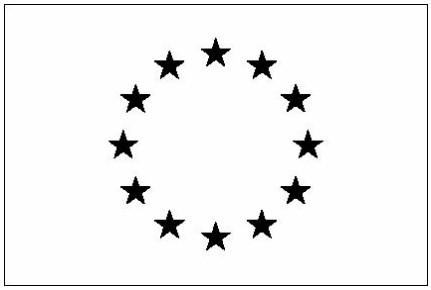

FP7 – SEC- 2011-284725

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 5.5: Report of the Third Annual Forum for Decision-Makers – Joint Final Event 29-30 October 2014, Brussels

Due date of deliverable: 30.11.2014

Actual submission date: 29.11.2014

Start date of project: 01.02.2012 Duration: 41 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 5.5: Report of Third Annual Forum for Decision-Makers
(FP7-SEC-2011-1; Grant Agreement No. 284725)
DEMOSEC : Democracy and Security
IRISS-RESPECT-SURVEILLE Joint Final Event 2014

Diamant Centre (DIAMANT Conference & Business Centre - Diamant Building - 80 Bd. A. Reyers LN, Brussels), Brussels, 29-30 October 2014

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

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

REPORT

Wednesday, 29 October 2014

Part 1. WELCOME AND INTRODUCTION

09:00 – 09:15 | **Welcome and Introduction by the European Commission (EC)**
Speaker: **Graham Willmott**– Head of Unit, Policy and Research in Security, EC

Mr. Willmott notes that the diverse nature of those attending the joint event meant that working together on the three projects will have proven challenging. In terms of the policy background, he highlights that the issues at stake are not just related to academic matters for research purposes addressed by the three projects but they will also influence the Commission's policies over the next five years.

Mr. Willmott further underlines that there is a new Commission as from next week and a new President of the Commission. The Commission has set very clear priorities in a number of areas and the work covered by these projects relates to some of these areas. He expresses the view that security research programmes contribute to competitiveness. Legal and ethical research has an impact on competitiveness and industrial policy. The work undertaken in the framework of the three projects relates to the Commission's policies on migration and security. The Commission that will start work in the new legislative period next week; it was further noted that security research henceforth shall be the domain of the DG also responsible for migration and home affairs will be responsible for security, migration and home affairs.
The European Union's Area of Freedom, Security and Justice is based on mutual trust. This is at the very core of what the three projects and the DEMOSEC (Democracy and Security) Joint Event itself are exploring.

Security research has also been done as part of previous programmes. Mr. Willmott mentioned that the funding for research projects has been increased in Horizon 2020 and that the aim is to continue working in this area by building on what has been achieved so far.

Despite the fact that there were different sources of funding, Mr. Willmott claims that it has been possible to coordinate the work of the three projects.

This conference is the opportunity to present the results of the research done on several topical issues: (1) the threat that surveillance technologies pose to citizen's fundamental rights, including privacy, data protection or even standards for privacy by design (taking into account privacy and data protection from the moment when a piece of technology is produced); (2) the costs of surveillance for society (financial issues and fundamental rights); (3) the everyday effects of security and surveillance; (4) and, finally, the EU's reaction to surveillance. DEMOSEC brings together three projects to examine common issues from different perspectives.

Society is increasingly concerned about surveillance. This was one of the focuses of the three projects. But society is also concerned about industrial policies and competitiveness.
One of the areas in which the European Commission (EC) has worked over the last few years is the protection of privacy and citizens' information. The EC is developing standards via different research projects and together with EU Member States.
There is also a link between industrial policy and privacy. Citizens must have a technology – a product - that they can trust and something that can improve their lives. In addition, technologies should help create jobs that have been lost in the last few years.
The privacy and personal preferences of customers must be taken into account when designing a product. The most sophisticated product can be produced but, if citizens perceive them as a threat, such products will never be successful.

09:15 – 09:45 | **Brief presentation of the projects by the project coordinators**
Speakers: Reinhard Kreissl – Institute for the Sociology of Law and Criminology (IRISS), Joe Cannataci – University of Groningen (RESPECT), Martin Scheinin – European University Institute (SURVEILLE)

Prof. Reinhard Kreissl
Cooperation between projects leads to exchanges of ideas about democracy and security. The three projects are at the last stage in their research. This conference aims to bring everything together.

The IRISS project is a response to the challenge that surveillance poses to democracy. While other projects provide operational ideas or projects that go to the market, the IRISS project has more freedom. So the project has the chance to look at the private sector too: Google, Twitter and Facebook are the big threats to citizens' privacy.
This project aims at investigating citizens' perceptions of surveillance. It investigates people's experience of surveillance and security and how they feel about it. Yet, when people are asked what their main concern about the development of surveillance technologies is, they answer that it is the cost of them and therefore the financial stability of the country. When we take the citizens' perspective into account, we end up with much more complex elements. When we ask someone about his security, we create a certain framework. Questions include: What kind of technology should be used?
When people think about security, this is a moment when they do not feel secure. The question is: What kind of technology should be designed and used to avoid this problem? What does it mean to be a human being that is closely connected to computer systems and other systems collecting data? These are the kind of questions that IRISS asked citizens.

Prof. Martin Scheinin
The SURVEILLE project deals with surveillance, ethical issues, legal limitations and efficiency. It looks into future prospects in terms of the development of surveillance technologies and legal rules. This demonstrates the multidisciplinary nature of the consortium.
The ethical issues and legal limitations of surveillance primarily refer to fundamental rights (cf. European Convention of Human Rights, EU Charter of fundamental rights and the broader framework of human rights).

Efficiency is the second layer of this multidisciplinary project. It generally depends on several considerations such as engineering sciences, technology assessment and social sciences through perceptions and also economics through the issue of the financial costs of surveillance.

The purpose of this project is to use this multidisciplinary background to explain and give more details on the use of surveillance technologies in order to assess them in an overall context. In particular, there are unacceptable levels of moral risk, there are unacceptable invasions of people's fundamental rights and there are unacceptable costs of surveillance technologies. If we can limit the discussion to these three parameters, we have a rational discourse. Answering these three parameters means answering to the following question: What is a proper method of carrying out surveillance and in a way that respects people's fundamental rights and how can we minimise the risks?

The Edward Snowden case has revealed the depth and intensity of electronic mass surveillance. Since his revelations more emphasis has been given to the idea of using mass surveillance proportionately and not indiscriminately. We are trying to match different contexts to the use of different technologies (*e.g.* scenarios developed through the SURVEILLE project). This electronic mass surveillance represents the complexity of the issues we face, such as the exponential growth in the costs of surveillance, the depth of intrusions (including collateral intrusions into the privacy of third parties) and the difficulties caused by the secrecy that is still associated with the regulation of surveillance. It highlights the dilemma between surveillance and democracy.
Very recently, in April 2014, the European Court of Justice (ECJ) underlined how important the legal discussion on the limits of surveillance is (in terms of EU law and fundamental rights).

The surveillance discourse is a continuation of the broader one following the 9/11 terrorist attacks and on the risks posed to society. We have witnessed a clear overreaction by States when they are countering terrorism. In recent times in the context of ISIS terrorist acts, there have been very similar reactions than immediately after 9/11. Again, there have been decisions taken in haste to show the population that the government was doing 'something' (*e.g.* in the EU, Australia, Canada and many other countries). In a sense, the pendulum is again swinging back to the post-9/11 atmosphere of panic.

Another transformation can be observed in the financing of security research by the Commission: in the early days, security research projects funded by the EC primarily served product development and focussed on improving the competitiveness of European technologies and helping to develop markets for these technologies abroad. This is a legitimate objective, but the Commission drew a lot of criticism because these projects were not always associated with ethical and privacy issues. Some years ago, new projects, which

focus on ethical and fundamental rights issues, started to be introduced and a more balanced overall research programme emerged.

However, the first calls within the Horizon 2020 Programme, suggest that also here the pendulum may be swinging back. The idea to integrate ethics and law, including privacy by design, into projects dealing with the development of technology projects is as such commendable but there should also be room for critical ethics and fundamental rights research.

Prof. Joe Cannataci
Prof. Cannataci gives a brief overview of the RESPECT project in which he specifies that it is very policy-oriented.
At the end of the project, RESPECT is expecting to present a policy brief both to the European Commission and to the European Parliament.
In terms of outcomes, there will be a RESPECT policy brief later and first a joint policy brief with IRISS and SURVEILLE. In addition, there will be a tool kit for policymakers and a tool kit for law enforcement agencies and possibly security servants and intelligence services with operational guidelines. The project provides evidence-based tools for policymakers. RESPECT has carried out a survey of all the legislation covering surveillance across EU Member States to analyse what the law says. The project has carried out investigation into surveillance in key areas: CCTV, social network analysis, tracking of financial transactions, data storing, etc. Those are the areas where technologies have been deployed. It has also been looking at the sociology of surveillance and specifically the social cost of surveillance, the economic cost of surveillance and the citizens' perception of surveillance.

RESPECT's research project is the result of analysis carried out by more than 58 people and 21 partners (academics and practitioners).

