



**FP7 – SEC- 2011-284725**

**SURVEILLE**

**Surveillance: Ethical issues, legal limitations, and efficiency**

Collaborative Project

*This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 284725*

**SURVEILLE Deliverable 4.6**

**Report of Project Meeting No. 4, related to WP4**

Due date of deliverable: April 30<sup>th</sup> 2014

Actual Submission date: April 30<sup>th</sup> 2014

SURVEILLE Work Package number and lead: WP4 led by Prof. Martin Scheinin (EUI)

**Author:** Jonathan Andrew, Mathias Vermeulen, Maria Grazia Porcedda

Project co-funded by the European Commission within the Seventh Framework Programme		
<b>Dissemination Level</b>		
<b>PU</b>	Public	X
<b>PP</b>	Restricted to other programme participants (including the Commission Services)	
<b>RE</b>	Restricted to a group specified by the consortium (including the Commission services)	
<b>CO</b>	Confidential, only members of the consortium (including the Commission Services)	

***Date and location: 25-26 March 2014 at Villa La Fonte, EUI, Florence***

**Attendees:**

EUI	Prof. Martin Scheinin
	Ms. Maria Grazia Porcedda
	Mr. Jonathan Andrew
	Mr. Mathias Vermeulen
	Prof. Tuomas Ojanen
UoB	Prof. Heather Draper
	Dr. Greg Moorlock
RWI	Dr. Karol Nowak
Delft TU	Dr. Coen van Gulijk
	Ms. Michelle Cayford
ALU-FR	Dr. Elisa Orru
Fraunhofer	Mr. Erik Krempel
	Dr. Ralf Eck
ULB	Dr. Francesca Galli
	Ms. Céline Cocq
EFUS	Mr. Sebastian Sperber
MERPOL	Mr. Brian McNeill
	Ms. Maggie Gorman
UoW	Prof. Tom Sorell
	Dr. Katerina Hadjimatheou
	Dr. John Guelke

### **SURVEILLE Advisory Board:**

Dr. Christiane Hoehn (Adviser to the EU Counter-terrorism Coordinator, COUNCIL OF THE EUROPEAN UNION)

Mr. Stephen Otter (Her Majesty's Inspectorate of Constabulary)

### **Invited external experts:**

Martin Gill (Perpetuity Research and Consultancy International)

Dariusz Kloza (Institute of European Studies IES, Vrije Universiteit Brussel VUB)

Prof. Iain Cameron (University of Uppsala)

Prof. Serge Gutwirth (VUB – PRISMS project)

Prof. Douwe Korff (London Metropolitan University)

Mr. Willem Debeuckelaere (President of the Belgian Data Protection Authority)

## **Day 1**

### **9.00 Opening**

Prof. Scheinin (EUI) opened the meeting and welcomed all participants to the EUI. Prof. Scheinin noted that SURVEILLE is a multidisciplinary project, where all the partners involved interact with each other in a common research process. Prof. Scheinin noted that the project's research during the last few months have delivered promising results, not only academically but also for the general public and the Commission.

### **9.30-11.00 Assessing CCTV Surveillance**

Chairing the session, Sebastian Sperber (EFUS), opened the first discussion session entitled "Assessing CCTV Surveillance" and noted that CCTV remains a very important form of surveillance as used by local authorities. Sebastian Sperber then noted that CCTV is a type of surveillance with which many people are acquainted, and that many increasingly accept it. Sebastian Sperber then introduced the first speaker, Prof. Martin Gill, who would talk about his work in the field of criminology on CCTV and its impact in societies.

Prof. Martin Gill had been requested by SURVEILLE to write a paper for the meeting. He began his presentation of the paper by noting that his work on CCTV

effectiveness has taken place within the context of his specialization in criminology, where he has looked at evidence and assessed different CCTV systems in terms of their efficacy in preventing and investigating crime. Prof. Martin Gill noted that questions arise as to the ethics of implementing CCTV systems both when they are effective and, indeed, when they are shown to be ineffective. As such, the question at hand is whether it is ethical to further implement systems when they have been shown to be ineffective, where one considers the potential interferences in fundamental rights. Prof. Martin Gill further noted that his examination of CCTV systems has taken place in many different jurisdictions on a global level, and that some of his more recent work has focused on gaining insight from criminals as to how they perceive CCTV systems.

Prof. Martin Gill explained that his interviews with criminals as to their views of CCTV in relation to the risks they run in committing crime gave invaluable insights into the systems' impact. It was noted that criminals are very often experts in terms of their understanding of the capabilities of technologies, and they are apt to explain where systems have deficiencies. Further, it was also noted that in examining the effectiveness of surveillance technologies we fail to consider the offenders' views - as such we risk missing out on much needed insight as to how surveillance influences whether persons commit crimes. Prof. Martin Gill then discussed his UK Home Office report authored with Angela Spriggs, which analysed various CCTV systems and assessed their effectiveness. He stated that the report had in some ways been misunderstood by certain parties, in the sense that it should be recognised that the research he conducted in fact pointed toward a general conclusion that it was extremely difficult to say whether or not CCTV was effective as a whole. As such, Prof. Martin Gill was stating that the differences and variabilities between the different systems meant that it was extremely difficult to compare one such system against another. Furthermore, he noted that the answers in themselves were not definitive: they evaluated CCTV as implemented at a very early stage, and that the technology had evolved considerably. Thus, his findings need be considered in the light of such changes.

