SEVENTH FRAMEWORK
PROGRAMME

FP7 – SEC- 2011-284725

SURVEILLE

Surveillance: Ethical issues, legal limitations and efficiency

Collaborative Project

SURVEILLE Deliverable 5.3: Report of second Annual Forum for Decision-Makers

Due date of deliverable: 31.10.2013

Actual Submission date: 29.10.2013

Start date of project: 01.02.2012 Duration 39 months

SURVEILLE Work Package number and lead: WP05 Prof. Tom Sorell

Authors: Ms Céline COCQ (IEE – ULB)

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

SURVEILLE Deliverable 5.3: Report of second Annual Forum for Decision Makers
(FP7-SEC-2011-1; Grant Agreement No. 284725)
West Midlands European Centre, Brussels, 23 September 2013

Attending:
Please see the annex for the list of attendees.

Accompanying documents (annexed):
1. Meeting schedule
2. List of attendees

Presentations:
PowerPoint (.ppt) presentations are available on request from the SURVEILLE Project Manager, Jonathan Andrew, via email: jonathan.andrew@eui.eu.

REPORT

Opening of the meeting

Prof. Anne Weyembergh (IEE-ULB) welcomes the participants, audience, speakers and partners to the second "Annual Forum for Decision-Makers."

Prof. Martin Scheinin (EUI) presents the state-of-play of the SURVEILLE Project, which includes a brief presentation on the "Matrix of Surveillance Technologies" (Deliverable D2.6), which represents the collaborative efforts of the SURVEILLE project partners.
Martin Scheinin also reflected upon the NSA and GCHQ revelations, which become the focal point of the policy debate during the afternoon.
Finally, Martin Scheinin explains that this year's "Annual Forum for Decision-Makers" will focus on the WP3 of the project: perception and effectiveness of surveillance technologies.

First Panel: Assessing Effectiveness and Efficiency of Surveillance Technologies

1.1. Dr. Claudia Diaz (KU Leuven – Member of the Advisory Board): chairs and introduces the speakers

1.2. Presentation: D3.4 and D3.5 "Effective and/or Efficient Surveillance Technology" - Dr. Coen van Gulijk (TU Delft)

Although there is no clear-cut definition of security, any security technology is required to be effective and efficient.

A heavy emphasis is placed on aviation security, focusing on the IACO 7300 – Convention on International Civil Aviation. According to the Convention, the development of civil aviation at an international level can help establish and build friendly relations as well as understanding among the States and peoples globally. However, if abused, it can become a serious threat to security.

Within the project's framework, several criteria play a role in the development of surveillance technologies for the purpose of strengthening security (WP3). They include;

- Effectiveness
- Efficiency
- Perception
- Satisfaction
- Cost considerations

These criteria need to be considered in a systematic manner in order to make coherent decisions.

Surveillance technology is considered effective when it *has the technical capacity to deliver the intended security goals, and when employed for a defined goal within the necessary context (good location, trained operators, a larger security system, etc.) achieves the intended outcome.* Therefore, clear goals are required.

Surveillance technology is considered efficient when it *delivers the intended security goals with low use of resources in terms of cost, time and/or physical and mental efforts.* The financial cost is the primary consideration. However, a NSA programme, even if efficient, can be extremely costly.

The efficiency criterion follows the one of effective. For example, cameras need to work effectively before analysing their efficiency.

For investigative purposes, the choice of surveillance technology, and its use, should pass a series of steps, including:

- An analysis of the crime itself
- Selecting a suitable surveillance tool, which is appropriate for the investigation
- Use of the technology
- An assessment of its use, which incorporates a risk analysis
- Records are analysed according to the effective/efficient criteria, which will be made available for future use.

Case study used: sound-recording in a hotel room.

It is important to note that the deployment of the surveillance technology is determined by political decision-makers. However, it is the "technicians", who, subsequently, determine the best method, which is to comply with the criteria of the decision-makers.

1.3. Presentation: D3.3a "Perception and Effectiveness to Surveillance" - Mr. Erik Krempel (University of Fraunhofer)

Different technologies can be employed to undertake similar surveillance tasks. The question of compliance with the national and EU data protection regulations raises important issues. Privacy is fundamental and must be taken into account when determining the most appropriate surveillance system and technology. An assessment of the application is important not only for privacy protection but also to verify the quality of the data gathered via these technologies. Such an assessment must be available to users.