There is a data protection reform package, which has been subject to discussion in Europe since 25 January 2012. But it is still not clear how this is going to end. There seem to be disagreements within the Council of the European Union but the European Parliament has pushed it through. One of the things the project had to do was to come up with a model law on smart surveillance. That led us to wonder whether there should be a wider approach to surveillance. RESPECT has not yet decided what to do about the approach that should be taken and therefore about the outcomes that will result.

PART 2. KEYNOTE

09:45 – 10:45 | **Keynote on Surveillance and Democracy**
Keynote speaker: Helen Nissenbaum – New York University
Panel members: Charles Raab – University of Edinburgh (IRISS), Nikolaus Forgo – Leibniz University of Hannover (RESPECT), John Mueller – Ohio State University (SURVEILLE)
Chairperson*:* Nikolaus Forgo – Leibniz University of Hannover (RESPECT)

According to the theory of contextual integrity, threats to privacy, which are often triggered by the deployment of computing and information systems, are due to inappropriate flows of personal information and not merely to exposure of personal information or losses of control over it. Appropriateness of flow is characterised by conformity with context-specific informational norms, which carry moral weight when they protect the well being of the

individual, data subjects and promote moral and political values. Beyond both of these points, ideal informational norms promote contextual ends and values and thereby the integrity of social life. Surveillance practices, which are not necessarily problematic, must be evaluated in these terms, namely in terms of their impact on relevant actors as well as ethical and contextual ends and values.

Dr. Nikolaus Forgo introduces the speakers.

Prof. Helen Nissenbaum
Title: "Contextual integrity as a measure of surveillance practice"
Generally, scholars attempt to offer a philosophical version of privacy and to explain its ethical legitimacy. At the same time, privacy has a heuristic dimension as a guide to policy and technology design.
Types of technologies involved in surveillance:

- GPS, mobile, implantable devices
- RFID, emanations
- Biometrics
- Pervasive sensor networks
- Image, video and audio capture.

There are technologies embedded in social structures and it is through these social structures that surveillance takes place. Surveillance can take place in the name of social security, law enforcement, open safety or open efficiency (*e.g.* surveillance performed by credit card companies to identify fraudulent uses of credit cards).

Surveillance has often been performed for our benefit (*e.g.* to identify the fraudulent use of credit cards even if it means monitoring every transaction we perform).

Prof. Nissenbaum expresses the view that the right to privacy is the right to an appropriate flow of information rather than the right to control information about us or the right to secrecy. If privacy is defined in this manner, it becomes a right that is impossible to defend and this is not what people care about. Therefore, she wonders what would be an appropriate flow of information (disclosure of information). People disclose private information on social networks but that is not considered as posing a threat to privacy.

Three key concepts are identified:

- Contexts: Structured social spheres defined by activities, practices and roles (healthcare, education, social and home life, professional and work life, the commercial marketplace).
- Informational norms: Rules, customs, conventions, expectations and laws defining appropriate flows of personal information. Our behaviour is influenced by expectations and contexts. These norms actually give us the measure of personal information we will share.
- Purposes and values: General ethical and political context, specific ends, purposes and values.

There are some norms governing information flow. The key parameters are:

  - A**ctors**: Who is sending the information? Who receives the information and who is the person related to the information (sender, recipient, subject)?

- **Type of information**: Demographic, biographical, transactional communications, financial information, etc.
- **Transmission principle**: Terms under which information flows from party to party. Offering people notice, consent of people: really important transitions principle but not the only one. Should you provide notice to people or not? It depends (*e.g.* you expect your doctor to share information only if it helps your health and you want to be aware of it). Consent, coercion (if the government asks you for something for example), stealing, buying, selling, in confidence, without notice, etc., are indefinite numbers of transmission principles.

Agencies, services or other private or public institutions must inform to whom they send the information. In a survey, it must be specified to whom the information will be disclosed when we ask the question. The US Fifth Amendment states that one cannot force the suspect to reveal incriminating information. It is thus an issue of *the way* of extracting information.
The control is one among many transmission principles. Information disclosure is not in itself relevant to privacy. No one has the right to be forgotten. The question is not about the right to be forgotten but under which conditions information will flow after a certain period of time.
Respecting privacy means respecting an entrenched context.

Reforms have to be undertaken with a principled approach. In this respect, the question that can thus be raised is: How should the States and the EU reform the use of surveillance technologies? An assessment of what is possible and should be improved is necessary.

Some groups in society pay the cost while others enjoy the benefits. Prof. Nissenbaum argues that we should think about the context of specific purposes and values. Privacy is a value for the individual but it is crucial for the integrity of social life. Privacy is protected by an appropriate flow of information.
For instance, tax systems would benefit from an appropriate flow of information as people are more honest in declaring their income if they know that their information is protected.

Techno-surveillance must be evaluated in democratic societies. We could ask about purposes and ends. It is important to ensure people act appropriately but the notices provided depend on the situation. Restrictions with regard to disclosing information in a liberal democratic society should be in balance with the need for transparency. We need to take the full picture into account.

Prof. Charles Raab
According to Prof. Raab it is extremely difficult to relate policy studies and democracy to surveillance. That is what the projects have tried to do: establish such a link. How can a balance be struck between privacy and security?

Prof. Raab considers that the political system cannot stand the concept of richness and the recent evolutions of surveillance. He is pessimistic about the projects' capacity to change the political system.
The surveys sought to evaluate the public's opinion on specific issues asking: do you prefer privacy or security? The IRISS project exports democracy. This project looks at democracy in terms of political democracy and democratic society. Privacy is not just an individual value. It is also a social value. What about society's resilience? Democratic political society is vulnerable to surveillance because of its open nature, which requires a variety of conditions to be put into place.

Prof. Raab concludes that the consent of the government is also a principle of a democratic political system.

Prof. John Mueller
With regard to efficiency/efficacy, if it can be demonstrated that surveillance technologies/techniques cannot do any good, nobody should worry about privacy. This is not just a legal or constitutional issue, it depends on whether it works or not. If it works well, it must be legal and constitutional. If it does not work, it is the opposite.
How much would you pay not to be monitored by the NSA?

The other point has to do with secrecy itself. It becomes more and more questionable why some information is secret. Transparency in democracy relies on people knowing what is going on. Classifying/keeping information secret can have a very perverse effect.
Why were the programmes that Snowden has exposed secret? One answer could be that the government did not want the terrorists to know it was spying on them. Governments keep information secret for a reason and the reason is national security. However, it can happen that information is classified without any scrutiny as to whether it should effectively be classified or not.
According to Prof. Mueller, it is not possible to have a democratic debate over the programme because huge aspects of it are secret. In fact, the NSA used to be almost a secret in itself.

Q&A discussion
Questions:
1) European Commission official to Prof. **Helen Nissenbaum:** This person considers that policymakers can understand and take into account what Ms. Nissenbaum has just presented.
How much of what you said can we perform in the end? We are living with all kinds of threats for privacy and for data control. Can we enjoy these rights through practice and jurisprudence or do we have to enshrine the rights in the legislation?
The EC official says that Prof. Nissenbaum did not mention the notion of intimacy. Prof. Nissenbaum, do you link privacy to the notion of intimacy that is either a transparent or secret concept?
Finally, you often speak of integrity. Maybe, the notion of vulnerability should be included along with integrity.

Answers:
Prof. Helen Nissenbaum*:* It is not so complex. If, as a teacher, you do not keep track of the performances of your students, you are a bad teacher because your role is to maintain surveillance on your students. It is the same thing for parents with their children. In some contexts, it is necessary to record information.
Doing this analysis, we already do the context analysis.
We do have things that we call fundamental human rights and they should be taken extremely seriously.
This is about information and data flow. This is not a theory of privacy. It is a theory of flows. To minimise intrusions into this privacy, you need a contextual framework.

Prof. Charles Raab: Prof. Raab said that he is not downplaying he value of that analysis. However, with some imagination and strategy, we can try and make the political system and the policy-making system a bit more sensitive to this kind of consideration.

Intimacy is not concerned with the isolated individual. It already implies a relationship with others. There is a very good theory of privacy that relates to making social relations and engaging with society. Politicians often do not understand that because they consider privacy to be a retreat from society.
The iconic image that we have of security is a castle and yet the iconic frame around the protection of privacy is to protect the castle.

Questions:
2) **Prof. Roger Clarke**: Data protection is an important point in the dimensions of privacy. Do you not think that it is asking too much to this right while there are other way to balance the practice of actors (*e.g.* mitigation measures, controls, etc.)?

3) **Dr. Nils Zurawski**: The problem of balancing privacy and security is that privacy is individualistic. It could be a common good such as security. Then, it could be that it is not limited in favour of security. There is always a balance and there is always a loser.

4) Member of the audience: The term "surveillance" gives the impression of control. Perhaps, we might consider prevention.
Are we together? What is democracy? Is democracy healthy? Democracy will necessarily lead to divisions and conflicts and certainly not peace.

5) Member of the RESPECT project: My personal data belongs to me.

Answers:
Prof. Helen Nissenbaum: In Prof. Nissenbaum's view, people do not protest because their information has been disclosed but it has been done inappropriately. In terms of balancing - the individualism of privacy - individuals benefit from the right to privacy. Privacy is not only a personal right but it is something that should be protected for the society as a whole.

There have been public initiatives to defend the fact that you have property rights over public information but - in Prof. Nissenbaum's opinion - that is going completely in the wrong direction.

