture and data-sharing regime in place. The project continues with evaluating current citizen sentiment in relation to these instances of surveillance through focus groups carried out throughout Europe. This gives the project a unique insight into potential geographic divergences and convergences of sentiment.

Having thus identified appropriate instances of application as well as a number of technical, procedural and legal options for safeguards, the project moves on to create a tool-kit which would be useful to for policy-makers, police and security forces across Europe (and hopefully beyond). The SMART project brings to bear significant EU-wide expertise in data protection legislation in order to prepare a draft model law which would contain a number of measures providing adequate safeguards for the data subject and thus rendering use of smart surveillance compliant with CFD 2008/977/JHA and its proposed successor and other applicable regulations.

Project Context and Objectives:
Project context

SMART project assesses the use of automated decision-taking as part of “smart surveillance” technologies in a society where privacy and data protection are fundamental rights. The risks and opportunities inherent to the use of smart surveillance were evaluated and a number of technical, procedural and legal options for safeguards of individuals fundamental rights and freedoms have been developed. The end product of SMART concludes by creating a toolkit, including a model law, which would inform policy makers and police forces and security services across Europe and beyond.

A key change in societal trends over the past twenty years has been the ubiquity of technological surveillance measures in an attempt to assist in the prevention and detection of crime in general and terrorism in particular. CCTV initially designed to enable scientists to observe rocket launches from a safe distance is today employed almost anywhere in public and private spaces, from observing crime-prone

areas to domestic settings where children in their playroom can be supervised from another room. While citizens gradually became accustomed to, if not always entirely accepting of, surveillance technologies, particularly CCTV, in public spaces, the move from analogue to digital technology over the past 10-15 years has produced new capabilities that police and security services are keen to use in their fight against crime. The digitisation of image capture and storage has facilitated the processing of those images in the interests of crime deterrence and detection. Furthermore, the move from analogue to digital has made it possible to move from surveillance to “smart surveillance”.

Automated recognition of individuals and/or pre-determined traits or risk factors/criteria lies at the basis of smart surveillance techniques. The proliferation of video surveillance devices led to realisation that producing billions of images every day in, say, London is quite useless if one does not have the ability to analyse those images. To counter this problem, leading police forces, like the London Metropolitan Police, have set up special units with specially trained officers to be able to make better use of the available technology. However, no amount of special units is enough to analyse the billions of images captured daily. This is the context where the notion of smart surveillance becomes attractive to law enforcement agencies: If one could somehow harness computer technology to analyse the images (and other sensor data) available with a view to flagging up pre-identified risk-related situations or individuals, then the paucity of human and financial resources could somehow be offset by “smart technology”.

Increase in availability and deployment of ‘smart’ technologies
During the course of the project, one has noted an increase in availability and deployment of smart technologies. Not only is there an increase in smart technologies but, if one is allowed to put it this way, these smart technologies are increasingly becoming ‘smarter’ – have greater capacity to store information and have stronger processing power, often in smaller technical equipment. If one were to look even at a smart phone that is currently in use one would see that it, as the Supreme Court noted in Riley v. California, “has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos.” [1]

Furthermore, as noted by Cannataci [2], the quantity of data which is being generated and which may need to be analysed is increasing exponentially and has in many cases already reached levels where human analysis of that data in the first instance is impossible without the assistance of smart tools. This increase in both supply of and demand for smart surveillance systems makes it even more relevant to reflect on issues of proportionality and necessity, both of which were discussed extensively during the course of the project.

Disclosures on state practices
Smart surveillance technologies have had added attention following recent disclosures on state practices. In June 2013, former systems administrator for the Central Intelligence Agency (CIA) and a counterintelligence trainer at the Defense Intelligence Agency (DIA), Edward Snowden published in international media thousands of classified documents that he acquired while working as an NSA contractor for Dell and Booz Allen Hamilton revealing widespread surveillance of telecommunications traffic and content without clear legal basis.[3]

Shocking as they have been, the revelations are to some extent a confirmation of suspicions many

researchers have had and now are confirmed that intelligence agencies have been using mass surveillance techniques without a clear process of review and accountability that is expected in any democratic state governed by the rule of law.

Following these revelations industry [4], civil society and in Europe, the European Parliament [5] are pushing for reforms of government surveillance and requesting greater transparency in the activities of secret services/intelligence agencies.

For the SMART project, these revelations have helped to encourage debate questioning the previously 'water-tight' distinction in legal treatment (and application of laws) to law enforcement and security services/intelligence agencies. It becomes more and more obvious that the distinction is less water-tight then has been portrayed so far (and which is furiously fought over especially by security services/intelligence agencies). As Cannataci argues:
"In many states SIS [Security and Intelligence Services] do not have executive powers, although there do exist a few exceptions especially in the case of anti-terrorist activities. In most cases however the prime function of the SIS is to produce "actionable intelligence" which is then passed on to the LEAs to take action about whether it is to further monitor, follow, detain, arrest or prosecute a person or group of persons. This fact about the practices of LEAs and SIS raises two important considerations especially in the light of the Snowden revelations: a) does it make sense to have a strict data protection regime covering the collection and use of personal data by the police and then have a much "lighter-touch" regime for the SIS if the SIS are then going to give the results of their findings to the police?" [6]

Law enforcement activities have been always more accurately and minutely scrutinized, given that in criminal procedures, evidence illegally obtained by the police can be struck out or disregarded by a court. While it is important that one recognises the differences in mission of both law enforcement and security services/intelligence agencies, both need to be subject to a legal framework which respects the aims of the work both are responsible for and the rights of individuals subject to surveillance, including by smart surveillance technologies.

Legal Developments that influenced the project
• The European Commission proposals for the reform of the data protection framework
In January 2012, eight months into the SMART project, the European Commission presented two important proposals aimed at reforming the current data protection framework. The Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012) 11 Final) is meant to replace the current Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23/11/1995 p. 0031–0050). The Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM (2012) 10 Final) is meant to replace Council Framework decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30/12/2008 p.0060-0071).

Both proposals have important implications for SMART: the proposed Directive for processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM (2012) 10 Final) is directly relevant as all personal data used by automated systems examined in the SMART project would fall within the remit of this (proposed) Directive. It is the first European Union legislation to cover the practices of Member States when processing personal data within the law enforcement sphere. Council Framework Decision 2008/977/JHA only regulates the exchange of such data between Member States. However, this does not mean that EU Member States have no common regulatory background: the Council of Europe Recommendation 87(15) of the Committee of Ministers to Member States Regulating the use of personal data in the police sector and national laws of Member States, has served as a common regulatory background since 1987. Apart from pertinent criticism [7], the proposed Directive is an important document for the SMART project and has been used as a source of reference in the preparation of the Model Law (as part of the Toolkit).