The software discussed in Deliverable D3.3a of the SURVEILLE project is particularly useful:

- To allow for an immediate assessment prior to deployment of a surveillance system
- To keep balance between the rating of every dimension and the speed
- To enable rating broad variety of surveillance technologies (phone-bugging *versus* complex IT system for data-mining)

1.4. Presentation: D3.3b "Assessing Effectiveness and Efficiency of Surveillance Technologies by Human Factors Evaluation" - Mr. Ralf Eck (University of Fraunhofer)

Evaluation of the usability of surveillance technology for users, such as security forces, designers and developers of technologies.

The objective is to assist them and if this is not possible, to provide some tools, such as:

- Approach by using human factors standards
- Collection of relevant standards (*e.g.* ISO, CEN)
- Development of a methodology to find the best standard
- Producing software
- Evaluating the approach

Because of the importance attached to standards, it is necessary to choose the optimal standard according to tools such as a decision-tree to assist in establishing clarity and applicability. Then, the standard is adapted to the specific security needs required by the end-users. Some difficulties have been encountered; for example, there is a lack of answers and statistical information. In October, the "End-User Panel" of SURVEILLE will provide inputs as well as develop the potential answers.

1.5. Comments from Mr. David Trembaczowski-Ryder (ACI-Europe - Head of Aviation Security): "Airport Operational Perspective"

Prior to 9/11, all EU Member States were responsible for their own airport aviation security. In the aftermath of 9/11, the EU Commission made steps towards establishing a common regulation for airport aviation. Regulation (EU) 185/2010 imposes airport requirements along territorial boundaries, in the security-restricted zones and critical parts of security restricted areas.

To assemble a bomb costs between 3.000 to 5.000 euros; however, for the industry to protect us from them costs millions of Euros.

For security purposes, surveillance is required at airports. However, a number of criteria are taken into account, which include:

- The size and the layout of the airport
- The number and the type of operations
- The restrictions on measures to undertake airport surveillance

Video-surveillance is the main technology used for this purpose. A question raised by a participant is whether it is effective to monitor all areas?
Mr. David Trembaczowski-Ryder gives the example of the Domodedovo bombing that took place on 24 January 2011. This incident illustrates the need to secure all areas in an airport. Since this event, additional police and security checkpoints have been installed at the entrance of airports.

Video-surveillance enables and improves:

- A large coverage area
- More efficient use of staff resources
- Tracking
- Command and control during incidents
- Incident investigations.

Surveillance technologies have been implemented to respond to the threat of terrorism; however such technologies need to be regulated properly in order to comply with EU regulations.

1.6. Q&A Discussion

Audience: Milton Mueller asked if there is a trade-off between intrusiveness and effectiveness? Is it possible to quantify human rights when evaluating the implications of the use of these technologies within algorithm calculations?

Dr. Coen van Gulijk answered that it is possible in this context. It also depends on the manner in which the effectiveness/efficiency dichotomy is analysed. Furthermore, engineers fail to take in account human rights when decision-makers do not provide a specific set of criteria.

Prof. Martin Scheinin: SURVEILLE employs a combination of surveillance technology assessments on multiple grounds, including fundamental rights. In respect of the scenario used in Deliverable 2.6, the right to privacy and the right to data protection proved to be most often affected; nonetheless, non-discrimination and equality, as well as freedom of movement and freedom of expression are also influenced but not on the same scale.

Question of Mr. Christian D’Cunha: In your assessment of effectiveness Dr. Coen van Gulijk highlights the necessity to reduce crimes. Does the matrix assess key performance indicators?

Do you assess the impact of the use of the technologies on human rights? You have to take into account that it may be the cumulative effect of a particular measure, which adds to the existing measures.

Dr. Coen van Gulijk: Goals are set and they must identify the type of crime that the technologies have to deal with.

Question of Mr. Barry Owino (ULB Student): How do you define a suspicious passenger?

Answer of Mr. David Trembaczowski-Ryder: Profiling is carried out by customs officers. A passenger’s travel pattern and behaviour are key indicators in the profiling process. In addition to the customs officers, there are behaviour detection officers at airports, who carry out behavioural analysis.

Prof. Tom Sorell (University of Warwick): The D2.6 is a matrix but not an algorithm. All technologies are not included. It is primarily based on a crime scenario, which involves different challenges for an investigation. This matrix provides relative rates concerning the technologies chosen as case studies, including for usability, ethics and law..