In a bank transaction, information about me is also information about my bank account, so we would rather drop that notion of "my" information and just go directly to how we should regulate the flow of financial information about me (pragmatic point of view).

Prof. Charles Raab: All forms of privacy ultimately amount to information privacy. People stick to privacy whether or not a flow of information is involved. Information about someone is information about others as well. Genetic data is a very serious issue to let us know about our family and genes. We should question the idea of what we mean by personal data. Are personal data exclusively personal?

Prof. John Mueller: It is a mistake to confuse democracy with outcomes. There are States convicting homosexuals and there are States that do not. There are nationalised air companies and non-nationalised ones etc.

PART 3. PANELS ON TECHNOLOGICAL ASPECTS OF SURVEILLANCE
Organised by RESPECT with contributions from IRISS and SURVEILLE.

11:15 – 12:00 | **Panel: Surveillance technologies in society**
Principal speaker: Tony Porter – Surveillance Camera Commissioner, UK
Panel members: Michelle Cayford – Technical University Delft (SURVEILLE), William Webster – University of Stirling (IRISS)
Chairperson: Caroline Goemans-Dorny – Interpol (RESPECT)

Balancing society needs via surveillance technologies.

Ms. Caroline Goemans-Dorny introduces the speakers.

Mr. Tony Porter
What does surveillance in the United Kingdom (UK) look like? Surveillance is everywhere in the UK. The question then arises: is it effective enough or does it need more power? Surveillance, especially CCTV, is partially public and partially privately owned. That creates a regulatory issue.
Capacity and capability are completely different concepts then what they were 25 years ago. In general, 84% of surveys show that citizens support the use of surveillance. But do they represent a conscious consent? Citizens do not have any idea how this surveillance is performed.
Technology is moving forward but it must be used with caution and intelligence. In this respect, several questions may be raised: How do we defend ourselves against hackers? How is this technology going to move forward?
The Automatic Number Plate Recognition (ANPR) captures around 14 million images every day. In terms of facial recognition, how can this technology "migrate" to everyday uses? Nobody is regulating these technologies. Drones are used to gain a more efficient system without adequate regulation. In fact, the changes in technologies are leading to a huge shift in the method used to operate in society. Therefore, developing standards that will fulfil standards of integrity will be necessary.
Mr. Porter concludes that a fine balance should be found to ensure a suitable regulation.

Prof. William Webster
Society and surveillance are evolving at the same time. However, security needs are the priority of policy-makers. The social side of surveillance is indeed often underplayed.

- Surveillance technologies have proliferated
- There are a wide range of different surveillance technologies and practices

Prof. Webster makes a number of assumptions such as "surveillance by definition is anti-privacy". Security and privacy need to be balanced in a very narrow way.

There is a broader social perspective (surveillance and humanity).

- Surveillance is unsurprising and ubiquitous. Surveillance via new technologies is all around us.
- Surveillance is normal and natural.
- Surveillance is rooted in social behaviour and control, making sure that others are fine with its implementation and influencing their behaviour.

- Surveillance manifests itself in a range of technologies and practices. The evolution of mass surveillance is having a strong influence on the shape of society. It is permeating our relationships. This could include a change in democratic practices.
- Surveillance is about 'power' controlling and shaping the behaviour of others.
- Surveillance is a fundamental facet of human existence. It is something that is bound to exist in society.

Although surveillance has always been present in society, it would be at present interesting to analyse the current interaction between the development of surveillance and society, including individuals and groups.
Prof. Webster considers that surveillance-related intensive security practices should be developed alongside a full understanding of their potential consequences. The debate is not about whether there should be more or less surveillance. There should be about appropriate safeguards.
The nature of surveillance means that technologically mediated surveillance must be governed in the broader interests of society. One should encourage the development of technologies that place a value on other human needs.
A lot of the empirical work looks at surveillance in different sectors and how it is experienced by end-users and citizens. It could be seen as a threat to other values in our society.

Ms. Michelle Cayford
Title: "Surveillance technologies in society"
In the framework of the SURVEILLE project, research has been carried out with reference to NSA surveillance technologies. Based on public sources SURVEILLE has tried to classify surveillance in two categories: mass and targeted surveillance. For example, wiretaps are part of mass surveillance.

How does it work? A 50/50 fibre optic splitter makes a copy of data and then sends it to the NSA. As more filters are set, the system starts to run more slowly. In this case, the system cannot analyse data that is gathered.
Whatever data is captured by the deep packet inspection technology (DPI), it can be held from three to thirty days. Then, all the information is sent to the NSA central database. The US government does not consider the data collected via this process as being mass surveillance because the major part is temporarily holding and facilitating the capture of data for specific cases. Only the data that are sent to the NSA, which are related to specific cases, are kept for five years. This is a lot in comparison with thirty days.
Government's mission is to stop a terrorist attack. Therefore, there is a need to balance society's needs with the use of surveillance technologies.

Q&A discussion
Question:
1) **Prof. Joe Cannataci**: The quantification of costs to stop a terrorist attack is to stop it at almost any cost. Is the importance of privacy greater than an attack? What about the principle of proportionality?

Answers:
Ms. Michelle Cayford: All the money that is invested in developing technologies to prevent terrorist attacks is not worth it. The question that needs to be answered is: is the cost of one attack greater than the privacy of data?

Prof. William Webster: The statement "at any cost" means the strong desire to get something done. The idea of proportionality is something that people would expect to see in a policy process, which has to be as rational as possible. It shows that policymaking is not always rational or proportional. There are probably serious risks attached to every policy.

Mr. Tony Porter: The question is: what is the legitimate aim of surveillance?

Questions
2) Member of the audience: You are not born as a criminal, though you may become a criminal. This is an important issue to address.

3) Member of the audience: If the Boston bombing has been rationalised by surveillance, how can one rationalise bomb attacks that could have been anticipated but were not?

Answer:
Mr. Tony Porter: In the UK, thousands of cameras capture twenty to thirty million images per day. There is a commitment towards a regulatory framework allowing police officers to capture information in a more balance manner.

Questions:
4) Member of the audience: The reference to the US statement saying that, as long as data is only collected but not really analysed, they will not be considered so much of an issue, is problematic.
Does a human being receive it or is it just a technical collection? The traditional concept of collection faces some limitations. They have a different impact on fundamental rights. Maybe policy-makers should start re-thinking the traditional concept.

5) Member of the audience: The private security industry is always growing and it increasingly operates by means of highly sophisticated mass surveillance systems in public spaces.

Answer:
Mr. Tony Porter: There is a process of mutual recognition. The regulatory framework is developing mainly through the recognition of benefits and not through States regulation.

13:00 – 14:15 | **Panel: Use of technologies in society (Social Media and CCTV)**
Principal speaker: Daniel Trottier – University of Westminster (RESPECT), Caroline Goemans-Dorny – Interpol (RESPECT)
Panel members: Jonathan Andrew – European University Institute (SURVEILLE); Richard Jones – University of Edinburgh (IRISS)
Chairperson: Simon Dobrisek – University of Ljubljana (RESPECT)

Security and surveillance practices are informed by a range of technologies, many of which are currently being trialled and used by law enforcement, security and intelligence agencies on a global scale. These technologies, including closed-circuit television networks (CCTV) and social network monitoring and analysis systems (SNMAS), are being developed in both the private and public sectors. This panel will highlight key findings from the RESPECT project that consider the uptake and integration of these technologies, in particular relating

to cost versus convenience, proportionality issues and privacy and data protection impact assessment.

Dr. Simon Dobrisek introduces the speakers.

Dr. Daniel Trottier
Dr. Trottier sets out a list of available technologies.
Social networking platforms contain both private and public data and the police could access any information on that platform.

Dr. Trottier identifies costs and advantages.

- Expenditure: software, hardware, etc. These aspects are of major concern when scaling up a technique at a national level as this means raising the level of expenditure.
- Training: bringing someone's enthusiasm across from social media to the law was tackled as a challenge. Low technological skill sets matter.
- Other costs and resources: time, language skills, careers, etc.

Dr. Trottier specifies the degree of automated decisions involved in online social network analysis techniques:

- No full automation of the Social Network Monitoring and Analysis System (SNMAS). Very little automation of data processing at present.
- Overwhelming support for manual decision-making (*e.g.* manual searching beginning with manual calibration and ending up with manual interpretation).
- Some steps may be automated but bookended.

SNMAS is especially well suited for interoperability purposes. It is facilitated via a partnership with local authorities such as the police in Italy.

The key findings are based, first, on a lack of a clear EU wide strategy toward the effective use of SNMAS; and, second, on trained staff remaining a virtual resource.

There is yet little consensus about the appropriate use of SNMAS technologies while the range of SNMAS technologies available to police is increasing. Social costs and other impacts are only becoming evident as these technologies are put into practice. Policymakers must consider the social context in which SNMAS are deployed.

Ms. Caroline Goemans-Dorny
CCTV is often subject to scrutiny and not only from civil liberties' organisations:

- It has a potentially adverse impact on the fundamental rights of citizens
- There are direct or indirect consultations.

CCTV is often criticised. There is a reasonable expectation from citizens that CCTV should provide value. In parallel, there is a clear need for openness and accountability when we use this kind of technology. It needs to be illustrated to the public, with public consultation and participation.