Prof. Martin Gill asserted that in essence it could be said that CCTV showed very mixed results in terms of whether it was effective. Additionally, it was noted that measurements of effectiveness depend to a certain extent on the criteria one selects for any assessment procedure. Further, it was noted by Prof. Martin Gill that a further concern that frequently failed to be assessed was the necessity to adequately describe the type of CCTV system being evaluated in detail. As such, it should be noted that rarely are any two CCTV systems implemented the same; differences in the systems' functionality thus need to be considered in any assessment.

Prof. Martin Gill then continued his presentation by discussing aspects of the assessment of CCTV system effectiveness, which include the need to ascertain whether the system addresses a specific crime problem. Also, the need was identified as to whether it could be effectively determined whether or not a system was being managed and operated effectively. Prof. Martin Gill suggested then that too rarely CCTV was assessed in terms of whether its use added value in terms of broader crime prevention strategies implemented.

Next, in terms of explaining his research methodology, Prof. Martin Gill discussed the notion of effectiveness in more detail. He then gave as an example a CCTV control unit that was embedded within a police station in the UK. It was noted that this setup allowed police officers to react to incidents swiftly, and thus this might be suggested reflects a capability of CCTV systems to save costs when used effectively.

Prof. Martin Gill then discussed in more detail his research in which he has been interviewing offenders in prison. He noted that he had conducted work in which he replicated certain crime events and asked prisoners as to their opinions in relation to the effectiveness of CCTV in preventing criminal activity. Prof. Martin Gill then gave an example of his discussion with a prisoner who had committed various bank robberies, noting that a security measure (safety screens in banks) did not discourage his committing crime (in fact it proved an asset insofar as he believed that it lessened certain risks for the bank robber). Again, Prof. Martin Gill reinforced his opinion that criminals' views and perspectives were too rarely taken into account when assessing the effectiveness of surveillance systems.

Prof. Martin Gill then discussed the views expressed by convicts he had interviewed in prisons in which they had stated that CCTV rarely deterred them from committing crime. It was noted that criminals could evade identification by wearing a disguise. Also, criminals noted that the image quality of many CCTV systems was very poor: as such, it often failed to adequately identify suspects.

Prof. Martin Gill then discussed his work in which he interviewed ten convicted murderers. He noted that his research had identified that the presence or not of CCTV was not a consideration when a potential murder considered whether or not to commit a serious violent crime.

In conclusion, Prof. Martin Gill asserted that CCTV had mixed effects in terms of the effectiveness of the systems as a whole. His findings might, he suggested, support some parties' affirmations that "nearly everything works, but just some of the time". However, this left open the question why systems prove effective some of the time.

#### ***Q&A Session:***

Stephen Otter (HMIC) asked whether austerity measures had had an impact on how

CCTV was being used in the UK. Prof. Martin Gill answered that spending on CCTV systems in the UK was increasingly open to question, and that more and more people were beginning to question how effective it was, and whether spending on it represented good value for money.

Prof. Martin Scheinin then asked: "How smart is SMART CCTV?" Prof. Martin Gill answered in noting that SMART CCTV looks good as a technology initially, but could easily be evaded or duped - criminals quickly learn measures to avoid detection and identification.

Prof. Tom Sorell asked Prof. Martin Gill for further elaboration as regards where CCTV proves effective. Prof. Martin Gill stated that it was very difficult to generalize as to when CCTV was effective. Further, he noted that the concept of excellence in regard to security measures was also difficult to determine. It remained poorly defined what constitutes excellence in this field. Prof. Martin Gill noted that a further difficulty arose where research findings and, particularly, the capability to name systems that were either effective or ineffective, was limited. Also, it was noted that systems were constantly being evolved, and thus this factor would need to be taken into account. Prof. Martin Gill also noted that it was rare for users to talk of a system's deficiencies; they instead tended to discuss only the positive effects and impacts of such systems.

Dr. Christiane Hoehn then asked whether, nonetheless, we could still identify certain benefits of CCTV. Prof. Martin Gill suggested that generalizations in this regard were still impractical. He then cited his more recent work on the concept of 'security excellence'. He had been looking at corporations' provision of security, and noted that it was extremely difficult to frame excellence as a concept. Similarly, he suggested it was difficult to measure CCTV systems objectively as to whether they were effective.

Prof. Iain Cameron noted that austerity measures could have impacts on different levels. Firstly, he noted that economic problems might make more people within a population inclined to commit crime. Second, it was noted that austerity measures might force parties to reconsider how they could use resources more effectively in implementing CCTV systems. Further, he also noted that mass surveillance using CCTV required a great deal of resources, thus potentially limiting whether it was resource efficient.

Prof. Martin Gill responded by noting that two main factors influenced the uptake of CCTV use in the UK. First, the UK government in the early 90s believed that the systems would prove effective in deterring crime. Second, it was noted that domestic terrorism in the UK in the 90s was also a factor in encouraging CCTV uptake. Furthermore, the high profile case of the murder of Jamie Bulger also raised

the profile of CCTV use in crime investigation. Ms. Michelle Cayford (TU Delft) noted that the report of Prof. Martin Gill for the UK's Home Office had found that CCTV systems used in public car parks did prove effective in preventing crime.

Prof. Martin Gill responded in noting that CCTV had been shown to work in certain circumstances in confined areas where access and departure from a limited area played a role the efficacy of the system.