Question from a member of the audience: Is the behaviour analysis not better than a machine?

Mr. David Trembaczowski-Ryder: Airports are huge. There are thousands of different kinds of cameras, which cater for night and day, good and bad weather, etc.. In the case of largest airports, the systems are fully integrated.

A question to ask is why is it mandatory for laptops to be removed from laptop-cases?

The answer is because it is possible to detect sheet explosive inside laptops. More and more liquids are restricted and controlled because liquids can be used to create liquid explosives. It is interesting that H_2O, (water) is just one molecule short of H_3O, which is a precursor to explosives.

Dr. Claudia Diaz asked Mr. David Ryder if profiling is used, is there a way to ensure that this does not result in racial profiling, etc. Do you have any statistics on this matter?

Mr. David Trembaczowski-Ryder answered that profiling concerns behavioural analysis. It is a question of appreciation based on criteria. He considers that he cannot say that no abuse occurs but such an assessment is controlled.

Prof. Martin Scheinin: The Passenger Name Records (PNR) also exist and they contain information that may be used for ethnic profiling, e.g. by using dietary choices as a proxy.

Mr. David Trembaczowski-Ryder: PNR is not allowed for aviation security in Europe although such an endeavour has received support.

Dr. Coen van Gulijk: A more accurate system can be developed to assess effectiveness and efficiency that would be better than the current state of affairs. An important criterion when using these technologies is transparency.

Mr. David Trembaczowski-Ryder: There are a growing number of airlines, which use behavioural analysis, PNR data analysis and financial data to profile. The effectiveness and data retention are related to issues of proportionality. Data retention has subverted a number of bombings. However, data is not made available to the public and the degree of intrusiveness is not openly discussed. There is always a necessity to conduct assessments, especially in cases when measures have failed.

Second panel: Perception of Surveillance Technologies

2.1. Dr. Kevin McNish (University of Leeds): Chair

2.2. Presentation: D4.5 “The Presumption of Innocence as a Moral Norm of Criminal Justice: Surveillance, the Right to be Free from Stigmatisation” - Dr. Katerina Hadjimatheou (University of Warwick)

The presumption of innocence is a moral norm or a moral right granted to individuals under suspicion. In this context, a pre-suspect is a person who is thought more likely to become a criminal in the future.

Two important factors must be taken into account:

- The right to be free from stigmatisation
- The right to be trusted and a presumption of innocence.

The objective is to avoid that surveillance results in creating a no-trust society.

Stigmatisation may be defined as marking a person out as having an undesirable character. It could be viewed as a form of humiliation or isolation from the rest of society. The act of stigmatisation has an effect on people stigmatised as well as society itself. There is a loss of trust in authorities. How can stigmatisation be legally justified? Criminal stigmatisation resulting from surveillance is justified if supported by evidence of unlawful harm and it is proportionate to the reduction of a specific kind of crime.
It amounts to a violation of the right to be free from stigmatisation when the use of surveillance is unnecessary and when it imposes a stigmatized label that is impervious to evidence of innocence.

The surveillance of pre-suspects can be defended because of the following:

- The strength of previous criminal behaviour
- The likelihood of recidivism
- The seriousness of the harm prevented
- The difficulty of obtaining evidence of imminent crime that is reliable enough to justify coercive preventive measures

Police may record interactions including those involving suspicious individuals and by extension their relations. However, domestic violence, one of the most serious threats if not the gravest, is difficult to establish before its commission and so it is difficult to protect people from it.

People need to be reassured when taking a flight, especially when accompanying children. Children are seen as the most important societal value to protect. However, there is an increased demand for the imposition of checks and balances. A potential presumption of guilt would justify a serious intrusion of privacy.

Finally, the presumption of innocence is not just a right but requires special attention and care. Surveillance affects trust but it is difficult to find empirical evidence to support this finding. We have to consider the stigmatisation/trust cost when analysing surveillance.

2.3. Presentation: D3.2 "Review of European Level Studies on Perceptions of Surveillance. Negative Perception, Effects, Side-Effects and Perceived Effectiveness" - Ms. Elisa Orru (Albert-Ludwig-University Freiburg)

The first premise concerns the difficulty in comparing different sets of data and how to make decisions based on this information. The results depend on the cities, the risks and the locations. For example, the answers in Vienna (41% of negative perception) are not the same as in London (only 4%). The studies are heterogeneous because of the type of questions posed to the respondents, the range of population targeted and the kind of surveillance referred to.