- Evaluation as a form of transparency and accountability
- Crowdsourcing and participative policies as a new form of empowerment

Evaluations are difficult and often criticised from a methodological perspective.

Law enforcement requires more assistance and guidelines.

The key questions are: is CCTV the only measure that can be used to prevent crime? Crime rates may also vary due to external factors. How does a specific measure crime prevention?

Ms. Goemans-Dorny gives an example of good practice that has been implemented in Amsterdam. In 2012, a new policy framework was adopted: a new law on the video-monitoring act. Video monitoring is not centralised: local police agencies are not simultaneously watching CCTV. All these changes led to a new regulatory framework applicable to public space video monitoring.
In this context, there has been a focus on maintaining public order (the prerogative not of the police but of the mayor) and not on the fight against crime. It has increased police efficiency and effectiveness, preventing disturbance to public order and increased safety among citizens.

To deploy CCTV there are some conditions:

- It is a really heavy measure. Therefore, there is a need to prove that such implementation answers the criteria of proportionality and subsidiarity. There must be proof of a very serious threat or continuous criminal activities for CCTV to be used.
- Other less intrusive measures have to be tried and tested before implementing and using CCTV.

The citizen's role is emphasised. They are called on to report and contribute to prevent crimes and to cooperate with the institutions.
Simultaneously, CCTV systems are evaluated on a regular basis: a long or short (6 months) temporary basis.

The evaluation is based on three criteria:

1) The level of insecurity in a monitored area and its evolution. A continuous evaluation of the areas is carried out according to the types of violence and their evolution. This evaluation is based on three analytic aspects:

- Number of incidents;
- Evolution of the number of incidents;
- Evolution of types of incidents.

2) The use of CCTV must be to increase safety. Some incidents have been reported only by using CCTV. The contribution of CCTV to the safety of citizens has to be proved. The survey carried out by the project includes both positive and negative statements.

3) The contribution of CCTV to the perceptions of safety of citizens and visitors (through surveys).

The majority of CCTV systems are owned by the private sector. In this case, there is a need for data transfer from citizens to law enforcement authorities. The collection of pictures by citizens is becoming increasingly important for law enforcement agencies.
For instance, after the Boston marathon bombing, law enforcement agencies went on Twitter and asked for videos and photos to identify the suspects. Citizens voluntarily sent videos and images to the police. However, this can lead to mistaken identifications.
The most topical issue is the citizens' lack of trust in the State. This leads to a situation of community empowerment. This can be dangerous. For instance, some people have been persecuted after having appeared in blogs that accused them of having committed a crime.

Dr. Richard Jones
How/Why are new technologies adopted by police forces?
In general, the technology the most used is often the one that fitted best with the cultural understanding and the social habits of people in a given society. The search for the most suitable technology used by police forces suggests that many of the practices, which are traditionally police practices, do not help to reduce crime. It also shows that hotspot policing can be quite effective.

In Dr. Jones' opinion, public and private sector should try to identify the appropriate technology in advance rather than introducing the technology and then going and looking for some evidence of their efficacy. In parallel, evidence shows that the nature of police-public interaction may be one of the causes of the falling police legitimacy in the eyes of the public.
The benefit that society could gain from the use of these technologies can only be reached by addressing the use of technology in specific circumstances. There might be some short-term temptation to adopt new technologies without a clear regulatory base. If they are not regulated and not used carefully, technologies can lead to some long-term negative consequences.

Mr. Jonathan Andrew
Often surveillance technologies are used without their impact being understood.
One point that the SURVEILLE project has been interested in is the discussion about open source intelligence. The role of automation is very important. Other questions include: what does automation mean and what has automation been used for in the implementation of social network analysis?
There needs to be reflection on how information reflects the decision-making process. People are not aware of the use of information by law enforcement authorities. From a legal perspective, it is necessary to clarify whether or not the use of surveillance represents a legitimate way of conducting prevention and investigation activities. It is a key issue for mass surveillance.
The SURVEILLE project has brought together the knowledge of law enforcement agencies to create realistic scenarios in order to establish what kind of problems exists. The objective was to analyse whether or not the surveillance used is proportional.
CCTV has been criticised on methodological grounds. One of the points raised regarding the effectiveness of CCTV is that, when citizens are questioned, it is important to question whether or not other forms of surveillance were considered (such as better lights in public areas). Very often, if you ask citizens, they will not foresee an alternative.
Very few surveillance systems are removed. Once they are installed, they will stay there, except for some cases in which they end up falling into disrepair.

Q&A discussion
Question:
1) Member of the audience: It is important to measure the safety of an area and ask people about their perception of security. There is a sort of social incapacity to understand risks. Is the goal to make people feel more secure or to reduce the crime rate in statistical terms? Depending on the strategy, the response will be different.
It would be a good idea to help the public to better understand the solutions proposed.

Answer:
Ms. Caroline Goemans-Dorny: There is a plethora of analysis on possible methods to

remove a problem before using CCTV, which is a heavy way of removing a problem. It was stressed, including by the police, that CCTV is just one element of a whole strategy regarding safety. It is just a tool, an additional eye. The participation of individuals is stressed too; it is even a new trend.
High priority is being given to objective and measurable results. But, the perception of the citizens is the first proportionality test. All the incidences given to the police are measured.

Question:
2) Member of the audience: No cameras installed have ever been removed. Do you think that it is because when it comes to balance, we always overestimate threats over limits?
Do you think cameras will be removed in the future and is there any evidence that this process has reduced the implementation of new cameras?

Answer:
Ms. Caroline Goemans-Dorny: There were arguments in favour of and against the implementation of CCTV. It is a fact that some cameras have been removed (e.g. five out of the nineteen cameras were taken down in Amsterdam after an assessment).

Question:
3) Member of the audience: In Slovakia, cameras have never identified who committed a crime. The law provides for cameras in every stadium but nobody is identified.

Answers:
Dr. Simon Dobrisek: The effects of the use of CCTV on crime prevention cannot be easily assessed.

Ms. Caroline Goemans-Dorny: Cameras have to be removed if they do not meet the purposes of their implementation. In cities, smart cameras will be used for basically everything.

Question:
4) Member of the audience - Journalist from Amsterdam: Do you have an explanation in your research for the huge differences between the different parts of the city of Amsterdam?

Answer:
Ms. Caroline Goemans-Dorny: There were nineteen projects because a particular problem was detected. However, even after their implementation, other tools were used to ensure public order. CCTV cameras were set up because nineteen areas had been identified as unsafe, regardless of other measures that had already been taken.

Questions:
5) Member of the audience: Is the data stored? How long is it stored for? Is there a network or is it just locally gathered? The public reaction could be very different depending on these factors.

6) Member of the audience: What about suicide bombs? Do you also explore how to improve the safety of the elderly and those who live alone?

Answers:
Dr. Daniel Trottier: It is a two-step process: the technological part on the one side and the

social and ethical part on the other side. The social and ethical part of the project needs some changes.

Ms. Caroline Goemans-Dorny: A lot of technologies have been invented and implemented. However, with regard to CCTV, only the private sector can afford to buy this product. There is no structure or procedure when public authorities, including law enforcement agencies, acquire the product. It should be at least a data protection officer.

There should be a sort of collaboration between law enforcement agencies and the private sector so that law enforcement agencies can be advised on what kind of technology should be bought.

Dr. Richard Jones: Some research suggests that implementing **s**treetlights would reduce crime more effectively than installing CCTV. Some other research in London on image analysis is looking to predict individual behaviour. It seeks to understand how effective these systems will be. However, the results focus more on probabilities than certainties. If the system is taken as the only criterion - and thus without taking into account the particular culture and the particular type of society - it is unlikely to be effective.

Mr. Jonathan Andrew: Both data retention and data gathering issues are important. For both of them, the capacity and the limitations of technologies must be understood to help law enforcement agencies to use these techniques.

PART 4. PANELS ON THE LEGAL ASPECTS OF SURVEILLANCE

Organised by SURVEILLE with contributions from RESPECT and IRISS.

14:15 – 15:15 | **Panel: Reconciling human rights protection and security: the role of European norms and discretion of competent national authorities in using surveillance technologies**

Principal speaker: Hielke Hijmans – Vrije Universiteit Brussel;
Panel members: Ivan Szekely – EKINT Budapest (IRISS), Jeanne Mifsud Bonnici – University of Groningen (RESPECT), Christiane Höhn – Adviser to the EU Counter Terrorism Coordinator;
Chairperson: Francesca Galli – University of Maastricht / IEE-ULB (SURVEILLE)

In the European Union, human rights are protected at both the national and European level. While the use of surveillance technologies for security purposes engages both, European norms and national legal frameworks may conflict. Such contrasts remain topical and are of interest in the development of surveillance technologies. Indeed, European institutions have an increasing focus on the potential harmonisation of the use of surveillance technologies. Thus it is important to achieve clarity as to the application of protective mechanisms vis-à-vis fundamental rights. In this context, we consider whether Member States retain a margin of appreciation. Furthermore, to what extent should the European Union further legislate on this matter?

Dr. Francesca Galli introduces the speakers.