The proposed General Data Protection Regulation is also important even if prima facie it may seem that prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties fall outside the scope of this proposed Regulation. There are several reasons to follow the developments in this regard. One reason is that the division between data collected for purposes that fall within the scope of the General Data Protection Regulation and the proposed Directive is becoming more and more blurred. Furthermore, personal data collected for one purpose may be used for law enforcement purposes at a later stage. One pertinent example for the SMART project is the following: in many cities around Europe, the security arrangements (and hence the collection of personal data in various forms, images, credit card information, identification data etc.) for what is often called the night time economy, are taken care of in a combination of the local council, the private sector (bars, restaurants, entertainment establishments etc.) and law enforcement. It is hard in such scenarios to clearly separate the application of the proposed General Data Protection Regulation and the proposed Directive.

• Court of Justice of the European Union on 8th April 2014 in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others
A second important legal development is the Court of Justice of the European Union’s judgement on 8th April 2014 in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, wherein the court declared the Data Retention Directive [8] invalid.

The Data Retention Directive has long been a controversial piece of legislation. The doubts surrounding the proportionality of the measures and purpose of the Directive (and the implementing legislation) have been a recurrent theme in the multiple court cases filed against the transposing laws.[9]

The confirmation by the Court of Justice of the European Union that the Data Retention Directive is disproportionate is a very important development, not only as the Court went on to confirm that the Directive is invalid but also as a strong reminder of the balance that needs to be sought in a democratic society between the actual needs of law enforcement and security services/intelligence agencies and the private-life interests of citizens.

• Legislative proposals following the Court of Justice's Decision

Following the Court of Justice's decision in Digital Rights Ireland and Seitlinger and Others Member States have started a process of reviewing what action (if at all) needs to be taken to change the national legislation authorising data retention. The latest of a series of declarations of Member States, is the presentation of a bill in the United Kingdom aimed at amending the regulations under the United Kingdom Regulation of Investigatory Powers Act 2000. On 10 July 2014, the United Kingdom Data Retention and Investigatory Powers Bill was presented to the UK House of Commons. Meanwhile the Austrian Constitutional Court on 27th June 2014 annulled the Data Retention Directive in Austria [10] and the Constitutional Court of the Republic of Slovenia abrogated the data retention provisions of the Act on Electronic Communications (ZEKom-1) in its judgment U-I-65/13-19 of 3 July 2014.[11]

Project objectives

It is against this background that SMART sought to complete eight main objectives. These were:

1. Determine the state of the art and likely future trends of smart surveillance, its proportionality and impact on privacy in four key application area.
2. Identify dependency and vulnerability of smart surveillance on underlying technology infrastructures (especially telecommunications networks) and explore system integrity and privacy issues therein.
3. Identify and explore smart surveillance and privacy issues in cyberspace.
4. Map out characteristics of laws governing surveillance and identify lacunae/new safeguards as well as best practices.
5. Map out characteristics of laws governing interoperability and data exchange and identify lacunae/new safeguards as well as best practices.
6. Explore the attitudes and beliefs of citizens towards smart surveillance.
7. Establish best-practice criteria developed on the basis of operational efficiency, established legal principles and citizen perceptions.
8. Develop a toolkit for policy-makers, police and security forces to implement and promote the best practice approach, including the development of system design guidelines and a model law balancing privacy and security concerns which would be capable of pan-European application.

References

[1]Supreme Court of The United States, Riley V. California (Certiorari To The Court of Appeal of California), Fourth Appellate District, Division One No. 13–132. Argued April 29, 2014—Decided June 25, 2014 pg.18.

[2]Cannataci, J.A. "Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector", in European Journal of Law and Technology, Vol. 4, No. 2, 2013 Available at: http://ejlt.org/article/view/284/390.

[3] Various articles published in The Guardian (http://www.theguardian.com/uk) between June 2013 and July 2014; and http://en.wikipedia.org/wiki/Edward_Snowden.

[4] One major initiative is "Reform Government Surveillance" where some of the major internet industry players - AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo – have written to the US Senate advocating reform of government surveillance. Available at https://www.reformgovernmentsurveillance.com/

[5] See for example, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and transatlantic cooperation in Justice and Home Affairs (A7-0139/2014) dated 21st February 2014 issued by the Committee of Civil Liberties, Justice and Home Affairs (Rapporteur Claude Morales). Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN; and European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) Available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference= P7-TA-2014-0230&language=EN&ring=A7-2014-0139

[6] Cannataci, J.A. "Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector", in European Journal of Law and Technology, Vol. 4, No. 2, 2013 Available at: http://ejlt.org/article/view/284/390

[7] E.g. by Cannataci, J.A. "Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector", in European Journal of Law and Technology, Vol. 4, No. 2, 2013 Available at: http://ejlt.org/article/view/284/390.

[8] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p.54).

[9] Three national constitutional courts – the Romanian Constitutional Court in October 2009 , the German Federal Constitutional Court in March 2010 and the Czech Constitutional Court in March 2011 – annulled the laws transposing the Directive in the respective jurisdictions on the basis that they were unconstitutional. Cases concerning data retention have also been brought before the constitutional courts of Bulgaria, which resulted in a revision of the transposing law; of Cyprus, where court orders issued under the transposing law were held to be unconstitutional; of Hungary, where a case was brought concerning the omission in the transposing law of the legal purposes of data processing; and the Irish Supreme Court also gave its opinion on the constitutionality of Ireland's implementation of the Data Retention Directive; in Slovakia too was the data retention law challenged. See Mifsud Bonnici, J.P. 'Redefining the relationship between security, data retention and human rights' in Ronald L Holzhacker and Paul Luif (eds), Freedom, security and justice in the European Union; internal and external dimensions of increased cooperation after the Lisbon treaty (Springer 2014) pg 55.

[10] Austria: Data retention provisions no longer apply. The Constitutional Court of Austria ('the Court') declared - on 27 June 2014 - data retention laws in Austria unconstitutional. Austria is the first EU Member State (MS) to annul data retention laws following the European Court of Justice (CJEU)'s decision to annul the Data Retention Directive (2006/24/EC) on 8 April 2014. The Court set aside the data retention provisions in the Austrian Telecommunications Act, the Police Authorisation Act and the Criminal Procedure Act. Companies now would only be obliged to retain data for specific purposes provided by law, such as billing of fault recovery.