Sebastian Sperber, the chair of the discussion, then introduced the next speaker of the session, Dariusz Kloza (VUB) who presented the work of the ADVISE FP7 project. ADVISE. ADVISE is aimed at designing and developing a unification framework for surveillance-footage archive systems. Dariusz Kloza then explained the work of ADVISE based on its consideration of the protection of privacy, personal data and ethics. It was noted that a challenge in looking at CCTV archive systems was the fact that surveillance systems grow in scale, heterogeneity and capabilities.

The approach of the project is to work from privacy by design principles using a privacy impact assessment (PIA) framework. Dariusz Kloza then explained the approach of the ADVISE project in relation to the process it adopts for addressing ethical, privacy and data protection challenges in developing unification framework for surveillance-footage archive systems. The presentation then discussed the difficulties in the process of creating a unification framework for surveillance-footage archive systems encountered, including issues relating to different types of PIA where information may not be made available to the public. As regards the publicly available findings of ADVISE research, Dariusz Kloza made available a PowerPoint slide that indicated how PIA findings in the deliverables was shared in public. It was then explained in more detail how ADVISE continues to fine tune its use of PIA, which includes work on risk identification and risk assessment.

It was noted by Dariusz Kloza that the process of conducting PIAs was very much a collaborative process, drawing on the expertise of different parties. Then, Dariusz Kloza presented an overview of the ADVISE PIA questionnaire, which provides draft answers to users as to how PIA is used within ADVISE. The initial results of the ADVISE project were then presented; it was noted that significant risks were found in the categories of ethical issues, privacy, data protection and other fundamental rights. The ADVISE project responds to these risks in the development of a unification framework for surveillance-footage archive systems by providing four response plans to the risks: avoid, transfer, mitigate and accept. Dariusz Kloza then discussed the difficulties encountered in the ADVISE project relating to the challenges of working on PIAs; problems included those of linguistic challenges, perceptions differing as to best practice, and the fact that PIA frameworks change over time. Future work of ADVISE will look at validation of the existing methodology, sharing knowledge and insight with others, and ensuring the continuity of the work

on the PIA after the deployment of the ADVISE project's prototype.

***Q&A Session:***

Sebastian Sperber then asked Dariusz Kloza to clarify the status of the model that ADVISE was developing. Dariusz Kloza confirmed that ADVISE is aimed at designing and developing a unification framework for surveillance-footage archive systems as a prototype.

Serge Gutwirth (VUB) asked how the ADVISE project specified ethical risks. Dariusz Kloza stated that the initial ethical risks identified were derived from the work of a European ethics board. Maria Grazia Porcedda asked how the ADVISE project conceptualized an interference into privacy? Dariusz Kloza explained that the approach is based on a legal framework, which considers the European Directives and case law of the ECtHR.

Prof. Martin Scheinin (EUI) then briefly presented for comparison the work of SURVEILLE in its deliverable D2.6. Prof. Scheinin noted that D2.6 develops a scenario and considers the use of different types of surveillance technology, the results of which are discussed and then presented in a tabular matrix. The types of surveillance analyzed were of both an overt and covert nature. Prof. Scheinin discussed the findings of D2.6 in particular relation to the use of CCTV. The means by which the matrix presents the calculations made as to the gravity of interferences in fundamental rights was then explained. Then, Prof. Scheinin explained the evolving work of the SURVEILLE project in relation to new scenarios. Two new scenarios feature a terrorism-related scenario and second which presents evolving incidents in a community situation. Sebastian Sperber then mentioned how the SURVEILLE Advisory Service may also serve to assist in the development of realistic scenarios for the work of SURVEILLE project to analyse. Dr. Elisa Orru (ALU-FR) then asked Dariusz Kloza as to how the ADVISE project will inform the future use of CCTV by law enforcement agencies. Dariusz Kloza responded in noting that the developed prototype is a functional and practical way by which the model can be used for future development of PIAs.

Sebastian Sperber then presented the work that EFUS has been responsible for in relation to the development of a new scenario in which events taking place in a community are considered in relation to the use of surveillance. The presentation then discussed the different uses of technologies for surveillance; Sebastian Sperber then discussed the latest developments specifically in relation to smart lighting systems as a possible alternative or complement to CCTV. Sebastian Sperber noted that a further consideration in relation to the community scenario was the tendency of the increasing automation on the analysis of data collected from monitoring, and the centralization of this data analysis process. This shifts need to be considered



when risk assessments are conducted, Sebastian Sperber said.

**Q&A Session:**

Jens Kremer (Univ. of Helsinki) noted that Chicago was another US city that had recently invested in a centralized monitoring capability. Jens Kremer then stated that the work being conducted in terms of the assessment of combined technologies should methodologically consider these possible combinations.

Serge Gutwirth (VUB) asked why the scenario had a certain positive or negative outcome. Sebastian Sperber stated that the scenario was just an example scenario, and that in theory either a positive or negative ending to the series of events might evolve, and that of necessity the situations described were simplified. Prof. Tom Sorell (UoW) noted that the scenario is still being developed.

Douwe Korff (London Metropolitan University) noted his concerns regarding the scenario in which individuals may be subject to surveillance absent any suspicion of wrongdoing.

Sebastian Sperber formally closed the session.

**11.30-13.00 Privacy in Public Space**

Session 2 was chaired by Prof. Tom Sorell (University of Warwick) and featured the presentation of SURVEILLE draft deliverable D4.7, titled 'the scope of the right to privacy in public spaces' and authored by Mr. Mathias Vermeulen (EUI).