Mr. Hielke Hijmans
Title: "Reconciling human rights and security"

Mr. Hijmans makes some preliminary remarks:

- Surveillance is nothing new in relation to developing technologies.
- In an information society, there will always be surveillance. We cannot imagine a society without surveillance.
- How to ensure that surveillance is in conformity with constitutional values? What are the legal limits to surveillance?
- Two sides of the same coin: fundamental rights with protection against intrusion to ensure the freedom of individuals and surveillance as an efficient means of law enforcement.

According to Mr. Hijmans, people need to trust governments in this area but, at the same time, governments should be trustworthy and should protect us. Surveillance can be analysed from different perspectives. One perspective is the enormous impact that surveillance can have on individual freedom and another relates to efficiency in terms of protecting individuals and providing services to individuals. The highest level of accountability possible is thus required.

Mr. Hijmans describes the impact on society:

- People adapt their behaviour. Society is seen as a space where everyone is being watched. It may change our behaviour. There is a division between "good" people who have nothing to hide and "bad" people.
- What is more intrusive: surveillance by governments or by private actors? When governments have information, it is always possible to rely on accountability mechanisms. This is not possible with the private sector.
- Companies assist government in surveillance: Is it acceptable? To what extent?
- With future technological developments, it will be possible to be more and more intrusive. Will that be compatible with fundamental rights? The idea of fundamental rights needs to be rethought to have the necessary tools to face modernity.

Then, Mr. Hijmans presents the different points to reconcile human rights and security:

- Security is the core task of any State. Citizens expect it.
- Governments should base their acts on finding a balance between the different interests.

Mr. Hijmans asks where legitimacy could be found in the use of surveillance by governments: in the fight against terrorism, for police or immigration purposes or also for health protection?

The role of the EU and Member States: the EU plays a role at the normative level. Member States are the main actors in law enforcement. Maybe we should look at them when we talk about surveillance. In fact, national security is outside the scope of EU law. However, Member States are bounded by national constitutions and by the European Convention on Human Rights (ECHR) and the case-law of the Court of Human Rights (ECtHR).
Given that, security has become a much more important issue in recent years, is EU legislation needed? What should it entail?

Dr. Ivan Szekely

Dr. Szekely mentions three issues:

1) Security is a trump card to legitimise surveillance. Surveillance has several purposes, including maintaining security. Even when security is not the real aim of surveillance,

it is used as it was (trump card). If people are asked, security and privacy may have nothing to do with each other.

2) How do you improve a balance in the legal domain? Law is able to handle such situations. The balancing in the US and the proportionality in the EU depends on two different methodologies. In Strasbourg, the principle of proportionality is used only in a limited number of cases. There are different successive sub-tests: legitimacy, suitability, proportionality, etc. If the case fails at the first level, the case cannot proceed. The courts should strengthen the first three phases of the test and leave a lot of room for the moral aspect.
3) New technologies and future: Possible classification between networks, interfaces and artificial intelligence-based technologies. In some cases, it is enough to use the existing legal framework but in an extended way. In other cases, the present definition will not be enough.

According to Dr. Szekely, self-regulation, policy tools and multilevel governance can have an important role. The aim does not justify the means. Security does not justify surveillance. The reverse is also true. The means do not justify the aims. Surveillance does not justify security.

Prof. Jeanne Mifsud Bonnici
Prof. Bonnici's presentation addresses a number of issues.

Firstly, Prof. Bonnici wonders if the current legal framework protects citizen's rights and support the operational needs of law enforcement for the detection, investigation and prosecution of crime and terrorism?
Prof. Bonnici says that a legal framework at the EU or national level must be implemented. There are a framework and a Charter. The law across Europe includes different mechanisms of protection and different operational practices for different surveillance practices. Is this collection of laws across Europe, which could be described as a patchwork, enough?
There are areas where no law exists. In particular, public authorities are using smart surveillance or smart technologies in surveillance. Those practices are very much unregulated.

Secondly, there is a lack of definition of the responsibilities of private actors in carrying out surveillance. It is easier to apply rules to governments and public agencies than to the private sector.

Thirdly, Prof. Bonnici asks: Do we need more surveillance? What steps should we take before introducing more? The fact that we have this technology does not mean that we have to use it. She specifies that it is perhaps naïve to say so. What is missing is a proper legal basis for the EU. This issue needs to be addressed quickly.

Finally, Prof. Bonnici concludes with a particular question: Do we need 28 different levels of effort in trying to answer the questions/filling in the gaps above? According to Prof. Bonnici, a better collaboration between States is clearly necessary. There is, of course, a margin of appreciation because the States have different cultural and social situations.

Dr. Christiane Höhn
Dr. Höhn deals with the question of surveillance and the EU's (potential) role.
Dr. Höhn highlights that a balancing act between human rights and security/surveillance should not be needed because both surveillance and human rights are necessary.

The European Parliament (EP) has a stronger voice on human rights. In a democratic society, it is parliament that decides how far to go in the area of human rights.
Surveillance is the key to prevent terrorists' attacks. Therefore, surveillance is important in its preventative capacity, especially when the suspect is not identified yet.

Regarding data retention, it is not enough to retain a suspect's data. Sometimes it is necessary to go back and find brand new suspects. In particular, the European Court of Justice decision in April 2014 on the Data Retention Directive stated that the Directive did not regulate the safeguards. Therefore, law enforcement agencies and other competent authorities should work on this shortcoming.

As things stand, there are no harmonised EU rules on topics such as surveillance. Standardisation has been attempted for areas such as data retention but not on other areas related to the use of technology.
In terms of law enforcement, especially in the investigation phase, techniques have neither been analysed at the EU level yet nor have they been regulated.

There is a lacuna in terms of cooperation. How do other States work on particular aspects of the procedure? For example, how is the use of evidence regulated in another Member State?
In 2010, the Counter Terrorism Coordinator proposed to potentially harmonise the law, especially when dealing with investigation techniques and surveillance technologies used by law enforcement agencies.
Dr. Höhn considers that a Data Protection Directive is also necessary. Harmonisation of data protection regulations would lead to more sharing (the other countries would respect the same rules).
Dr. Höhn opens the debate in declaring that there is also the issue of drones as new surveillance technologies that should be addressed.

Q&A discussion
Question:
1) **Mr. Emmanuel Giakoumakis**: We believe that the harmonising of security interests is a core interest of the Council of Europe. This can also be reflected in the case of the European Court of Human Rights (ECtHR), where the Court has pointed out that there are lacunae in the policy-making proposal. National laws do not refer just to the norms of the EU. They also refer to the existing norms in the Council of Europe. Some are non-binding but still exist (recommendations).
When establishing a common policy, these existing tools need to be taken into account.
Do you believe that the standards set by the Council of Europe will be considered as useful tools for setting up policies and implementing legal bases?

Answer:
Prof. Jeanne Mifsud Bonnici: The members of the RESPECT project have looked to the Council at various points for inspiration. The Council of Europe is the best authority and the right forum to implement common legislation on this topic. At various points, the RESPECT project came to the conclusion that the Council of Europe is much more open than the EU.
The EU does not have a legal basis for surveillance by private agencies. So what does the Council of Europe do? The Council of Europe is much more open when referring to the opportunity to give a legal base to this issue. So it is and will be taken into account for sure.

Question:
2) Member of the audience: There are links between the Council of Europe and the EU. The LIBE Committee had a meeting with the Council on the modernisation of the EU regulatory framework in this respect. A Commissioner in charge of EU PNR mentioned that they would come up with a new project. Is that correct?

Answers:
Dr. Christiane Höhn: What I mentioned was how important it is for the EU to adopt an EU PNR Regulation. I do not know what the Commission has said and what the Commission has in mind but the point is that it is important for everyone that the Parliament and the Council work together on this issue.

Mr. Hielke Hijmans: The issue of EU PNR is related to a number of other discussions. It is an area, in the field of data protection, where there has always been criticism. If you strike a balance to create a 'win/win situation', policy-makers must find solutions that can be profitable for security and for privacy at the same time. It will be useful to harmonise rules to fight terrorism.

Dr. Ivan Szekely: Balancing security and human rights out is necessary. In a zero sum game, you must give up exactly the same amount as you do on the other side. In the context of using more surveillance, it is not the right approach because, in the end, there is a negative sum game.

Question:
3) Member of the audience: Generally speaking, there are probably confusions. One concerns the process and the other concerns the outcome. People have to give up some privacy to have more security. Nobody ever really ask how much security people have to give up to have more privacy.

Answer:
Mr. Hielke Hijmans: Security is a very difficult issue. Reflecting on what people are able to accept to protect privacy is not a good way to deal with the issue.

Question:
4) Member of the audience: The balance between surveillance and security is not a zero sum game it is a *coin game*. For intelligence services, police and politicians, this type of game is perfect because, every time, privacy will lose. They perpetuate the notion of a balance whilst knowing that it is a *coin game*.

Answer:
Prof. Jeanne Mifsud Bonnici: This is a bit too cynical an approach. There is a genuine attempt to achieve a balance even if the balance is not achieved in the end.