"There is no requirement and legitimisation for retaining data beyond the limits provided by the general data provisions [and] this would also apply to data retained prior to the ruling," Dietmar Huemer, Attorney-at-Law at LEGIS, told DataGuidance. "The [data retention] provisions have been vacated as of 1 July 2014. The general data protection provisions apply." Last accessed on 15 July 2014 at www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2586

[11] Decision available here https://www.ip-rs.si/fileadmin/user_upload/Pdf/sodbe/US_RS_ZEKom-1_3julij2014.tif

Project Results:
The research carried out in the SMART project is based on four distinct project streams which built on and informed each other. These are explained in more detail under 'research parameters' and include a status quo analysis, an exploration of citizen attitudes towards smart surveillance and privacy issues, an analysis of the technical infrastructures supporting the use of smart surveillance systems and the creation of a model law and toolkit. The three work streams (status quo analysis, citizen attitudes, and technical infrastructures) operated initially as stand-alone pieces of research but the research design allows these findings to inform the development of the model law and toolkit.

The following are the key findings from these work streams:

Status Quo Analysis
The research in SMART was divided into first establishing a technological and legal assessment of the status quo of automated surveillance systems. Five application areas were explored in detail – border control areas; counter-terrorism, law and order; consumer sector multi-purpose mobile devices; e-government; and cyberspace.

The main results have given an overview of smart surveillance being deployed throughout Europe. There is a great diversity of application by the various law-enforcement agencies. However, the trend suggests that more surveillance technology, particularly smart surveillance, will be deployed over the coming years. The respondent police forces are either using or plan to use the technologies under consideration in the project. Whilst there are technical limitations to the use of the technology, these limitations will most probably be minimised as the surveillance technologies become more ubiquitous.

In all of the key application areas researched, except e-governance (namely border control, crowd control; law & order and counter-terrorism and cybercrime), a trend towards intensifying the integration of large-scale identification technologies was identified. Police forces are either using or plan to use the technologies under consideration in the project. Whilst there are technical limitations to the use of the technology, these limitations will be minimised as the surveillance technologies become more ubiquitous. Proportionality can be assessed at the operational, legal and technical level. At a legal level for example, regulations that are currently applicable to the private sector do not guarantee that smart surveillance technologies must be used in accordance with existing human rights standards. At the European level there is a fundamental right to privacy and data protection (art. 8 ECHR respectively art. 7 and 8 of the Charter in conjunction), but constitutions throughout Europe address the issue differently – for example, Germany recognises a distinct fundamental right to privacy as well as a right to informational self-determination, often intrinsically part of or woven into an overriding concept of an individual's right to unhindered development of one's personality (personlichkeitsrecht). This is not shared in some other member states, which can create disparate operational and legal environments.

In the following paragraphs we report on the most important findings in each of the status quo work packages. These are organised thematically as indicated in the title of each numbered paragraph:

1. The challenges and risks in ‘smart surveillance’ are inherent on a fundamental level.
In WP8, the underlying technology identified the technological architecture for many types of databases and the means by which to analyse them. These technologies are developed with consideration for operational robustness as well as data security. Moreover, these are almost always private networks and not accessible over public IP networks. There is some issue however with the increase in demand for mobile access. This technology uses public networks and is developed within public protocols, thereby increasing the security vulnerability of the system and database.
This is not to suggest that the technology is without risk. In a computer network, there are a series of major risks and vulnerabilities such as - attacks from within the community of network users; -un-authorized users who get inside the network; and eavesdropping from outside the organization or the authorized working group. People working with the infrastructures represent one of the key vulnerabilities. They can reveal classified data without authorisation or tamper the personal data integrity.
However, the research also identified that the human element in these systems is one of the biggest vulnerabilities, either because of not following security protocol or misusing the authority and access provided. Significant concern has been expressed over the lack of human involvement in the decision-making process, but this is not to suggest that humans beings are infallible or not prone to mistake and/or abusing power.

2. Surveillance and accompanying data analytics technology is becoming more commonplace in a diversity of arenas
The SMART project analysed smart surveillance technologies in key application areas: border control (WP2), law & order and counter-terrorism (WP3), mobile (WP4), e-government (WP5), and cyberspace (WP9).
Smart surveillance technologies in relation to border controls can be classified broadly as both those controlling cross-border traffic (information systems, personal and vehicle identification systems, automated border crossing systems) and border surveillance ‘on site’ (land border control systems, sea border surveillance systems). Biometric matching of fingerprints, iris, and face images is being increasingly used as a high-tech identity integrity management tool in border control. Most of the investigated technologies employed for border control in Europe seem to be proportional to their application aims. However, PNR and API are classic examples of function creep as they had not been originally created for border control. The security risk assessment in this key application area is based on broader political considerations and goals than for others.
WP2 found that border control is perhaps one of the few areas where smart surveillance is most visible and acknowledged by ordinary citizens. Border-control surveillance is mainly an overt surveillance and, consequently, the awareness of surveillance is higher than in other application areas. WP2 found that the large-scale European information systems used for controlling cross-border traffic, like VIS, SIS, and EURODAC, are relatively well regulated and subjected to relatively strict supervision of independent privacy and data protection agencies and authorities. This is not to suggest that the work package did not find concerns relating to privacy. The WP leaders were concerned that once the information has been collected and stored in such databases it can be easily used for other purposes than originally intended, i.e. function creep.

WP3 - Smart surveillance technologies in relation to law & order and counter-terrorism can be classified broadly as large-scale identification technologies (such as automated facial recognition); movement-

tracking technologies (such as automatic number plate reader (ANPR); and object and product-detection technologies (such as X-ray devices). The use of smart surveillance technologies in counter-terrorism and crowd control is a recent topic and is subject to continuous technological developments. It is a dynamic area in which users, sellers (including manufacturers) as well as the legislator lack experience to be in a position to fully implement proportionality at their level of activity. A number of specific smart surveillance technologies, particularly object and product-detection technologies, are governed by police codes of practice or internal guidelines/staff instructions and are technology-specific.

3. The deployment of surveillance technologies is rapid and largely opaque in some sectors
Work package 5 (e-Government) was particularly hindered by a lack of information. This is not to say that there is no smart surveillance deployment in the public sector, but rather that any information about an answer is difficult to ascertain.

Border control is a rapidly evolving space and the trend is likely to move toward more automation in scanners as well as enhancing the reach and scope of video and audio surveillance, through intelligent analytics. These technologies will form an integral part of unmanned aerial and ground border surveillance vehicles, as well as unattended border surveillance ground sensors. The regulatory regimes for these technologies are only barely being discussed amidst the accelerated adoption of these technologies. Furthermore WP2 found there are no metrics or methodologies for assessing impacts on a social or legal level. When designing a tool-kit useful to system designers and policy makers across Europe comprising such system design and operational guidelines, the most important further task of the SMART project is to develop a model framework to be used for a proper proportionality analysis and privacy impact assessment of the existing and newly developed surveillance technologies. Whenever private data is collected, accessed or processed by such systems a clear mapping and analysis of all data flows need to be carried out, from collection, use, disclosure, access, retention, correction, and destruction.