After introducing himself, Mr. Vermeulen explained that D4.7 aims to clarify the scope of the right to privacy in public spaces in Europe, a topic that became increasingly relevant in conjunction with drones, location trackers and social media. Mr. Vermeulen argued that, although the abovementioned technologies are not considered intrusive, as they do not violate home as the ultimate private space, they can be more secretive (due to the lack of control, and as such affect the core principles of DP), and affect the right to privacy mainly in public spaces. Mr. Vermeulen explained the content of D4.7, articulated in three sections.

Section 1 covered a brief history of the drafting of article 8 of the European Convention of Human Rights. He noted, in particular, that the rationale for including article 8 is its importance for a democratic society; the choice of wording, i.e. 'private life' (vie privée) instead of privacy does not seem to be tied to any value-laden choice.

Section 2 encompasses an analysis of the evolving scope of the right to private life. Since the European Court of Human Rights (hereafter ECtHR) has interpreted the Convention as a living instrument, the scope of the right to privacy has expanded to

include the right to develop social relationships, and the protection of personal data as defined in Convention 108 of the Council of Europe. However, Mr. Vermeulen noted that the ECtHR eschewed providing a definition of the meaning of private life and the other features of Article 8.

Section 3 systematizes the case law of the ECtHR, where Mr. Vermeulen focuses on private life, which encompasses the categories of physical and psychological integrity. Both categories are strained in the public space whenever the individual is 'observed'. He then identified three situations where observation takes place in the case law: search of business/commercial premises (the scope of private life is not limited by the nature of the premise); monitoring cases (private life extends into public space); article 10 cases on freedom of expression affecting the privacy of public figures.

Mr. Vermeulen also discussed the limits of the test of reasonable expectation of privacy (REP), which is used in incoherent ways (cases: *Niemetz*, *Halford*, *Peev and Halford*, *P.G. & J. H.*), and is subsumed under the data protection and social relationship tests. The REP test is relevant in cases of conflict between article 8 and 10 (freedom of information), which are treated differently depending on whether the plaintiff is a public figure (in which case the decisive factor depends on the nature covered by the activities and the goal of the publication).

Mr. Vermeulen then encouraged the audience to provide comments on the following open questions: what are the dangers and usefulness of the reasonable expectation of privacy test? Which links can we build with other SURVEILLE deliverables? Is the right to establish and develop relationships a part of Article 8? Can the right to privacy in public be narrowed down to the mere application of data protection principles?

Prof. Iain Cameron (University of Uppsala) and Prof. Serge Gutwirth (VUB – PRISMS project) provided comments to the draft. Prof. Cameron asserted that it is time to develop a conceptual framework for analyzing privacy, but that looking at case law may be insufficient, because cases look backwards, and depend on contingencies and the doctrine of the margin of appreciation. Prof. Cameron appreciated the taxonomy developed by Mr. Vermeulen on the different cases of public intrusion of privacy. However, he commented that other cases could have been dealt with in details, such as cases based on a generic understanding of the technology (*Uzun*), cases where no intrusion was found and cases where the balance is drawn wrongly.

Prof. Cameron said that Mr. Vermeulen should stress that states have the duty to provide a framework within which balancing is conducted, a process where the test for reasonable expectations of privacy become useful. He then encouraged Mr. Vermeulen to pay attention to the deferential enjoyment of rights, in that different

legal entities (individuals, corporations, media etc.) could be entitled to different levels of enjoyment of a given right.

Prof. Cameron concluded with some theoretical contributions to the debate. He claimed that individuals ought to have a continuation of their private life in public. Privacy should be seen as a residual concept, that is, what is left after the criminal and tort law has entered into the area. Privacy is also a nationally dependent concept: different states draw the balance differently. The ECtHR has always followed a broad conception of human rights.

Prof. Serge Gutwirth (VUB – PRISMS project) reminded participants that every domain of law could generate an ecosystem of cases. He began from the history of privacy, rooted in the XVIII century revolutions, within which the private sphere was created as a shield of protection against the absolutist intrusion and power of the former rulers. Since the first rights formulated were very limited, privacy developed as a juridical invention in court, taken from the dispositions of the constitutions. As a consequence, privacy means liberty, 'la liberté par excellence'. He then suggested considering that privacy lies at the crossroads of two stances, the private and public law perspectives, which is visible in the case law of the ECtHR. On the one hand, the private law perspective (continental European law) requires clarifying the objective of the right to privacy as a substantive right. On the other hand, the public law perspective, sees privacy as the shield against intrusion. In the case of *Laskey and Others* (1997), which involved the practitioners of sado-masochism (interference in private sphere), the Court said the right to privacy had to be seen in the light of the morality of one's deeds. In a later case on sado-masochism, privacy was seen as an issue of liberty instead.

Prof. Gutwirth then commented on the expectation of privacy test, which is used in a contextual manner. But privacy is more than contextual, it is a public good, and therefore protecting individuals against the dangers linked to their consent might be limited: human rights cannot be waived, so consent is not enough. He concluded by saying that privacy and data protection cannot be conflated.

Prof. Sorell intervened to introduce draft Deliverable 4.8 on the ethical analysis of the right to privacy in public, and he reiterated the importance of distinguishing the *forum internum* of the right.

#### **Q&A Session:**

The chair opened the floor for Q&A. Prof. Scheinin stated that it could be said that the right to be left alone is the 'forum internum' of privacy. Moreover, since the 'external' dimension of privacy in social interactions is predominantly a liberty right about the right to choose what to share and with whom, the reasonable expectation theory becomes important for interactions conducted in the public, but should be

dismissed in general for privacy, e.g. whenever we choose a private method of communication.