15:30 – 16:45 | **Panel: Data retention and fundamental rights: the CJEU Judgment of 8 April 2014**
Principal speaker: Paul Nemitz – Director Fundamental & Union Citizenship, EC
Panel members: Paul de Hert – Vrije Universiteit Brussel (IRISS), Erich Schweighofer – University of Vienna (RESPECT), Walter Coenraets – Director Federal Cybercrime Unit, Belgian Federal Police, Tuomas Ojanen – University of Helsinki (SURVEILLE)

Chairperson: Martin Scheinin – European University Institute (SURVEILLE)

The Data Retention Directive aimed at harmonising Member States' provisions concerning the retention of certain data generated or processed by providers of publicly available electronic communications services or of public communications networks. In April, the Court, which declared the Directive to be invalid, took the view that, by requiring the retention of data and by allowing the competent national authorities to access it, the Directive breaches the fundamental rights to the respect for private life and to the protection of personal data. In this panel we consider the implications of the decision taking into consideration that Member States adopted legislation to ensure compliance with the Directive. Discussion shall further debate how issues raised by the ruling will be resolved by European institutions and Member States.

Prof. Martin Scheinin (SURVEILLE) introduces the speakers.

Mr. Paul Nemitz
In Mr. Nemitz's opinion, there are limits in law regarding what exists or should exist with reference to mass surveillance. It is an issue that can be addressed under EU law. It is true that the treaties say that national security comes under the competence of Member States, but at the same time, the ECJ has stressed the importance for a State to show (in a way a judge can appreciate it) that its decisions are necessary and proportional to national security purposes. If ever it were confronted with a situation in which a Member State is conducting mass surveillance, the ECJ would probably say that it does not meet EU standards.
From the judgment on the Data Retention Directive, Mr. Nemitz highlights four questions:

1. Generally, a new and more rigorous standard of scrutiny is necessary.
2. More specifically with regard to data retention, is it necessary to ask whether there will be changes in national legislation after such a judgment? Does this affect the validity of national complementing measures?
3. Can private parties invoke the ECJ's decision before national courts or ask for the continuation of the application of the national implementing law, on which basis and with which effects referring to data retention?
4. The EC will examine the possibilities for a way forward. What are the options? What are the needs to make sure, from an institutional point of view, that the ECJ will give further effect to this Directive? What guarantee do people have that this decision has an effect on our legal system?

The Court examined the potential breaches of fundamental rights. The essence of the right was in the Court's view untouched because the retention was limited to meta-data. It is in the proportionality test that the court goes into details and gives some guidelines to regulate fundamental rights restrictions. The Court also mentioned other possible interferences with fundamental rights (freedom of expression – art. 11 of the Charter). When interfering with fundamental rights, the discretion of the EU's legislator is reduced.

Prof. Tuomas Ojanen
Prof. Ojanen's presentation addresses the intensity of the review. The Court judgment demonstrates the willingness and the ability of the ECJ to embark on a very rigorous judicial review. It is also a very neat example of the application of the permissible limitation test.

Prof. Ojanen specifies the methodological steps through which the Court of Justice normally proceeds:

1) What fundamental rights are applicable? The applicable rights have to do with privacy and the right of protection of personal data. The judgment distinguishes only between privacy and protection of personal data up to a limited degree only. The Court seems to start with the premise that personal data is just one dimension of privacy.
2) Is there an intrusion into the right to privacy? In case of positive answer, what is the degree of that intrusion? Special emphasis in the degree of privacy intrusion is given in the judgment. The ECJ emphasises that the right of privacy is protecting our personal data.
3) Was such interference justified? The Court stresses the fact that even national security measures must not go beyond what is strictly necessary.

Prof. Erich Schweighofer

There is intense judicial activity by national and European courts in terms of information gathering/knowledge management of police/security services. The ECtHR is very active. The questions are: who is doing the best? Who is applying the most rigorous standards?

It is not very clear who is doing the balancing - who is doing the proportionality test - because there are other people and other legal frameworks. Sometimes, they have to find solutions that the Court has left behind.

What can they do to apply the proportionality test? The activists, particularly in Austria, say that is impossible; that they cannot do it. On the other side, ministers and lawyers in Austria are waiting for a meta-political context. In the UK, the government said no and that the proportionality test is necessary.

The judgement of the Court in Austria demonstrates that decisions were different because the timing was different. This is particularly relevant. And, now, the national parliaments have to develop solutions following the rulings of the ECJ.

Prof. Paul de Hert

One of the first objectives of the IRISS project was to find a common language for lawyers and others. In particular, effectiveness is one thing while efficiency is another. Data retention is effective because it reaches its goals but the question is whether it is efficient or not. Questioning the efficiency of a tool is to ask what the cost of reaching the goals is?

Social scientists are not convinced by the legitimacy of this measure. Does data retention work? Could it be done differently? A lot of studies have been done on the efficiency of data retention. This judgment simply does not address this issue.

There was so much empirical evidence that is not efficient. The judges have understood the message about data retention not being so efficient but they simply do not refer to that kind of questioning and reasoning. They remain in the framework of traditional guidelines. Is there a legal basis? Check. Does it serve legitimate purposes? Check. Is it proportional? Check.

The evidence-based reasoning should be the method used in the future when dealing with surveillance but it has simply not found its way into this judgment yet.

Prof. De Hert would have preferred another approach. However, he considers that the outcome is good. Fortunately, lawyers do not deal with efficiency. According to Prof. De Hert, the lawyers know it did not work but they do not address this issue.

The problem of trying out testing technologies is the lack of evidence about whether it is efficient until they are launched. And, the results generally arrive five years later. Competent national authorities can only promise civil society that they will be listened to and that the government will come back to the initial project five years later. It is important to think more creatively, making surveys accountable in terms of numbers, in terms of efficiency and to

have an enlightened debate.
Prof. De Hert concludes in saying that we should go beyond traditional checklists.

Mr. Walter Coenraets
Mr. Coenraets presents the reality check: Law enforcement has to be efficient, particularly at this time of financial crisis.
Together with the Computer Crime Unit, law enforcement agencies attempt to combat cybercrime but they have also to deal with complaints concerning minor felonies. These minor felonies are not examined by the ECJ.
In almost every case, they realised that success can only be obtained through the process of identification based on data retained. The discussions following the decision are not about the police using - or not - data but rather on the conservation duration and amount of data authorised to be gathered by the police.
The main objective of police work is to catch the offender and protect the victim. Mr. Coenraets so asks whether these objectives can still be provided by law enforcement agents. Nobody will know in advance if the investigation concerns huge cyber attack or minor events on the internet.
As everything in future will be connected, more data has to be retained. In fact, to identify clearly the hacker, police officers must login.
Cybercriminals can act against many victims in different countries simultaneously from another country (transnational nature of the crime). There is more time to identify, lots of data is needed and there are more traces to identify the criminal. It is necessary to give law enforcement agencies the opportunity to secure and analyse electronic data. In his opinion, as it is impossible to know in advance what data will be needed, it is essential to law enforcement agencies to have access to a large amount of data for a long period. When law enforcement agencies ask to access data, the protection of data is ensure by the prosecutor or a judge who decide whether the data can be obtained or not and the amount of data.
Mr. Coenraets concludes by saying that, in the end, it is all about the context and purpose. Privacy is an essential issue but has to be placed in the appropriate context.

Q&A discussion
Questions:
1) Member of the audience: We have seen that there is a legal issue to be addressed. There is a problem of compatibility between national and European level. If you were the policymaker, would you try to solve the issue (data package) at a national level or somehow at the EU level? And how?

2) To **Mr. Paul Nemitz:**
- From your perspective, do you see room for a new legislative initiative from the EC for a data retention regulation at the European level?
- How can a Court decide, on the basis of evidence, in cases like the ones with which we are confronted today?

3) To **Mr. Walter Coenraets:** You said that you need data retained to investigate crimes. Is there also a limit in time for the availability of information to solve a crime?

Answers:
Mr. Paul Nemitz: The European Commission can take a political decision and propose a new regulation. It has full discretion. However, everything cannot be done at the same time. There is a complex legislative process currently going on.

Data retention has always existed but are we able to convince ourselves that this is an effective measure that will make a real difference? The Court should sometimes address the issue of efficiency. There are many cases in which evidence needs to be collected and in these cases the proportionality test applies.

Prof. Paul de Hert: Judges have and preserve their autonomy. They do not feel tied by a checklist.

Prof. Erich Schweighofer: From the Austrian court case, the ECJ has taken evidence to study the criteria.

Mr. Walter Coenraets: Just this year alone, there has been more than two thousand demands from local police to identify somebody by using data on cybercrime cases; cases on child pornography, disappearances of people, people that announced on Facebook that they will commit suicide the next day or rape someone. In these cases, the identification by data is essential.

The main problem for lawyers and NGOs is the limit in time. For example, in Belgium, the retention period is twelve months. It is enough to identify a victim or a suspect, for a minor case. For major cases, it is not enough and law enforcement agencies would like to have a period of two years because the attacks come from different countries. They need to complete a motivated notice about particular facts that need to be investigated, then they have to make an analysis of the facts, then they have to write reports about everything (this can take several months), then contact other countries for identification (this can take up to six months). Therefore, it is impossible to know in advance when data will be useful.