WP4
Mobile communications technology has become the backbone to modern society interactions from socialising to commerce. This is evident in that over 40% of the world's population which is active on-line now use smartphones and portable tablet devices for accessing Internet services. The technology itself continues to make large bounds forward, with capabilities of mobile devices evolving at a swift rate. There has been little thought given to the abilities of these devices for use as a surveillance device as well as being a target for surveillance itself. In addition, the legislative regime for this technological development is underprepared.

In addition to this these devices can be compromised by malicious code that often employs covert means to allow unauthorised use of features or extraction of data from a device. This could include recording conversations or video footage without the end user knowing or consenting to this type of activity. Furthermore, a simple theft of data from these devices allows for highly targeted fraud, theft, extortion and espionage to be conducted. The propagation of these types of invasions of privacy can be conducted by the person standing next to you or from across the other side of the world via the Internet. The findings of the SMART project suggest that the process of being observed, monitored, geo-located or marketed to as a result of using these devices is increasingly an issue that has serious privacy and personal security issues for end users. To access many of the services end users are required to surrender what may seem

to be innocuous and basic information but these disclosure statements are seldom read, let alone understood. Often the providers enable the user to make use of a free service in exchange for behaviour data, which the providers may then leverage to develop new products and/or more efficiently advertise existing ones. When this information is aggregated with specific device identifiers, network location, network provider and other physical attributes of the device, as well as other embedded attributes in the form of metadata produced by an application or service, it ultimately produces a rich and unique profile of the end user.

The variety of technologies and practices used to monitor individual behaviour in cyberspace is immense. WP9 found that in cyberspace, there appears to be a broad usage of surveillance methods and technologies. This may incongruous at times with many agencies claiming only a very limited technological reach. However, the questionnaire in WP9 demonstrated that many law enforcement agencies are planning to massively extend their variety of tools to use for surveillance in cyberspace. In total, there seems to be not a single technology being available, which is not either used or at least intended to be used in near future by one or several states. The vast majority of technologies employed for smart surveillance in cyberspace are multi- purpose technologies - the data collected is likely to be used for purposes other than those for which the data was originally was collected. Results tentatively suggest that surveillance technologies and practices used in cyberspace are comparably easy to apply and are prima facie less invasive, such as analysis of meta-data. More sophisticated and more invasive technologies such as Trojan horse software or session-hijacking appear to be used by fewer agencies. While many agencies state that they have only very limited technical possibilities and only some of them are (publically) planning to extend their field of possibilities, there are a number of agencies using powerful tools and methods to access data. This is in relation to the development of crime, which now may often have a digital component, whether in the organisation or execution of the illegal activity.

4. There is a need for more pertinent rules on surveillance
Essentially the large and extensive work carried out in WP6 shows that the law is not prepared for the increased use of automated decision technologies. The legal environment in which smart surveillance operates in Europe is disjointed, lacking consistency in statute, application, and interpretation. The national laws governing the use of personal data for security and law enforcement purposes as well as the procedures for complaints are not harmonised. While the broad EU-level legislative principles such as those to be found in the Personal Data Directive (95/46/EC) are transposed across all states of the union, it cannot be said that the measures employed for transposition are uniform or are uniformly applied.

Furthermore, the European Commission has sought to reform the data protection regime within Europe to meet the new challenges and realities of evolving technology. The General Data Protection Regulation and the draft Directive on Police Data were introduced in early 2012. At the time of submission, this ‘data protection package’ is still undergoing the legislative process. It remains to be seen what the final result will be.

With regards to the latest revision, the SMART project found a number of issues with the Regulation with specific focus to smart surveillance:
• National security (and the surveillance measures undertaken to this end) are excluded;
• The definition of personal data could be potentially problematic in its wide remit and vague parameters;

• The Regulation will still overlap more sophisticated and detailed national legislation. This may lead to an adverse simplification of interpretation and application;
• Specific kinds of surveillance are not addressed, leaving the unique challenges of each type of surveillance open to uncertainty;

This all said, the current draft of the Regulation is, on the whole, a more robust, more useful, and more protective piece of legislation than the original Commission proposal. However, the problems of oversimplification and extrusion of sophisticated national legislation remain an issue. It rests with the legislator and policy-makers to decide whether or not technologically-neutral texts are preferable or not. There are a host of arguments in favour of formulating legislation without particular consideration of possible technologies and areas of application, with the perception of legal flexibility, wider applicability, and timeless applicability as main points.

The legal review in SMART revealed issues in connection with surveillance -and particular smart surveillance-which require transparency, foresight and a level of consistent protection that is in line with the developments of modern surveillance technologies. Privacy protection should not be left to the application of general principles by single persons, as this approach is more prone to errors than the provision of comprehensive and specific information as to the proper application of the law. The Regulation would not allow Member States to act independently. Therefore, supervisory authorities, the Commission and especially the new European Data Protection Board should issue accompanying legislation and non-legislative information for controllers and the people, in order to assure proper application of the Regulation in all possible areas of surveillance by the private sector (e.g. video, multiple sensors, smart cities, mobile devices, mass events, drones, etc.) and thus guarantee protection of privacy and personal freedom. The intended Regulation draft provides possibilities for such specification, for instance through delegated acts (cf. Art. 86), codes of conduct (cf. Art. 38) and the issuing of guidelines, recommendations and best practices (cf. Art. 66 para. 1 (b)).

The draft Directive on Police Data is the second plank of the data protection package and has its own issues as well as developments:
• Whilst there may be argument about whether the provisions in the draft Directive are better joined as part of the Regulation, it cannot be disregarded that there are positive effects in terms of the upgrade from a ‘decision’ to a ‘directive’. There are still competence and applicability challenges, but the trend seems to indicate more cooperation and greater enforcement;
• The definition of the term ‘personal data’ is problematic for the same reasons as the draft Regulation;
• The missing principle of direct collection is still an issue;
• The regulation of profiling is improved, although advocates of greater individual protection would rather these measures go further;
• The Directive as a legal act leaves room for national specification. This may be a positive or a negative, depending on how member states take these measures forward in transposition. The SMART project is unable to comment further on this until there is further development;
• The Directive Amendment introduces and improves some general innovations (e.g. access to data initially processed for purposes other than those referred to in Art (1), time limits of storage and review, different categories, further processing for incompatible purposes, processing of genetic data, general principles for the rights of the data subject, impact assessments, joint operations, transmission to other

parties);
• The draft is still formulated in a general manner and does not consider specific kinds of surveillance or the technologies which will be regulated;
• Especially Art. 49 para. 1 (b) provides possibilities for necessary specifications of particular technologies and relevant areas of surveillance.