Dr. Orrù noted that there are important distinctions to make when considering the reasonable expectations of privacy test. There is a difference, for instance, between wanting to take part in a protest, and being identified as one of the participants.

Prof. Korff noted that the protection of privacy couldn't be conflated with data protection and vice-versa. Data protection concerns the power relations that exist in holding information. He suggested looking into the link between jurisdiction and the online context. Dr. Hoehn suggested that Mr. Vermeulen's theory should be applied to Sebastian Sperber's scenario. Mr. Debeuckelaere claimed that the margin of appreciation doctrine is a tool that can be useful as it takes into account two factors; the law, and the notion of reasonable expectation.

#### **14.30 – 16.00 Assessing Electronic Mass Surveillance: the Edward Snowden revelations**

Ms. Michele Cayford (TU Delft) categorized and explained a number of mass-surveillance technologies that were described in a number of recently disclosed internal National Security Agency documents. A first category focused on "splitters" and the use of deep packet inspection technologies. On the basis of publicly available information from the media and from an earlier court case in the US, Ms. Cayford explained that splitters copy to the NSA or GCHQ all information that flows through a specific fibre optic cable. This technology covers what is referred to as 'upstream' collection in the NSA documents. In a second stage, deep packet inspection technology can be used to detect certain types of content, or it can be used to act upon certain detected data (for instance by blocking or prioritizing the transfer of certain data packets). Ms. Cayford treated the 'PRISM' programme as a separate category, since revealed slides claimed that this programme allowed the "direct collection" of data from servers of US service providers. There has been a lot of misunderstanding about the exact meaning of "direct collection", but it appears that PRISM has been more targeted than what was initially thought. However, the exact type of technology that is used in this programme is still unknown. A third category of technologies attempts to circumvent encryption protocols. Ms. Cayford described the use of Foxacid, which is partly used to identify ToR-users. A last category of technologies includes analysis tools and databases. Ms. Cayford explained how Xkeyscore worked in this context. Xkeyscore collects raw packet content data for 3 days and metadata for 30 days.

Prof. Douwe Korff (London Metropolitan University) who had been requested to produce an expert paper for SURVEILLE presented a hypothesis on how the filtering process in the context of upstream processing and Xkeyscore might work. Prof. Korff

emphasized that much of the revealed technologies cannot only be used against legitimate (terrorist) targets, but also for much wider purposes. There is a danger that ordinary citizens are “watched by dynamic algorithms” that are so complicated that they become effectively “uncheckable” and unchallengeable. In this context he referred to the work of Oscar Gandy on “engaging rational discrimination and cumulative disadvantage” which could be interesting for the SURVEILLE project. Finally, Prof. Korff asserted that the world has not yet fully understood the wider (jurisdictional) implications of the recently disclosed internet surveillance programmes.

The president of the Belgian Privacy Commission, Mr. Willem Debeuckelaere, emphasized that there was clearly a period “before” and “after” the Snowden revelations. Nevertheless, from 2005 onwards many data protection authorities have witnessed a desire to move towards more ‘mass’ surveillance, for example in the discussions on the PNR and SWIFT agreements with the US. Mr. Debeuckelaere described his experiences as a member of the ad-hoc EU-US Working Group on “data protection issues” that was established in July 2013. Initially, the main aim of the working group was to establish the facts about US surveillance programmes and their impact on fundamental rights in the EU and personal data of EU citizens, but according to Mr. Debeuckelaere “not that many facts were established”. The main reason for this lack of success was the lack of jurisdiction of the European Commission to discuss issues of national security.

#### ***Q&A Session:***

The Q&A afterwards focused on the difference between data-mining and contact-chaining, whether PRISM was indeed a ‘targeted’ programme, and the need to separate discussions on human rights violations vis-à-vis interferences into a country’s sovereignty.

#### **16.30-18.00 SURVEILLE Assessing Electronic Mass Surveillance**

Prof. Scheinin (EUI) introduced the ongoing work on SURVEILLE deliverable D2.8, then introduced Prof. Sorell (UoW) and Dr. Van Gulijk (TU Delft).

Dr. Van Gulijk presented his work on developing usability scoring for assessing mass surveillance. Dr. Van Gulijk described the approach, which focuses first on the rationale and approach to the method adopted. Dr. Van Gulijk then presented an explanation of the calculation conducted for Robert Alexy's weighting scale, and explained the calculations behind the 10-point scoring system used by TU Delft in D2.8. Dr. Van Gulijk further explained the work on scoring the usability of a surveillance technology, noting that engineers rarely did such a calculation (usability), so it presented some challenges. Dr. Van Gulijk then continued in discussing the level of measurements that were developed and the scales.

The nominal scoring method was then described, in which questions arose in relation to costs (as an indicator). Dr. Van Gulijk discussed in more detail the follow-on work from WP3; the development of the 10 nominal point scores. Elements that were presented included cost, excellence, privacy by design (PBD) and effectiveness.

Dr. Van Gulijk then explained the work on the delivery of surveillance: delivery follows from the initial definition of effectiveness. The assessment of the attribute of delivery hinges on whether the technology delivers the expected outcome. Dr. Van Gulijk then discussed how earlier work for SURVEILLE deliverables D3.2-3.6 had provided insight into the complexity of the matters used in the scoring method.

Dr. Van Gulijk noted that the scoring method had been simplified. Discussion then looked at the use of surveillance in relation to the terrorism scenario developed, Dr. Van Gulijk discussed whether PbD elements could be integrated into the technologies, noting that any assessment was hypothetical in that we couldn't know how the algorithms of covert technologies were developed.