Prof. Tuomas Ojanen: Prof. Ojanen highlights the following issue: if Member States want to introduce a piece of legislation allowing mandatory data retention, one of the key questions is whether they are able to take into account the EU Charter of Fundamental Rights as it has been interpreted by the ECJ. A number of people seem to think that the Data Retention Directive is now invalid and that Member States are now free to act on their own, without being constrained by the EU Charter.
However, Prof. Ojanen would like to think that even if the Directive is now invalid, Member States are still exercising their competence within the scope of EU law. If Member States really want to introduce national legislation, they have to take into account what the ECJ has said in its judgment.
This judgment is not necessarily a total knockout for data retention but it is an example of judicial rulings in which the court indicates what factors legislators should take into account if they want to introduce some kind of mandatory data retention at a national or European level.

Question:
4) **Prof. Martin Scheinin:** It has been said that data protection does not deserve to be a human right, that it is not worthy of that status. Or that not everything that was written into Article 8 of the Charter should have the status of a fundamental right. What is fundamental in data protection, if not the full scope of current data protection principles? Have national and European decision-makers instituted a standard that is too strict?

Answer:
Mr. Paul Nemitz: Mr. Nemitz considers that it could be an American debate. In the USA,

one would look into the Constitution. The intellectual effort should be: what is privacy for? Why is it essential? The reality is that our Charter of Fundamental Rights is primary law and what is said there should be considered as such.

Question:
5) **Prof. Helen Nissenbaum:** Prof. Nissenbaum expresses concern about the right to be forgotten.

Answer:
Mr. Paul Nemitz: Everybody needs to recognise that, firstly, the right to be forgotten has to be balanced with other fundamental rights and, secondly, fundamental rights have to be balanced with important objectives of public interest. Mr. Nemitz has no doubt that a reasonable judge will always find a solution to these two aspects. The debate about the right to be forgotten is largely inspired by an American tool: Google.

16:45 – 18:00 | **Panel: Targeted use of surveillance technologies to control individuals considered as dangerous**
Principal speaker: Michele Panzavolta – University of Leuven
Panel members: Nils Zurawski – University of Hamburg (IRISS), John Guelke – University of Warwick (SURVEILLE), Antonis Samouris – Counter Terrorism Specialist / future Europol Counter Terrorism Specialist, Ilana de Wild – Human Trafficking and Child Exploitation Team, Interpol / National Police of The Netherlands
Chairperson: David Wright – Trilateral Research & Consulting (IRISS)

Surveillance technologies have long been developed to prevent and investigate offences. Dealing with terrorism and organised crime, States have extended this use for security purposes more generally. Suspicion has become a pretext for conducting targeted surveillance over specific individuals or groups and this surveillance may involve a plethora of different technologies. With respect to criminal justice procedure, distinct issues arise that shall be addressed in this panel. For example, competent national authorities are using information gathered more generally against suspects and potentially infringing their rights (gathering information may interfere with the right to data protection): practices may challenge the presumption of innocence, which is said to have been increasingly replaced by a presumption of guilt. Further, administrative measures in the spheres of immigration and post-detention monitoring are increasingly implemented using surveillance capabilities due to the risk an individual is believed to represent. What is the legal basis for such activities? Are such measures implemented in compliance with human rights standards?

Mr. David Wright introduces the speakers.

Prof. Michele Panzavolta
Public authorities are using surveillance to control dangerous individuals. There is a growing tendency to use preventive surveillance in this way before crime (*ante delictum*). In many countries, monitoring powers for preventive purposes - mostly connected to national public security - are in expansion. In preventive surveillance, the objective is the identification of a profile of dangerousness before the commission of a crime. This can lead to different forms of interference with personal data.

Why are criminal lawyers sceptical about preventive surveillance?

- They are afraid of authority because it encroaches on citizens' rights.
- Criminal lawyers are afraid of the future. Criminal law is more about being retrospective. Retrospective judgments are safer.

Subjective and objective perspectives can be easily blurred. There can be a shift of focus from an objective element to a subjective perspective.

There is something that the judicial control mechanism cannot do: control over the principle of subsidiarity. The authorities should have the entire bank of evidence but sometimes information is secret.

Mass surveillance concerns the entire population without being particularly extensive. By contrast, targeted surveillance can be very extensive and worse than mass surveillance from an individual perspective. Is it possible to draw a line between mass and targeted surveillance? Does it make a difference whether it is targeted or not?

Preventive surveillance is also a concern regarding the presumption of innocence. Is using surveillance technologies interfering with this principle? Does it affect personal liberty? There are several degrees of surveillance. Does this level of surveillance respect the principle of the presumption of innocence? Is monitoring people equivalent to considering them to be guilty? According to Prof. Panzavolta, there is no clear answer.

Dr. Nils Zurawski

The way new technologies should be used by law enforcement agencies and other competent national authorities is not clear. It is important to look at how they reach the degree necessary to suspect an individual of preparing a crime or of having committed one. What is the power of statistics that lead to categories of suspicion? Who is in the categories of suspicion? And why are some people in these categories? How does the police generate information on a suspect from the data?

The process of making someone a suspect depends on the motivation made by police to get technologies and how they use that technology. Technologies can be used in many different ways; potentially different from what the constructor had originally thought.

Dr. John Guelke

Dr. Guelke is working on ethical aspects of surveillance in the SURVEILLE project. The main ethical risks of both mass and targeted surveillance are encroachment into privacy, mistakes that can damage the relationship of trust between communities and police, even when surveillance is justified.

Mass surveillance usually involves everyone in a particular area or activity. By contrast, targeted surveillance focuses on a specific context. The latter is more intrusive in terms of privacy than the kind of attention involved in mass surveillance. Dr. Guelke suggests that targeted surveillance is worse than mass surveillance, where attention is split among a large number of potential targets.

For example, somebody is walking around in a public space. He is watched by a CCTV just in the context of a normal operation of public order monitoring. However, he can also be photographed by a surveillance team as a suspect in a specific investigation.

Similar technology can be used for mass or targeted surveillance purposes but with completely different consequences. The distinction is still very problematic. In particular, a series of problems can be encountered with mass surveillance: whether it is discriminatory or not, whether it is directed towards the wrong people, etc. By contrast, targeted surveillance

can be justified if the evidence is strong enough.
Dr. Guelke considers that limitations on liberties require a higher threshold of control when surveillance technologies are implemented for prevention purposes than for investigation purposes.

The final question asked by Dr. Guelke is: where is the boundary between controlling individuals and preventing threatening criminal acts?

Mr. Antonis Samouris
Mr. Samouris starts by asking several questions: How is the suspicion created? Who decides on dangerousness? And how is it done?
Mr. Samouris considers that there is a link between immigration and terrorism. It is much more intense nowadays with conflicts in the Middle East, Africa and Asia. With the increasing levels of migration, there is a clear tendency towards securitisation from external threats.
As a practitioner, Mr. Samouris declares that law enforcement agents decide who is a potential suspect everyday. Therefore, they also decide who should be the subject of surveillance measures.
Mr. Samouris expresses a particular concern about the large number of EU citizens travelling to Syria, to Iraq or to other conflict zones. The main issue that law enforcement agencies face is related to the return of these people because they do not know whether they were involved in extremist activities or whether they had gone to these countries to help their relatives. How do competent national authorities approach these people? How do they approach people that wish to travel to the conflict zones to offer humanitarian aid? Practitioners, including police officers, security officers and even judges are affected by this climate of securitisation.
At the European borders, the EU is introducing smart borders, it merges biometric databases with other databases and it creates big network of mass surveillance.
This also challenges the presumption of innocence. Do competent national authorities think that they are guilty in advance because they come from a conflict zone? They face big challenges and they would like to be helped by policy-makers and lawyers to find out what constitutes a proportionate use of surveillance.

Ms. Ilana de Wild
There are specific rules on individuals considered as dangerous, including transnational sexual offenders. Generally, these offenders reside in another country and sexually abuse children whilst abroad. In this kind of group, most of the people have already been convicted for child abuse. Knowing that, it is important to take some action. The internal movements of these groups and their communication should be better observed (targeted surveillance).
For Interpol and the law enforcement community, it is very important to share information. Therefore, they are developing communication tools such as national police databases including people who have already been convicted and information about threats to society. Ms. De Wild asks whether this information sharing is very targeted.
Looking into such a groups it becomes apparent that communication takes place via the internet to establish how one might sexually abuse a child. This information is normally found on public websites but also on the private and deep, dark web. This is where law enforcement really needs technologies. It is not logical to do a manual search. Specific tools are needed to find specific information.
With regard to transnational sexual offenders, there is a need to know which countries people go to, the geographical areas, just to make the right decision where to go and where to place Interpol's people.

Q&A discussion

Question:

1) **Mr. David Wright:** A clear distinction between targeted and mass surveillance is absolutely necessary. Regarding the daily-based tools used to identify offenders, is this mass or targeted surveillance?

Answer:

Ms. Ilana de Wild: It is more the other way around. In this field, there is so much material already that there is no need for us to find information about suspects.

Question:

2) **Prof. Martin Scheinin**: One category is surveillance by profiling, which should not be accepted as targeted surveillance. Targeted surveillance is surveillance of individuals that are already suspected because of their conduct, not because of fitting a profile. The key message should be that the initiation of suspicion must not be based on mass surveillance. There must be other factors that drive the suspicion. Another thing to remember is that the presumption of innocence is triggered as a legal right only when a person is charged with a criminal offence. There is no fundamental right not to be suspected of a crime but a right to be presumed innocent even when named as a suspect.