The passing of the draft Directive would be a very useful measure in bringing in certainty and protection into the operations of police data collection. The possibility for further implementation by and specification within national legislation is a strong point of the legal act. Still, precise regulation for specific kind of surveillance or technologies would nevertheless be useful. In order to guarantee harmonised protection in line with the possibilities of modern data processing, additional information at non-legislative level as well as accompanying legislation would be equally useful as for the Regulation. The intended Directive provides fewer possibilities for such specification, the most important of which is the issuing of guidelines, recommendations and best practices under Art. 49 para. 1 (b). To be on the safe side, it should also be noted that there are still serious doubts as to the lawfulness of the intended scope of the Directive.

WP3 felt that the technology-neutral approach to these technologies is not as effective as a technique-specific legislation, which could be a more operationally efficient and application to operators and authorities given the direct specificity. By identifying and categorising the various techniques (e.g. profiling or data mining), when these elements are incorporated into smart surveillance systems, the legislation would be more prepared to meet the challenges that novel technology deployment often provides. It would also be able to be revised and altered more rapidly than starting from scratch, as the legislative process for completely new legislation may be very time-consuming. WP3 goes on to suggest that technique-specific legislation would also be understood as purpose-specific legislation since it would highlight the specific purpose pursued by a specific technique. As such, legislation would become effective and provide operational criteria and corresponding safeguards to be implemented by law enforcement agencies.

5. Surveillance data is being shared at increasing rates with mixed levels of privacy protection for the individual
Although they may be improved, there are data-sharing regimes in place that do strike a balance with operational efficiency, prioritising public security, and maintaining privacy of the individual. In WP7, data sharing between data-bases was examined. While there is always room to develop and improve the balance between privacy, public security, and operational efficiency, the WP's findings show at least a few examples which can serve as basis for better practice. It was found that the exchange of (personal) data in the course of police and judicial co-operation is based on an already well-established network in terms of legal provisions/agreements, information exchange channels and according technical networks. Within the EU this framework shows a higher level of interoperability through various special instruments such as Europol, Schengen Information System (SIS), Prüm mechanism, Visa Information System (VIS) and EURODAC. Beyond the borders of the European Union the data exchange is based on the framework of INTERPOL and on multi- or bilateral agreements. However, the network of data protection authorities and the legal framework for data protection do not have the same level of international cooperation than the respective framework for police and security services. Although data protection is considered as an important issue and there have been important developments in recent years, the data protection framework is not able to maintain the same developmental pace as the deepening of the technological and

operational interoperability of cross-border police cooperation.

A central issue which could be identified is the high fragmentation of laws concerning data protection. The established framework consists of well written and important principles but the real content of subjective rights and compliance mechanisms is not transparent and easy to determine due to a number of cross-references between the various regimes, e.g. Council of Europe, European Union and finally – and most important – the national laws. Moreover, the central data protection regimes allow too much derogation on national level also of core provisions such as the duty to information and the right to access. Consequently it remains difficult to evaluate in which situations the specific instruments apply and which rules are applicable. For instance, Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters exclude from its already limited scope additionally the central databases of Europol or the SIS. It would possibly be better if the cooperation tools as well as the respective safeguards are centralised on EU level, e.g. regarding EURODAC or VIS.

The purpose limitation is marked by open and abstract notations such as detection and prevention of (serious) crimes or threats for the public security. The national traditions of security and law enforcement differ so much that narrow definitions would hinder the co-operation. Central catalogues of crimes are rarely to find, only the most intrusive instrument “European Arrest Warrant” provides an exceptional piece of harmonisation in this respect. Consequently, the purpose definitions are usually kept very open and/or are complemented by rather blanket references to national criminal and security law. Even purpose definitions with precise definitions are accompanied by very generous provisions for the reuse of data for others than the original purposes. Hence, the state practice determines the limits and proportionality of the purpose limitation principle. The national level defines which facts justify the use of investigation powers for both prevention and detection of crimes, and national courts or other supervisory authorities are in charge to ensure compliance. But in practise it can be rather difficult for the data subject to claim the rights in another state with different laws and procedures. Council Framework Decision 2008/977/JHA improves some particular data protection rights but is not strong enough because the further national processing of personal data is not covered by this instrument.

6. While there is an acceptance that surveillance is a necessary function of modern society, there is a marked anxiety and concern about surveillance deployment that is done without the knowledge and consent of the wider population
Focus group discussions were held in the following 14 partner countries: Austria, Bulgaria, Czech Republic, France, Germany, Italy, Malta, Norway, Romania, Slovakia, Slovenia, Spain, the Netherlands and the United Kingdom. The analysis and results are based on 42 focus group discussions comprising of 353 participants, which were held in order to examine the beliefs and attitudes of citizens towards smart surveillance and privacy.

The focus group discussions were conducted in line with a discussion guide mainly consisting of different scenarios aimed at stimulating a discussion amongst the participants. While some scenarios dealt with surveillance in everyday contexts likely to be encountered by research participants, other scenarios were hypothetical in nature and their aim was to elicit the feelings, beliefs and attitudes of the participants in relation to dataveillance, the massive integration of data from different sources and the “security versus

privacy trade-off".
Moreover the focus groups findings shed light on individual sentiment in geographically and culturally diverse areas. The results were striking in how much convergence of opinion participants from the different member states

Work Package 10 was the one responsible for the qualitative research carried out by the focus groups. It established that the general findings and common themes which emerged from the analysis of all 14 countries include that:

a) Participants were highly aware of being under surveillance in different contexts including commercial spaces, public places and boundary spaces such as airports. They were also knowledgeable about the wide range of surveillance technologies and methods employed in these contexts.
b) Participants were also rather knowledgeable about the extent of surveillance and the collection of citizens' data when making use of a mobile device. Similarly, most participants expressed their awareness of being systematically under surveillance in the virtual space. It appears that participants perceived a higher loss of control over personal data in this sphere.
c) Participants argued that individuals are, in part, responsible for divulging personal data, especially with regards to the virtual sphere. In particular, several participants criticised the naiveté of internet users in relation to online data sharing, especially on social networks.
d) Surveillance in public places and high risk areas was generally considered as acceptable, although a minority of participants did object to being monitored in public places. On the other hand, surveillance in private places was regarded as unacceptable. Participants also appeared to show a higher acceptance for surveillance when such monitoring was not covert. The lack of information available about implemented surveillance measures was criticised.
e) Participants perceived the surveillance of citizens and customers to take place either for security or for commercial purposes. Surveillance in public and boundary spaces for purposes of national security and citizen safety was generally considered as more acceptable than surveillance conducted by private companies for commercial objectives.
f) Participants typically perceived the extensive integration of data from dataveillance as a threat to citizens' privacy, and were thus generally against it. Nevertheless, acceptability appeared to be contingent on a number of factors, including type of data, purpose of use and whether consent was provided for data sharing. Concerns about risks of misuse and manipulation were also taken into consideration by the participants.
g) The collection and sharing of some types of data, some of it sensitive personal data, such as location data, financial information, as well as medical and health data, was deemed unacceptable by most participants. Nevertheless, it appears that in certain specific situations, especially in potentially life-saving circumstances, the use of certain types of confidential data was considered as justified.
h) The majority of participants considered the massive integration of personal data as technically possible, however, in most countries, it was perceived as currently unlikely due to legal restrictions or ethical constraints.
i) Acceptance of dataveillance appeared to be contingent on several criteria including purpose of data collection and use, whether consent was provided, type of data collected and shared, which entity – state or private – was conducting dataveillance and whether personal data was anonymised prior to being shared with third parties.