Question on the negative effect of surveillance: “Negative” perception is defined as the *perception subjectively associated with feelings such as unease, fear, annoyance, etc. or influencing a person’s attitude toward surveillance in a way that brings this attitude closer to criticism or rejection than it was previously.*

The results are based on two main studies: Urban Eye and Flash EUROBAROMETER 225.

Objectives of surveillance technologies include the desire to reduce fear of crime, to reduce criminal activity and to decrease the potential misuse of such technologies. In fact, the negative perception is context-dependent (*i.e.* CCTV in banks or in public places). However, according to the data, the negative perception is not a limited phenomenon. The methodology can have an influence on several results and sometimes the results appear to contradict each another.

The majority of people interviewed do not see surveillance as effective: Urban Eye reveals that 55% of the population consider that CCTV “displaces rather than reduces” crime and in Hamburg, almost 60% consider that it displaces instead of solves the problem of crime.

Finally, perception issues are part of the actual effectiveness of a measure. The perception has an impact on the assessment of effectiveness. However, there is no cause-consequence relationship between the two.

2.4. Comments from Prof. Sabine Roeser (TU-Delft):

Perception plays an important role and is not a marginal issue. It has a major impact on actual effectiveness. It is important to integrate moral values. The use of data should not be viewed and used in a technical way only. It is important to take into account the public perception of technologies, especially moral values, when creating new surveillance technologies.

How do ethics and studies on the public perception of technologies impact the development of technology?

Ms. Elisa Orru argues that we should distinguish between actual and perceived effectiveness. Very often we think about perception as something emotional, not based on sound information, and actual effectiveness on the basis of statistics, etc. Is this correct?

Dr. Katerina Hadjimatheou pointed to the ethical issues, which are raised in surveillance. It might be that the public’s perception is not well-informed but it also encompasses moral values, like fairness, justice, etc.

These values are frequently not incorporated in studies, which are of a technical nature, when assessing “actual effectiveness.” However, moral values should be integrated into the development of technologies.

If technologies are considered “justified”, then they are well-perceived even if it involves a potential violation of privacy. While technologies are considered “unjustified” if their negative effects on privacy largely exceed the security threat. When States and their citizens feel insecure and unsafe, States implement more surveillance and there is an increase in privacy violations. The most worrisome problem is that we do not know how much of our personal data is under surveillance.

It came as a surprise when US President Obama stated that “we are not surveilling American citizens” even though NSA is gathering large volumes of data on US citizens. Political international relations do not have an ethical perspective. In this context, what is the role of Europe? Could the EU develop technologies that take into account the protection of data as well as values?

2.5. Q&A discussion

Prof. Iain Cameron (University of Uppsala) comments on the first presentation and reminds that the *S and Marper* ruling by the European Court of Human Rights on DNA retention includes a passing reference to the presumption of innocence. There is an important threshold between what can be authorised, such as data collection, and what is problematic, such as the release of information to others.

Dr. Katerina Hadjimatheou contends that there is no reason to have only one threshold. More content can be given.

Mr. Ivan Koedjikov (Counter-Terrorism Coordinator in the Council of Europe): The very important threshold is whether or not the person is aware that she/he is under surveillance. For instance, analyses of online banking behaviour remain undisclosed and we do not know what the banks are permitted to do and what they actually do.

Are we in the Minority Report world, where the surveillance technologies govern the world? In this case, reference should be made to the project FAST; people may interact with you based on face recognition technology.

Another question raised: How far can we adapt the old checks and balances?

Dr. Kevin MacNish says that providers claim to have succeeded in designing immediate facial recognition.

Ms. Elisa Orru: Do you have other options? Is there a different way to travel without being under surveillance? Is there any other possibility to work without email correspondence? Thus, the key question is: what can we do even if we are aware?

Prof. Martin Scheinin: The awareness of people of being under surveillance is not a singularly decisive criterion but it is one of the elements, which is factored into the assessment of intrusiveness.

Dr. Katerina Hadjimatheou: The assumption that everybody is suspicious cannot justify data retention and invasion of privacy. However, such activities serve as a means to gather evidence in advance. It is important to note that the gathering of this information is not being monitored, but rather it is profiling. There are two different approaches, which necessitate a distinction between gathering data and privacy intrusion.

Prof. Tom Sorell asked what is the threshold for the panopticon.