Dr. Van Gulijk then discussed how the scenario featured in the work of D2.8, noting that non-technical surveillance operations tend to be useful as they are highly specific and straightforward. Dr. Van Gulijk then concluded in noting that straightforward point scoring is beneficial but noted that it is crude and requires further development.

Prof. Scheinin then discussed how the scoring system worked in terms of the higher scores representing the better technologies. Prof. Sorell discussed the ethics work of UoW on security and privacy, noting how they developed a theoretical framework. The framework comes from political philosophy. The UoW team looked at what the requirements were for liberal democracy, including the promotion of welfare. Prof. Sorell then discussed the concept of preventative justice, that justice might be framed in terms of being applied after an event, and whether crime prevention should be included in this definition of justice.

Prof. Sorell noted that the UoW team felt that preventative methods were justified in preventing serious crimes. Prof. Sorell then discussed the moral risks that they needed consider such as error, intrusion, consent, discrimination, distinctions of domestic/foreign citizenship, damage to trust, chilling effect, and ethical proportionality. Prof. Sorell noted that there remained questions as to whether mass surveillance was a proportionate response in relation to the threat of terrorism. Prof. Sorell further noted that the distinctions drawn between foreigners and domestic citizens could not be justified. Prof. Sorell then discussed the ethics scores in relation to D2.8. The ethics scores use a traffic light system to measure moral risks. Dr. John Guelke then discussed the moral risks scoring, explaining how different technologies were assigned different colour codes based on risk level. Dr. John Guelke further

noted that moral risks could be assigned individual columns in the matrix in relation to more nuanced views in respect of moral risk level. Additionally, he noted that the moral risk level could be expanded upon with more written descriptions.

Prof. Scheinin then discussed the work of the EUI team working on fundamental rights side of the matrix assessment. Prof. Scheinin noted that Alexy's weighting formula was being used in conjunction with the work by TU Delft. The scale being used by the EUI team is a logarithmic scale (1-2-4). Prof. Scheinin then described how the scale functioned and how scores were assessed and assigned. Prof. Scheinin noted that it was feasible for certain technologies not to be justified in any scenario, based on their being too intrusive into fundamental rights. Prof. Scheinin noted that the resulting scores were very high for mass surveillance technologies in relation to terrorism investigations, and that this was due to the fact that many persons could be affected who were entirely innocent in mass surveillance.

Prof. Scheinin noted that social network analysis scored very differently in terms of the legal assessment and the moral risks. Prof. Scheinin further noted that the work was not yet complete, but was being completed in terms of its ongoing assessments. Prof. Scheinin noted that even where mass surveillance was allowed for under a country's legislation, it breached human rights norms and was therefore impermissible. Prof. Scheinin also noted that the distinction that foreigners had no rights in a jurisdiction was untenable, that human rights norms were such that blanket exclusions of rights based on citizenship were not permissible. Prof. Scheinin then outlined the basis for which interferences into fundamental rights could be justified in a terrorism investigation.

#### ***Q&A Session:***

Prof. Cameron (Univ. of Uppsala) asked a question relating to the cable splitting method of gaining data, noting that different jurisdictions had different limits on the quantity of data that could be collected on domestic law.

Prof. Scheinin noted that the assessments of technologies required several rounds of discussions. Prof. Scheinin further noted that the NSA in general wished to collect all data, if possible. Prof. Scheinin noted that terrorists adapt to threats to their activity. Prof. Sorell noted that liberal democracy would not theoretically allow for large proportions of the population to be subject to suspicion.

Prof. Cameron then asked whether the chilling effect should be considered. Prof. Sorell noted that it was a significant factor. Jens Kremer then asked Prof. Tom Sorell to elucidate the ethical basis for their formulation of privacy in the ethical assessment. Prof. Sorell stated that the chilling effect is different from, for example, the notion of dignity. Prof. Sorell emphasized that the surveillance conducted by the NSA presented risks to democracy; it represented a fundamental risk, rather than a

more narrow risk to privacy. As such, Prof. Tom Sorell expressed concern that mass surveillance represented an overall threat to democracy as a whole.

Prof. Scheinin noted that human rights could be considered pre-cursors to wider aims, such as democracy, such that human rights should be considered first in terms of assessing whether surveillance is justified. Stephen Otter suggested that mass surveillance could be considered an attack on liberal democracy, but perhaps cyberspace has different rules - the state cannot perhaps solve the sorts of problems they now arise online. Prof. Sorell noted that cyberspace could evade jurisdiction, and escape punishment for their activities by conducting activity online. Prof. Tom Sorell noted that surveillance required discretion, that judgment was needed. In the NSA case, Prof. Sorell noted that the amount of data being accessed by authorities could create worrying degrees of control.

Erik Krempel (Fraunhofer) commented that basic notions of gauging privacy interference based on the percentage of data collected didn't prove workable.

Prof. Cameron noted that the idea that cyberspace is beyond jurisdiction is popular in the US. Further, he noted that the US tended to see law only in terms of US law, rather than recognizing international law. As such, Prof. Cameron suggested that the issues around jurisdiction were being resolved differently by different domestic jurisdictions. Prof. Sorell stated that considerations of consent and control need to be considered when analyzing whether mass surveillance is appropriate in a liberal democracy, noting that liberal democracy could be put at risk by excessive surveillance.