j) While participants typically perceived smart surveillance technologies as more intrusive compared to traditional surveillance measures, some argued that the use of smart surveillance could have less of a negative impact on privacy as well as decrease the risk of data misuse and manipulation.
k) Upon reflecting on the automated decision-making process of smart technologies, participants generally appeared sceptical of a wholly automated process devoid of human agency. Although participants pointed out that an automated process would be more objective, and thus more reliable than a surveillance process involving humans, they also argued that an automated process could possibly result in misinterpretations and in erroneous decisions being taken. In light of this, the majority of interviewees believed that the surveillance process should include a combination of technologically-mediated surveillance and human agency.
l) Different types of surveillance technologies typically met different levels of acceptance:
a. The use of video-surveillance appeared to have undergone a process of normalization and participants generally tolerated its deployment in public places for security purposes.
b. The use of Automated Number Plate Recognition was generally tolerated, while the use of sound sensors was subject to mixed reactions.
c. The use of biometric technologies and electronic tagging, hence surveillance involving the physical sphere, was perceived as extreme and deemed unacceptable.
m) Extensive surveillance was perceived as posing a threat not only to privacy but also to the freedom of citizens. Concerns were also expressed by the participants in relation to the possible abuse of power by the state, since the collection of surveillance data was regarded as creating a power imbalance between the state and its citizens. Other perceived concerns resulting from the use of extensive surveillance included the possibility that monitoring could facilitate processes of dehumanisation in society. The intensification of surveillance was also considered as labelling each citizen as a potential risk, and thus as possibly resulting in a general criminalisation of citizens.
n) The majority of participants rejected the concept that extensive surveillance would result in increased security. The surveillance of citizens was not seen as a viable solution for the reduction of crime and therefore most participants were not willing to sacrifice their privacy for increased surveillance in case of a rise in crime. Alternative options to surveillance, such as the use of education, were suggested by several participants.
o) Participants perceived a variety of threats deriving from surveillance, including the use of surveillance tools by the state as a means to control citizens and a higher risk of misappropriation of surveillance data. As a consequence, rather than enhancing feelings of personal safety, an increase in surveillance measures resulted in feelings of deep insecurity.
p) Participants strongly questioned the effectiveness of surveillance measures in relation to the deterrence and prevention of crime. On the other hand, surveillance appeared to be considered as effective for the investigation of crime.
q) The majority of participants displayed a lack of knowledge of privacy laws and regulations. The participants mainly attributed this lack of knowledge to the perceived complexity of the legal jargon used and a general lack of initiative by citizens in getting informed about the legislation.
r) While some participants regarded current privacy legislation as inadequate and also as outdated due to the fast advancement of technology, others appeared satisfied with the level of protection offered by privacy legislation.
s) Expectations regarding ideal length of data storage for surveillance data varied. While some participants appeared to prefer a relatively short storage time ranging from hours to weeks, others stated that

surveillance data should be stored for months, years or even indefinitely in certain cases. Additionally, some participants appeared indifferent to length of data storage. Overall, participants suggested several criteria which in their opinion should determine storage period, including type of data and purpose of use. In relation to the latter, it appears that most participants were in favour of a relatively longer storage period in case surveillance data is utilised for purposes of crime investigation.
t) Whilst on the one hand acknowledging that the storage of surveillance data is useful in investigation and prosecution of crime, on the other hand it appeared to be a cause for concern amongst the majority of participants since this was regarded as increasing risks of data misuse and misappropriation.
u) Data sharing between public actors for security or administrative purposes was considered as more acceptable than the sharing of data between private actors for commercial purposes.

7. Identification of best practices

Best practice criteria for privacy-enhanced and user-friendly use of smart surveillance technologies were also examined. The criteria are based on a theoretical model of a sociological kind, utilized in the SMART project to study a range of social dynamics related to contemporary surveillance. In particular, the notion of a "context of meaning" was adopted to analyse the relationship between four constitutive phenomena: the increase in human agency, leading to a greater presence of individuals on the social scene; the new demand for privacy amongst those who expose themselves on this social scene (especially via ICT); the consequent increase in security demands and protection services or technologies; and the concomitant development of surveillance strategies and policies. The interlinking of these phenomena is complex and is based on the relationship between dangers (menacing events or processes that are potentially out of control), social regimes (regulatory activities aimed at handling the dangers, to limit their range) and risks (dangers when known and handled by social regimes). In light of these dynamics, the policies of surveillance and security technologies – created, in principle, to protect citizens – may, in turn, produce new dangers in terms of personal freedom, civil rights and privacy protection. These need to be tackled through a governance perspective that is adequate to the task.
It is argued here that the implementation of the institutional and regulatory measures in this field requires a conducive social environment to allow a growth in the relevance, effectiveness and impact of such measures. This favourable context is characterized by the presence of a specific social agency. This agency is identified through certain practices which, in the light of the experience and results of the SMART project, appear particularly conducive to a privacy-friendly use of smart surveillance. In an attempt to conveniently group these practices in a limited set of types, we may consider them to be "best practice criteria" promoting privacy and data protection. 9 specific best practice criteria have been identified, which are both interconnected and each correspond to strategic areas of intervention.
1. Research and knowledge dissemination: promotion and support of more relevant and contextualized research with respect to society and intra-and inter-disciplinary scientific exchange.
2. Innovation management: adoption of advanced approaches in the field of technological innovation, such as "privacy by design".
3. Regulatory control and accountability: consolidation of a culture and practice of accountability: from the normative to policy and the use of technologies).
4. Coordination and partnership: networking and co-ordination among public institutions at national and trans-national levels, and partnerships among the "triple helix" actors.
5. Transparency: promotion of a wider awareness about smart surveillance and citizens' rights, as well as widespread public debate about this issue.