Prof. Sabine Roeser: There is a significant difference between CCTV surveillance and prison surveillance. Governments have access to data stored by companies and undertake analysis, which go beyond the panopticon. The downside of these activities is that they give away privacy.

Prof. Tom Sorell: Isn't there a danger also in the business world and business practice? Industries, banks and other commercial business are treating us like potential consumers for commercial purposes. In addition to this, it is not part of a once-off phenomenon; even though the data can be used by government, it remains the same data. Is the existence and deployment of CCTV cameras sufficient to talk about a panopticon?

Dr. Katerina Hadjimatheou explains that while she focuses on trust and stigmatisation, this does not mean that other fundamental rights are not at risk of being violated.

Dr. Kevin MacNish considers that efficacy and acceptability are very important in the assessment of perception. Isn't public perception simply an issue of education in order to inform the public of its significance?

Ms. Elisa Orru disagreed. In the perception assessment, a part of it also includes effectiveness. The issue of transparency is not just based on education. Transparency will not necessarily lead to further public acceptance.

Prof. Sabine Roeser says that it is difficult nowadays to exercise choice in the use and means of communications. The public is alerted to this fact but more data than before is required. Technology has a moral responsibility to take into consideration values.

Prof. Iain Cameron considers that surveillance technologies should be placed within the context of the ECHR jurisprudence. On data retention and issues of privacy, people are protected by Article 8 of the ECHR. Is this a movement towards a mass surveillance society or a backward move? The study of perception could cover areas that have evaluated surveillance technologies already, such as the financial tracking system. The European

Commission sought an evaluation on this and managed to have an assessment carried out. Nonetheless, there are areas that have never been evaluated.

It is very interesting to look at the case of the United Kingdom where the impact of technology on crime level has been evaluated. According to the evaluation, the impact is much lower than what UK government claims.

Third panel: Policy debate

- **"The Future of European Data Retention and Data Transfers for Law Enforcement and Intelligence Purposes after PRISM?"**

3.1. Session 1: State of Play following the NSA Revelations

3.1.1. Mr. Mathias Vermeulen (EUI): Chair
He introduces the participants.

3.1.2. Mr. Ahmed Ghappour (University of Texas): **American Perspective**
PRISM is the preferred means of data collection because it receives the data directly from the company and they do not have to process it.

On the one hand, the NSA surveillance is a data storage system of metadata. The metadata includes details of communication records in the framework of authorised investigations and foreign intelligence information. It also covers more general information relating to the fight against terrorism. PRISM allows the NSA to receive data directly from US companies. 99% of global communication travel over the United States via sea fibre-optic cables. On the other hand, the Xkey serves as a search engine for data already collected.

The NSA does not keep all data. In the 3 to 5 days after the data is collected, it is verified in order to determine its significance. If it is significant, it is retained for one year. There is no specific law prohibiting the retention of data. Section 215 of the Foreign Intelligence Surveillance Act allows for communication details record to be gathered while Section 702 allows for the content of the communications to be collected.

What can NSA target for long-term storage?

- Specific targets
- Metadata pertaining to individuals as many as three degrees removed from the specific target

This data is used in law enforcement, emergency responses, intelligence analyses, etc.

Case study: *United States* v *Moalin, et al.* The accused denied being a terrorist but allegedly transferred funds to terrorists. The initial information collected by human techniques in the investigation did not reveal any connection with terrorist groups.

Questions for discussions:

- Why automated analytics? Simply because it does not require a court order.
- Once data is obtained, are automated analytics fair?
- What activity is permissible with the results?
- Could it be possible to challenge the integrity of the intelligence?
- What does this mean for traditional methods of law enforcement?

Indeed, the more we rely on computerisation, the more likely it is to compromise our traditional law enforcement procedures. In addition to this, it now includes less serious crime crimes like financial crimes. It also includes independent actors with no affiliation to terrorist groups..

3.1.3. Dr. Ian Brown (Associate Director, Oxford University Cyber Security Centre): "Regulation of Large Scale Interception in English Law": National Perspective

The Regulation of Investigatory Powers Act (2000) ("RIPA") regulates on a large scale, the interception of telecommunications in the United Kingdom. The majority of communications from the USA to the EU pass through the UK. Tempora, the code name of the Government Communications Headquarters (GCHQ) programme, is an important part of cooperation with the NSA, which engages with non-domestic data traffic.