Prof. Gutwirth (VUB) remarked that a signatory state to the ECHR should not infringe the rights of others outside its own jurisdiction. Prof. Gutwirth also noted that the US should also respect the rights of persons outside its own jurisdiction. Prof. Scheinin responded that the US position was that they see certain human rights principles as policy, rather than a legal obligation. Prof. Douwe Korff (London Metropolitan University) noted that terrorism is poorly defined in terms of what it constitutes under law. Prof. Scheinin responded that fighting terrorism was a justifiable aim but required scrutiny of how the term terrorism was used. Dr. Van Gulijk noted that the capabilities for mass surveillance were evolving fast, and this was prompting concerns of greater and greater resort to monitoring.

Prof. Scheinin announced details of the Joint Event with IRISS and RESPECT to take place 29-30 October 2014, and further mentioned that things were in motion to merge the SURVEILLE final event with the State of the Union event to take place in May 2015 at the EUI. Prof. Scheinin noted that freedom and surveillance would provisionally be the theme for this event.

Prof. Scheinin then closed the session.



## Day 2

### 9.00 – 11.00 SURVEILLE Work in Progress

#### **Dr. Coen van Gulijk – Presentation of D3.5 Cost Model (submitted 28.2.2014) – work towards D3.8 Results of all effectiveness research (due 31.5.2014) and D3.9 Final report from WP3 (due 31.1.2015)**

Dr. Coen Van Gulijk (TU Delft) presented D.3.5 “Cost modelling of surveillance technologies”. Dr. Van Gulijk first explained that it is difficult to do a cost modelling analysis of surveillance technologies since it is not easy to gain insight into exact prices and costs of these technologies. Two distinctions had to be kept in mind. The first distinction was between conducting a ‘prospective analysis’ and a ‘retrospective analysis’.

The first ‘ex-ante’ analysis aims to determine whether there is a justifiable or feasible investment decision to make. It can also provide a basis for assessing different projects or alternatives. A retrospective analysis can be used for three different goals: justifying the program expenditure of an existing system, evaluating the continuation or expansion of an existing system or evaluating whether an existing system has achieved its intended goals. A second important distinction to take into account was between “cost-benefit analyses” and “cost-effectiveness analyses”.

The first type of analysis compares a programme’s benefits to a stakeholder with the costs to stakeholders (usually in comparable monetary terms). This type of analysis usually does not take into account benefits that cannot be expressed in monetary terms. The cost effectiveness analysis determines how much is spent on a programme to produce a particular outcome. This type of analysis requires the monetization of costs, which is notoriously hard to do. How do you monetize car theft, sexual assaults or – even more difficult – costs of a terrorist attack, let alone the consequences of such an attack? TU Delft decided not to do a quantitative risk analysis, but adopt the cost factors identified in D2.6.

Dr. Van Gulijk further commented on the work that is being done in D.3.8 on the usability scoring. TU Delft is currently developing the usability scoring system that will use a nominal scale. Based on prior reports in WP3 TU Delft is considering 10 nominal score points in four different categories: delivery, simplicity, and sensitivity (to measure “effectiveness”); purchase cost, required personnel and required

external personnel (to measure “costs”); object, collateral intrusion, and technical privacy by design rules (to measure “privacy by design”) and the fact whether a technology has been tried and tested (to measure “excellence”). Deliverables 3.2 to 3.6 have provided some insight into the complexity of the matters used in the scoring method, and TU Delft is currently further refining the scoring method.

#### **Jonathan Andrew (EUI) – Presentation of D6.4 Second dissemination report (due 28.2.2014)**

Mr. Jonathan Andrew (EUI) thanked Ms. De Concini for the excellent organization of the Consortium Meeting. He then explained the nature of the report, which is to list the different dissemination activities carried out by the partners and the consortium. This report developed along the lines of the first, and covered twelve months of activities from January 2013 to February 2014.

The document, Mr. Andrew continued, is 30 pages long and factual. The first part covers the various publications, presentations and speeches given by the partners, whom he thanked for helping drafting the report. The second part recapitulates media activities of two types. On the one hand it covers blog entries, radio and journal interviews and articles published on paper. On the other, it highlights the main achievement of the website.

In the reporting period the website had 2,000 visitors/month, with a total of 3,800 pages viewed. The website has been enriched by uploading the interviews with participants in the two Annual for Fora for Decision Makers and the podcast for the first annual forum for decision makers. The details of the downloads for the research publications are contained on page 12.

The project’s website hosts a Twitter widget. Twitter feeds were used to advertise SURVEILLE-related activities and mention articles that are of relevance for the project. The SURVEILLE twitter account has currently 109 followers, with 36,600 people who saw tweets over the past 12 months (source SproutSocial). The coordinator, Prof. Scheinin, who chaired the session, reported that our partner at Warwick holds a Twitter account too (SURVEILLE Ethics), and opened the floor for questions.

#### ***Q&A Session***

Prompted by Prof. Scheinin, Mr. Vermeulen noted that the reach of 36,600 tweets to the account’s followers show that SURVEILLE bears influence. Dr. Hoehn congratulated the consortium for its activities and asked more information about the coordinator’s testimony for the US Privacy and Civil Liberties Oversight Board. She further thanked for the informative newsletter, and asked an update on the advisory service.

Prof. Sorell explained that the advisory service works by telephone appointment, provided the applicant fill in a form about its expectations of the services of the advice. The advice is then given, and a summary is issued. The advice is currently involved in 20 interactions. The service is used by technology developers in security areas, in particular related to FP7 project, and consortia that do not have a partner expert in ethics. The objective of the service is to increasingly support potential applicants to the EU Horizon 2020 research programme to comply with the ethics requirements. For this purpose the advisory service is active in exhibitions (i.e. the launch of Horizon 2020 in London) and ICT events. Since the deadline for the security call of Horizon 2020 has been postponed to August, Prof. Sorell noted that most requests would come towards the end of the summer.