6. Capacity building: reform of the professional competencies and knowledge of managers and operators in this field, and the promotion of continuous learning policies underpinned by a comprehensive training strategy.
7. Actors' responsibility: promotion of a high level of accountability of all key actors within smart surveillance systems, e.g. in the context of public administration reform and of corporate social responsibility.
8. Citizens' awareness and engagement: promotion of a strategy to support and develop citizens' participation, through inclusiveness and public dialogue at various levels .
9. Diversity and equality: paying appropriate attention to diversity in the design and implementation of strategies and policies for smart surveillance, e.g. regarding social exclusion and gender.
Developers and implementers of strategies and policies in the field of smart surveillance should remain aware of all 9 criteria contemporaneously. This is to avoid any reductionist and unsystematic approach in an area which is complex and constantly evolving.

8. Through the identification of best practices and status quo analysis, the SMART project's Toolkit and Model Law can help in addressing the risks and concerns identified in the project
The results and foregrounds covered thus far are meaningful and provide insight as stand-alone investigations. The SMART project is unique in that it has combined these cross-disciplinary results into two outcomes that are potentially very valuable for policy makers, legislators, and operational authorities. This meets the final objective of the SMART project, which is to begin to address the issues raised.
Two key outputs of the SMART project with policy implications are (a) the model law and (b) a complementary toolkit. The model law introduces the concrete legal safeguards which have already been recognised as necessary by Europe's policy-makers in legal instruments as diverse as the Council of Europe's/Schengen Agreement's Recommendation R(87)15 on the protection of personal data used for police purposes and Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This model law provides a number of concrete safeguards specifically designed with smart surveillance in mind, implementing a series of scalable measures which would be made mandatory at system design and operational stages. It should be noted that while the Model Law is capable of being used in the case of smart surveillance systems alone, as will be mentioned later, work on development of the Model Law continued even after the conclusion of the SMART project. Indeed, in the nine months following submission of the deliverable containing the SMART project's model law, work on the further development of this legal instrument was continued within another EU FP7 project, RESPECT .[12] The latter had, by April-May 2015 developed the SMART model law on smart surveillance into a legal instrument with a scope which is wider than that of smart surveillance and which indeed is intended to provide safeguards for all types of public sector surveillance situations.
The SMART toolkit addresses the problems raised while examining border control (WP2), counter terrorism and law enforcement (WP3), consumer sector multi-purpose mobile devices (WP4), e-government (WP5), surveillance in other areas of law (outside data protection law) (WP6), Interoperability and data exchange between police/security forces and private sector (WP7), underlying telecommunications infrastructure (WP8), and on-line surveillance in cyberspace (WP9), outlined above.

(i) Model Law
The first part of the Toolkit is the Model Law which is created in such a way so that it could be adopted

across the EU member states providing scalable measures including explicit safeguards for smart surveillance especially in furtherance of Section 7 and other parts of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The measures envisaged could be promulgated as stand-alone pieces of legislation or be included in other legislation addressing the same issues.
At an abstract level, the Model Law presented in this Toolkit has three central aims:
• state and reaffirm the value of privacy in our society: In Europe, the value of privacy is reaffirmed in both the European Convention of Human Rights (Art. 8) and in the EU Charter of Fundamental Rights (Art. 7 & Art. 8). Apart from the legal value of legislators and policy makers reaffirming the value of a fundamental right, there is also in it a symbolic perspective;
• address some pivotal aspects of privacy-related issues and other fundamental rights and freedoms in an age of smart surveillance;
• create a shared culture where all (law enforcement, security services/intelligence agencies and citizens) are aware of the importance in a democratic society to carefully balance the potential benefits of the extensive use of surveillance technologies that assist law enforcement and security services/intelligence agencies in their mission against important private-life interest.

At a more tangible level, the Model Law lays down safeguards to protect the fundamental rights and freedoms of individuals when smart surveillance systems are used primarily aimed at:
• reducing the impact of the deployment of smart surveillance systems on fundamental rights and freedoms of individuals by requiring that no smart surveillance systems is introduced without prior:
o privacy impact assessment including an examination of whether the smart surveillance system is necessary and proportionate;
o assessment of the error threshold of the system carried out by an expert authority specifically set up for this certification;
o assessment of the security means put in place to prevent illegal access to the personal data, and the algorithms of the smart surveillance system by unauthorised persons or systems;
o authorisation by law to be so deployed.
• providing for review of outcomes of smart surveillance systems that may have an effect on fundament rights and freedoms of individuals by:
o establishing a system for human re-assessment of an outcome based on a smart surveillance system;
o establishing a system for appeal from a decision given following a human re-assessment;
o giving access, without prejudicing on-going operations, to the reasoning followed in the outcome of the smart surveillance system and the personal information processed by the smart surveillance system.
• providing additional safeguards to be set in place where the outcome of a smart surveillance system may lead to an arrest (and reduction of the right to liberty of an individual) and when the smart surveillance system may be processing a watch list/black list upon which an individual may have been placed;
• drawing attention to important principles and fundamental rights and freedoms that come into play in the treatment of individuals by law enforcement and security services, including requiring the least intrusive physical intervention respecting one’s dignity, bodily integrity, reputation and presumption of innocence (as part of the procedural rights of an individual);
• providing safeguards arising from the way smart surveillance systems are maintained: namely assurance that personal data is kept securely; and that a system of supervision and of the security of the systems and personnel accessing the smart surveillance systems is in place.

(ii) Toolkit
The Toolkit complements the model law by focusing attention on eleven aspects of an evident mismatch between reality (that is, what is going on in practice) and the current regulatory framework. These are the eleven themes:
i. Opaqueness: lack of transparency of practices
ii. Limited awareness
iii. Social Costs of Surveillance
iv. Shortcomings of Law
v. Function Creep
vi. Use of Sensitive and/or Biometric Data
vii. Differences between Member States
viii. Storage/Retention
ix. Inherent Risks of Certain Technologies
x. Security of Systems
xi. Mass surveillance without specific reasons or reasonable suspicions
Within each of these themes, the document lists appropriate strategies to be followed to improve or remedy the conditions noted in the issue. Appropriate tools or measures that can be taken are identified for each of the themes. The target for each of the tools is mainly to provide a balance between the responsibilities democratic states to provide for the protection of the state and individuals within the state and to protect the private-life interests of the same individuals.