Section 8 of RIPA enumerates the situations when a warrant is not required for interception. It includes interception carried out outside the UK territory. In this case, there is no need to specify whether this type of interception concerns an individual or a private place. The scope of the interception is extremely broad because it includes national security, which is a far-reaching term, as well as the economic well-being of the United Kingdom. With regard to the latter, this term is even more illusive than the topic of national security.

Section 12 of RIPA enumerates the competent authorities and the rules of authorisation. There is no need for a specific interception order to be authorised by the government.

Concerning ECHELON, Section 94 of the Telecommunications Act 1984 states that if the interception relates to private companies, this measure is permissible in the interests of national security. The main problem is that this opens up the possibilities too broadly. Section 7 of the Intelligence Services Act 1994 deals with the authorisation of acts outside the territory of the UK (*e.g.* case with Belgacom 2013) If the GCHQ wants to escape the law, the government can permit this.

How do we should create an EU-model, which is more protective of human rights?
The question at the national level is whether the statutory framework in the UK is sufficient.

The objective is to preserve the rule of law at a national, European and international level. However, the EU has no competence in intelligence matters. Consequently, it is a challenge to determine how to implement meaningful checks and balances at the European level. Would it be possible to request warrants to implement oversight and/or to make calls for further transparency? Such possibilities, even from a purely economic perspective, are not particularly efficient.

3.1.4. Dr. Christiane Höhn (Adviser to the EU Counterterrorism Coordinator): European Perspective

She makes a request to speak off the record.

.

3.1.5. Q&A Discussion

Dr. Ian Brown: One of the key principles of data protection is to minimise the collection of data. If data is collected for the purpose of counter-terrorism and counter-espionage, it is extremely tempting to use data for other legitimate public purposes. The Drug Enforcement Agency uses NSA information for drug prosecutions. Taxes investigation bodies are also gaining access to this data.

However, what will it happen in the future?

Question from a member of the audience: Are there statistics indicating how valuable US information is?

Prof. Emilio de Capitani is surprised that many are so clear in separating national from European security. Article 4(2) is not exceptional but is interpreted in an abusive manner. Governments cannot use this exception to jeopardise the very notion of European security, which is not simply a matter of adding to it the national security of its Member States. After 9/11, there has been a grey area so that we do not know if information has been collected for intelligence purposes or police or judicial cooperation. Regarding SWIFT, data is collected for intelligence purposes but the legal basis is police and judicial cooperation in criminal matters.

Why do we want more intelligence cooperation with the US and not among the EU Member States?

Dr. Ian Brown: The Optional Protocol to the Cybercrime Convention should be a suitable option for the Council of Europe (CoE) because it may also involve non-EU Member States.

There is a movement away from a multiplication of non-traditional norms to traditional international law.

Mr. Ahmed Ghappour: There is clearly an issue of effective oversight. I am pessimistic and I think we are moving towards global surveillance. This is the problem with national security; we have created an enemy with no national boundaries. Furthermore, the new theatre of war is the cyber-theatre with no enforceable system of oversight. It can, therefore, be easily evaded.

3.2. Session 2: Legal responses to the NSA revelations

3.2.1. Prof. Martin Scheinin (EUI): Chair

3.2.2. Mr. Christian D'Cunha (DG Home Affairs, European Commission)

He presents the EU data retention regulation. This regulation was essential to harmonise the conditions of the EU internal market.

The rules are constantly being evaluated in order to improve EU regulation. The Commission launched several consultations with industry and law enforcement forces, in light of the possible limitations in the retention of data.

There are three difficult areas: availability, accessibility and accountability.

3.2.3. Prof. Cees Flinterman (United Nations Human Rights Committee)

Human Rights Committee will soon have a dialogue with the US on the implementation of the ICCPR by considering a periodic report.

He focuses on three issues

- Article 17 ICCPR
- Article 17 is viewed as a fragile basis to address current issues
- The need to focus on the implementation of State Parties under Article 17

The Universal Declaration on Human Rights includes an article on privacy protection (Article 12), forming the basis for Article 17 of the International Covenant on Civil and Political Rights. This article does not set down the criteria for the lawful restrictions on this right.
The Committee is the monitoring body of the Covenant and the correct forum to discuss Article 17 issues as well as its possible improvement.

He discusses two proposals: The German proposal of an Amending Protocol to be ratified by states to strengthen Article 17, and a common proposal of Special Rapporteurs that the

Human Rights Committee adopts a new General Comment as an interpretive document under current Article 17.