Prof. Sorell finally explained that advice on the ethics is more requested than on fundamental rights (where it typically concerns questions on the EU data protection regime). Prompted by Prof. Sorell, who asked the partner from Fraunhofer to advertise the advisory service, Mr. Krempel asked whether the service entails signing a non-disclosure agreement, which is usually a precondition for ICT companies disclosing the information. Prof. Sorell said he was ready to sign such non-disclosure agreements, as all interactions are confidential.

Prof. Draper, who is evaluating the service at the University of Birmingham, noted that the recipients of advice are not always completely satisfied with the results of the service, and some potential customers do not request advice because they believe that developing the ethical analysis in their applications is their own competence.

**Dr. Karol Nowak (RWI) – Presentation of D5.2 Report on interactions with law enforcement professionals in a training context (submitted 31.12.2013) and work towards D5.4 Second report on interactions (due 31.8.2014) and D5.7 Proposal for a training course (due 31.1.2015)**

Dr. Karol Nowak (RWI) presented the work of RWI in relation to the deliverable D5.2. Dr. Karol Nowak noted that there had been 5 interactions thus far, and that there would be a further 2 in the spring of 2014. The interactions had targeted police officers in the main, though judges too had also participated. Thus far Dr. Karol Nowak noted that trainings had taken place in Sweden, Turkey and Kenya. A further session would take place in Sweden with Jordanian police officers. Dr. Karol Nowak solicited input from the project partners for more feedback if they wished to provide input as to the progress on the trainings that RWI were conducting. Dr. Karol Nowak also noted that there were risks that some of the information being given in the trainings, for instance information on cost-benefits of surveillance, could potentially be misused.

Dr. Karol Nowak then explained that training had taken place recently in the Police

Academy in Ankara of senior officers. In addition, training took place in Kenya with judges. It was further noted that the training session in Kenya was very useful in terms of the perspective it gave of the situation in Kenya, which differed from that in other jurisdictions where training took place in Europe and Turkey. Dr. Karol Nowak had distributed further questionnaires to solicit input from police officers in Sweden, but it was noted that it was still difficult to get input from these persons, as they were often unable to give sufficient time to complete the surveys (the questionnaires aim to solicit information as to the knowledge of officers about the topics the training would cover).

Dr. Karol Nowak then discussed the future trainings that would take place, on noted that participants tended to fall into two areas: those with a technical background, and those with a less technical background but with legal knowledge. Dr. Karol Nowak noted that it was generally easier to make contact for the purposes of engaging parties in training with the police and the judiciary as opposed to people with a technical background.

Prof. Martin Scheinin then noted that the trainings had been quite different where simultaneous language translation was needed, as opposed to when the trainings were entirely in English. Prof. Martin Scheinin stated that the initial draft of D5.2 had needed more descriptive content.

Dr. Karol Nowak thanked the other project partners for their feedback on the draft of D5.2, then noted that the training module developed would constitute the end result of the ongoing process in relation to conducting training. Brian McNeill (MERPOL) then discussed the work of the law enforcement End User Panel (EUP), noting that the next, fifth session would take place on 23rd April 2014 at Fraunhofer.

At the last session both Brian McNeill and Dr. Nowak discussed with other parties present the use of the questionnaire developed for D5.2. Brian McNeill also noted that feedback was given on the Advisory Service's flyer. The agenda for the next session was currently being finalised. Sebastian Sperber (EFUS) noted that the end user panel involving municipal authorities had been working on the municipality scenario relating to events in a community that is being used for ongoing work in the SURVEILLE project. Sebastian Sperber then invited the project partners to get in contact should they wish to participate in any further activities with EFUS.

#### **Univ. of Warwick Team – Report on work towards D4.9 Profiling at borders (due 31.10.2014)**

Dr. Kat Hadjimatheou (University of Warwick) presented the plans of the University of Warwick's upcoming deliverable D4.9 on profiling at the border, which aimed to identify and discuss the moral wrongs of trafficking and the reasons for its classification as a serious crime, and the ethical risks that arise in connection with the prevention of trafficking at borders. The deliverable will examine how these moral wrongs and ethical risks arise in relation to existing, proposed and potential

techniques used to identify victims of human trafficking at borders. Finally, it will assess the current EU practice around the use of profiling, the use of 'indicators' and the use of databases in this context. A literature review is underway and Dr. Hadjmatheou had completed a number of telephone interviews with relevant practitioners. An agreement for cooperation from FRONTEX' anti-trafficking coordinator was obtained.

### **Sebastian Sperber (EFUS) – Presentation on urban security scenario and discussion on WP2 work beyond D2.8**

Mr. Sebastian Sperber (EFUS) discussed a new scenario on the use of surveillance technologies by local authorities in order to illustrate that the use of these technologies is not limited to police and intelligence agencies. The scenario was based on D2.6 and a 2006 report on the 'surveillance society' by the surveillance studies network. The scenario focused on a day where a large demonstration takes place in a city, and is made from the point of view of an 'urban supervision centre' of city X. Technologies used included CCTV, facial recognition technologies, ANPR, UAVs etc. Mr. Sperber highlighted a number of potential problems surrounding the dual use of certain technologies, function creep and the linking of several of these technologies. Partners were invited to comment on the scenario, and it was agreed that other partners (and not EFUS) would do the scoring.