Reference
[12] The RESPECT project was undertaken under Grant Agreement 285582 and ran from February 2012 to May 2015. More details at www.respectproject.eu

Potential Impact:
The project findings from SMART provide policy makers with:
• An overview of the current smart surveillance systems in use in five key application areas were explored in detail – border control areas; counter-terrorism, law and order; consumer sector multi-purpose mobile devices; e-government; and cyberspace. This overview includes a review of the legal basis used and a proportionality impact assessment. This will enable policy makers to establish the relevant gaps in the regulation of a fast developing area.
• An overview of the legal framework regulating (to varying degrees) smart surveillance technologies at a European level (covering both Council of Europe and European Union legal framework) and national level.
• The results of in-depth empirical research into (the list below) may help policy makers understand their citizens' needs:
- Citizens' understanding of the types of technologies and applications identified in the project;

- Citizens' understanding of the implications of MIMSI (Massively Integrated Multi Sensor Inputs) technology;

- The beliefs and attitudes of citizens with regards to sharing of personal information about themselves and others which is often a feature of smart surveillance and especially MIMSI;

- Citizens' perceptions of the "security v. privacy trade-off" in smart surveillance. Which additional factors may influence citizens' decision to approve the state entering into a "security v. privacy trade-off" when deploying smart surveillance;
A Model Law which can assist European policy makers and governments in the formulation of legislation aimed at providing safeguards for citizens when smart surveillance is used or planned to be used.
It balances privacy and security concerns which would be capable of pan-European application; the model provisions below are thus not modelled to fit one particular legal system. They are designed to be adapted to the needs of each State, whatever its legal tradition and social, economic, cultural and geographic conditions.

The SMART Project's policy impact may be very considerable if the Model Law as further developed by the RESPECT project is eventually taken up for pan-European adoption. With this aim, possibly during the process or just after the European Data Protection Reform Package is moving towards being finalised, it is expected that the Model Law on Surveillance will be presented to the LIBE Committee of the European Parliament for its further consideration. If the European Commission, Council and the European Parliament were to adopt or adapt the measures contemplated in the SMART project tool-kit together with the model law as further developed by the RESPECT project, then impact could be maximised within Europe. The model law is written in such a way so as to be easily used outside Europe too so a snowball effect cannot be excluded and would indeed be welcomed.

Main Dissemination Events

• Visit to Frontex Headquarters: Warsaw, Poland (November 2011) - As part of WP2, the Project Coordinating Person, Prof. Joe Cannataci and the WP2 coordinator, Dr. Simon Dobrišek travelled to Wrocław, Poland to visit the headquarters of Frontex, the EU's independent body coordinating operational cooperation in border control.

• Cyber Security and Privacy EU Forum: Berlin, Germany (24-25 April 2012) – A presentation was given by Dr. Mireille Caruana from the University of Malta about SMART at the Cyber Security and Privacy EU Forum. [13]

• 41st European Regional Conference (Interpol): Tel Aviv, Israel (8-10 May 2012) – The project coordinator and consortium partner Interpol attended and participated including the delivery of a formal presentation in plenary session.[14]

• INTERPOL 21st Asian Regional Conference - The SMART Project Co-ordinating Person Joe Cannataci and WP3 Co-ordinator Caroline Goemans-Dorny participated in and made formal presentations during the Interpol 21st Asian Regional Conference held in Amman, Jordan (September 2012). The meeting provided an opportunity to disseminate research from the SMART project as well as develop new relationships with law enforcement agencies, which will strengthen the impact of the SMART project.

• First SMART Policy Workshop (Florence 2012): The proceedings of the first SMART policy workshop, Surveilling Surveillance, [15] were published in the European Journal of Information Law Autumn 2013

volume. [16]

• Round Table at Slovenian Protection Commission: Ljubljana, Slovenia (1 July 2013):- RESPECT and SMART project representatives engaged with the Slovenian Data Protection Commission in a discussion on “Status Quo and Challenges of the Present and Forthcoming EU Regulation of the Use and Exploitation of Modern ICT for Surveillance Purposes”, “Challenges for a Balanced Use of Open Source Intelligence (OSINT): A Law Enforcement Perspective” and “Social Network Monitoring and Analysis Systems”

• Second SMART Policy Workshop: Brussels, Belgium (19-20 September 2013). The Second Policy workshop, Intelligent Investigation - Challenges and Chances [17] was held over two days and hosted at the Representation of Lower Saxony in Brussels. The event was attended by a wide variety of stakeholders, including law enforcement, data protection authorities, policy-makers and industry. The proceedings of this event will form part of a published volume within the coming months.

• Discussion Panel at CPDP Conference: Brussels, Belgium (23 January 2014): The SMART consortium co-hosted a discussion panel entitled “Regulating Automated Decision Making: A Case For Evidence-Based Policy-Making In Privacy And Surveillance”. The panel session was chair by Mr Joel Sollier (Interpol) and moderated by Prof Antoinette Rouvroy (University of Namur, Belgium) and the panels were Prof. Nikolaus Forgó (Leibniz University Hannover, Germany), Ms Caroline Goemans-Dorny (Interpol), Mr Bogdan Manolea (Association for Technology and Internet, Romania) and Dr Andrej Savin (Copenhagen Business School, Denmark). The panel discussed ways policy makers can address the current gaps in the regulation. The panelists addressed the topic both from a citizen and a law enforcement perspective.

• The Perth Workshop: Perth, Australia (4-6 February 2014): This event was held in Perth Australia, organised by consortium member and work package 4 leader, Edith Cowan University. The event was changed from a conference to a workshop in reaction to the response as well as opportunities to receive specialised information from the Western Australia Police. The event allowed the project to (a) continue discussions on the next available draft version Model Law and (b) to further understand police surveillance technology from a primary operational source. The event was instrumental in informing the Model Law and toolkit as well as preparing for the final conference.

• SMART Final Conference: Brussels, Belgium (4-5 March 2014): As described in the SMART DoW, the results of WP6, 7, 10 and 11 were presented at a conference at EU level. The SMART Final Conference had established a planning committee comprised of members from the coordination team (University of Malta), Masaryk University (WP14, Dissemination), and the University of Vienna. The decision to base the event in Brussels had been motivated by the drive to give the greatest possibility for attendance by relevant EU policy makers. The theme of the final conference centred on smart surveillance, its global impact (building upon the event in Perth, Australia), and plans on how to best approach current and future challenges.

Further dissemination through publication: Some of the project findings will be made available on the project web-site. In order to widen dissemination of the project findings and recommendations, a good

portion of the project findings will be published by the Austrian Computer Society in both a hard-copy version as part of a three volume set and also through free access on-line.

References

[13] http://www.cspforum.eu/
[14] http://www.interpol.int/News-and-media/Events/2012/41st-European-Regional-Conference2
[15] http://www.ittig.cnr.it/smart2012/
[16] European Journal of Law and Technology Vol 4, No 2 (2013). The volume is available online at: http://ejlt.org//issue/view/18

List of Websites:
Website: www.smartsurveillance.eu
Prof. Joseph Cannataci - jcannataci@sec.research.um.edu.mt

Dernière mise à jour: 24 Février 2016

Permalink: https://cordis.europa.eu/project/id/261727/reporting/fr