- It is interesting to see the recommendations of the Special Rapporteur on Human Rights and Counter-Terrorism and the Special Rapporteur on Freedom of Expression, including to include in a General Comment a permissible limitations test. The restrictions should be established in law and serve particular and specific aim(s) as well as be proportionate and necessary.

- Regarding the German proposal of an Amending Protocol, this would take the discussions to a broad intergovernmental forum and allow for input by NGOs and broader civil society. However, the negative issue is the difficulty to predict the duration of the negotiations.

The two proposals are not mutually exclusive. In each case, it is important to have more input from NGOs.

3.2.4. Q&A Discussion

According to Prof. Martin Scheinin, the Human Rights Committee has been very explicit in articulating that human rights have to be applied beyond national borders. If one or more EU Member State would generate an inter-State complaint against the United Kingdom or the United States, would this cause a shock?

Dr. Claudia Diaz notes that a further problem is that there is no protection if you are a non-US national. The blurring of intelligence agencies, national security and law enforcement may not be the best solution. If they were separated at the beginning, then it was probably for good reason. How should they interface today?

Prof. Iain Cameron considers that the European Parliament should be granted competency in this domain.

In relation to the work of the CoE, we should have a look to the report on best practices of security agencies.

What can we do in the meantime regarding the NSA problem? Only the US can legislate in this field. We can only express our dissatisfaction and make recommendations to the US to improve its oversight measures.

Mr. Christian D'Cunha has been involved in drafting the EU's internal security strategy. The EU is still at the early stages of performing governance in the area of security. It is a very new area of law. The problem is how can the EU legislate when a large chunk of the population thinks there should be no competency in this domain.

Dr. Ian Brown: The Commission asked for a Directive governing proportionality. The European Court on Human Rights (ECtHR) has struggled with the issue as illustrated in the case of a DNA database of UK nationals.

Prof. Emilio de Capitani: After the entry into force of the Treaty on the Functioning of the European Union, data protection is no longer considered to be an internal market issue. The EU as a supranational entity needs to establish standards to be defended by Germans in international forums and/or before the CoE.

Mr. Christian D'Cunha: The crucial question is how can the EU have an input and add value in the area of security in Europe. Even before the revelations during the summer this question was asked in light of the EU's identity crisis (*e.g.* extent of EU competence).

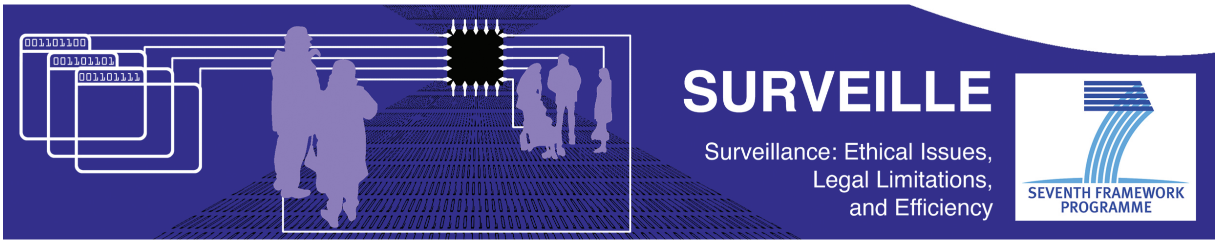
Closing of the second Annual Forum for Decision Makers

Dr. Francesca Galli (IEE-ULB) expresses a word of thanks to the speakers for their presentations and involvement in the discussions, the partners for their work and the audience for their participation. She concluded with a briefing about the Third Annual Forum for Decision-Makers, which will also be a joint event with FP7 projects IRISS and RESPECT, which will take place in Brussels next year (end of October 2014).

The Annual Forum closed at 17:30.

Annex

1. Meeting schedule:


0011101100
0011101101
0011101111
SURVEILLE
Surveillance: Ethical Issues, Legal Limitations, and Efficiency
SEVENTH FRAMEWORK PROGRAMME

SURVEILLE's
Second Annual Forum for Decision Makers
Monday 23th September 2013

"Perception and effectiveness of surveillance technologies"

9:00 **Arrival:** West Midlands European Centre, 22-28 avenue d'Auderghem, Brussels

9:15 **Opening of the meeting** (Prof. Anne Weyembergh, IEE-ULB)

Project status report

9:30 **State of play** (Prof. Martin Scheinin, EUI and former UN Special Rapporteur on the protection of human rights while countering terrorism)

9:45 – 11:15: Assessing effectiveness and efficiency of surveillance technologies

Chair: Dr. Claudia Diaz (KU Leuven)

9:45 – 10:30 Speakers: Dr. Coen van Gulijk (TU Delft), Mr. Erik Krempel (University of Fraunhofer) and Mr. Ralf Eck (University of Fraunhofer)

- ➢ Comments from Mr. David Ryder (Airports Council International Europe)

10:45 **Q & A Discussion**

11:15 **Coffee break**

11:30 – 13:00: Perception of surveillance technologies

Chair: Mr Kevin Macnish (University of Leeds)

11:30 – 12:15 Speakers: Dr. Katerina Hadjimatheou (UoW) and Dr. Elisa Orru (University of Freiburg).

- Comments by Prof. Sabine Roeser (TU Delft)

12:40 **Q & A Discussion**

13:00 **Buffet lunch**

14 :00 – 17 :00 debates: The future of European data retention and data transfers for law enforcement and intelligence purposes after PRISM

14:00 – 14:45 Session 1: State of play: the NSA revelations

Chair: Mathias Vermeulen (EUI)

- Dr. Ian Brown (Associate Director, Oxford University Cyber Security Centre)
- Dr. Christiane Höhn (Adviser to the EU Counterterrorism Coordinator)
- Mr. Ahmed Ghappour (University of Texas)

14:45 **Q&A Discussion**

15:15 **Break**

15:45 – 16:30 Session 2: Legal responses to the NSA-revelations
Chair: Prof. Martin Scheinin (EUI)

- Mr. Christian D'Cunha (DG Home Affairs, European Commission)
- Dr. Christopher Kuner (Senior Counsel, Wilson Sonsini Goodrich & Rosati)
- Prof. Cees Flinterman (United Nations Human Rights Committee)

16:30 **Q&A Discussion**

17:00 ***Close of session*** (Dr. Francesca Galli, IEE-ULB) *and coffee*

2. List of attendees

SURVEILLE Annual Forum for Decision Makers

23th September 2013, West Midlands European Centre, Brussels

First Name	Surname
Eecke	ALTENA
Stéphane	ALONSO
Jonathan	ANDREW
Ralf	BENDRATH
Francesca	BOSCO
Philipp	BOTTCHER
Clémentine	BOULANGER
Chloé	BRIERE
Noellie	BROCKDORFF
Ian	BROWN
Ciara	BURBRIDGE
Antoine	CAHEN
Iain	CAMERON
Joseph	CANNATACI
Céline	COCQ
Charlotte	CONINGS
Michèle	CRAWFORD
Tomaso	CRESTO DINA
Christian	D'CUNHA
Emilio	DE CAPITANI
José Manuel	DE FRUTOS GOMEZ

Kristel	DE SCHEPPER
Claudia	DIAZ
Heather	DRAPER
Christian	FELD
Kirsten	FIEDLER
Cees	FLINTERMAN
Francesca	GALLI
Ahmed	GHAPPOUR
Maria Cannella	GIUSY
Andy	GOLDSTEIN
Gloria	GONZALEZ FUSTER
Margaret	GORMAN
Nathalie	GRIGNARD
Marga	GROOTHUIS
John	GUELKE
Katerina	HADJIMATHEOU
Christiane	HOHN
Katrin	HUBER
Iryna	IEVDOKMOVA
Alexander	KAHAN
Ivan	KOEDJIKOV
Jens	KREMER
Erik	KREMPEL
Christopher	KUNER
Juha	LAVAPURO
Kevin	MACNISH
Brian	MCNEILL
Milton	MUELLER
Sylvie	MURENGERANTWARI
Carmen	NECULA
Nielsen	NIKOLAS
Nitoi	NITOI

Karol	NOWAK
Tuomas	OJANEN
Elisa	ORRU
Barry	OWINO
Pavel	PALENCAR
Michele	PANZAVOLTA
Maria Grazia	PROCEDDA
Carl	PIRON
Eck	RALF
Gavin	ROBINSON
Sabine	ROESER
Ruben	ROEX
David	RYDER
Ludovic	SAAS
Martin	SCHEININ
Simone	SILLEM
Tom	SORELL
Brooks	TIGNER
Coen	VAN GULIJK
Mathias	VERMEULEN
Anne	WEYEMBERGH