Answer:

Prof. Michele Panzavolta: Surveys have been conducted in the States about discrimination when dealing with mass surveillance. It is not clear whether it can be counted as some form of control. How far can we control these practices? The notion of "charge" on an individual must be substantiated with evidence. The tracking in prison is replaced with electronic tracking. The problem of the presumption of innocence is still present. When there is an acquittal, data must be erased. Otherwise, the simple fact of considering someone dangerous runs against the presumption.

Question:

3) Member of the audience: The terminology is not clear: blanket surveillance, blanket collection of data (both terms agreed by the police), etc. We really need to define the terms at stake to understand the reasons and the process.

To **Ms. Ilana de Wild**: A very high proportion of child sex abuse happens in families. What about the implications of that for this kind of surveillance? If the goal is to reduce child sex abuse, how significant is Interpol's work, starting with the assumption that most of the abuses take place in the family?

Answer:

Ms. Ilana de Wild: Indeed, the majority of child sex abuse takes place within the family. Some people say it is even 75-80%. Using the internet is very easy for families to sort of distribute the material on demand. This is directly connected. There are abuses in some families but it is then distributed and available for everybody on the web.

Question:

4) **Dr. Francesca Galli**: With regard to presumption of innocence, do we really understand what surveillance is and could be? The problem is how surveillance is done and at what level. We do more and more surveillance at a preventive stage. Then, the issue becomes: What do

we do with the material we gather? Who controls it? We have no agreement between different States. Law is one of many answers to help us to identify when and how to use surveillance. We need to find common ground on what is a suspect. What can be used and when?
What next? There are many issues. So how do we cope with all the issues?

Answers:
Prof. Michele Panzavolta: As a lawyer, Prof. Panzavolta considers that he is ignorant in this matter. He is not sure that a lawyer can address these issues.

Dr. Nils Zurawski: We should find more common ground to answer your question. The answer is that there are many aspects and a common ground in many aspects must be found.

Mr. Antonis Samouris: We have a methodological problem in our work, especially when it comes to defining suspicion and dangerousness. We deal with law enforcement agencies and security services that have different methodologies to define suspicion, which lead to different conclusions. In particular, agencies are somehow obliged to share resources and, in practice, to exchange data. Therefore, this is how suspicion is created. It is also a question with respect to politicians: what do they say about the groups of risk? It is also a media issue. It is a whole complex set of issues that finally defines suspicion and dangerousness.

Mr. Walter Coenraets: A clear definition of surveillance and privacy is the first essential step before going further. Privacy in 2006 is different from privacy right now. Surveillance with CCTV is different from surveillance on the internet. The context is essential. It is what makes the difference on privacy matters.

Thursday, 30 October 2014

PART 3. PANELS ON THE TECHNOLOGICAL ASPECTS OF SURVEILLANCE (bis)

Organised by RESPECT with contributions from IRISS and SURVEILLE.

9:00 – 10:30 | Panel: **The Role of Law Enforcement Agencies in Surveillance**
Principal speaker: Christian Karam – Digital Crime Officer, Interpol
Panel members: Gemma-Galdon Clavell – University of Barcelona (IRISS / RESPECT), Ilana de Wild – Human Trafficking and Child Exploitation Team, Interpol / National Police of The Netherlands
Chairperson: Edward Beaman – University of Central Lancashire (RESPECT)

Criminal trends have rapidly evolved over the last twenty years mainly due to the fact that criminal innovation pools its resources directly from society and is able to adapt to technological changes with little legal restrictions implemented. Moreover, new technologies enable and facilitate the perpetration of criminal acts and, as a consequence, law enforcement agencies need to step up the level of appropriate tools to combat those crimes with a view to protecting the security of citizens. This panel will discuss challenges that law enforcement agencies are currently facing.

Mr. Edward Beaman introduces the speakers.

Mr. Christian Karam

What is available in the current public sphere for everyone to use? Indeed, a lot of cybercrime nowadays is about the use and misuse of products available to the public.

Great innovations are actually changing the way technological evolutions are seen. Some technological developments can be seen as great initiatives. They give developers and researchers the possibility to receive funds and achieve production goals. However, it can also be used by anyone for criminal purposes.

- **Ghost gunner**: It was released two months ago. It prints 3D guns in metal and it costs only 200 USD. A solid concept is a company providing free maps so that you can create your own weapon at home. The product was crowd-funded. This is one way in which crowdfunding could be a threat. The problem is that the bigger these printers get, the bigger the weapon printed will be that is circulated without being registered.

- **Radio-centric communication:** A lot of companies are developing applications and products which tend to circumvent the internet. They use radio as an alternative.
  - ***Gotenna*** is a small antenna with a range of five miles, which makes it possible to connecting the computer with another *gotenna* and makes it possible to communicate between smart phones and PCs in encrypted codes. It can be used as a messaging platform, which is great for terrorism in a city, for geo-localisation and also to trigger functions like triggering a bomb without needing the internet.
  - **Mesh technology**: *Firechat* is, for example, very successful. In Hong Kong, in the past few weeks, the internet was shut down. *Firechat* can create a restricted network. People like this technology, firstly, because they do not pay for data any more and in this way they do not have to go on the internet. There is an even more interesting aspect about that: people do not think about security on these networks. They use data that are not encrypted. People think about functionality more than about paranoia. However, applications like *Firechat* could be used by drug trafficking cartels, etc.

Crowdfunding is a great opportunity to develop new technologies but it is essential to limit what is produced on the base of a proactive and preventive method. These tools could be used to circumvent law enforcement agencies from reading data and analysing data.

- **Dark Wallet**: if people have Bitcoins, they use a Bitcoin wallet. The dark wallet is a Bitcoin wallet that provides anonymity features and money laundering features. The creator of the dark wallet is the same as that of the ghost gunner.

The *Coin joint feature* works as such: Helen wants to buy a pair of socks and John wants to buy LSD. There are two different buyers and two different sellers. Usually, if you make a transaction with Bitcoins it is from an anonymous entity to an anonymous entity. This means that nobody is recorded but the transaction itself is recorded. In this case, the dark wallet does not allow the *blockchain,* which is the process by which the transaction is recorded. The dark wallet merges the two payments into a single one. If competent national authorities try to trace back the item that was bought, there is no way to reach the sources.

- **Actual onion routers**
  - **Anonabox**: It is a small router that you can connect that has its own proxy. It has been suspended because there was a scam with the developer.
  - In the main period, a dozen similar products were released, such as *Tor network Project Sierra, Onion pie* and *Wemagin*: routers anonymising data connection.

These products create the possibility for cybercrimes to act completely in the dark, with no forensic evidence when the case comes to court.

Now, the new rush is to create anonymous Tor routers. These devices will anonymise data and are available for the public and so for criminals. With the aim of securing the data of individuals, these devices provide an opportunity to hide cybercrimes much more importantly than before.

- **Illegal market places:** Grams, Helix Light, Silk Road, Tom, Evolution, Hydra, Outlaw are some of the main illegal market places where you can basically buy everything from guns to fake identities. There are systems that give "fresh, clean" coins that have not being involved in any transaction (*e.g.* Helix).

The Dark Market is a market place that is designed to sell everything completely freely, which obviously also includes illegal goods. The network cannot be shut down as a whole. Only single pages of sellers could be shut down and so it takes a huge amount of work and effort to do that.
If one note is compromised by the NSA, you cannot shut down the entire system but only the single user page.

- ***Github*** is a network that allows people to code together. A parallel project was developed to develop illicit marketplaces. Open Bazar provides similar services.
- ***Storj.io*** is a crowd-sourced platform that is a decentralised cloud storage company insuring that data uploaded is protected.

"I get into the network, I become a note, I upload a file – the file is divided into three chunks – shared with three people encrypted." To analyse a file, the three people that received the chunk should be found. Someone can rent a free space in her/his computer and nobody will know what she/he is hosting. It could even be child pornography.
Again a big tool for everybody - anonymous and secure – means that it is also a great tool for criminals.

- **Dark-er Coins** *i.e.* **Blackcoin, Neutrinocoin:** bit coins are blown into pieces in multi-fragments. When you receive a payment from these types of Bitcoins, you can receive the payment from 400 people. Therefore, it is impossible to reach the actual buyer.

Taking down a note does not really affect the whole ecosystem. Law enforcement agents are really out of this scope. Law enforcement has very little capability when it comes to cybercrime. They need more power to intervene.
The implications and the impact of crowdfunding and crowdsourcing can be huge. Law enforcement is quite limited in this connection. Decrypting or shutting down these pages is a long and complex process, which often takes longer than the time needed to create a new page.

Ms. Ilana de Wild
Internet can be used for innocent or criminal purposes, including paedophilia. The internet helps to get in contact with children easily. At national and international levels, it is fundamental to work with databases on child pornography. Interpol owns a single database for child abuse gathering information from all over the world. These databases could be better used if some technological tools could be implemented in them:

- Tools such as *facial recognition* could be useful to identify victims. It is very

expensive to integrate these tools and it also takes a lot of time.

- Another useful technological tool to identify suspects is *sensor-based technology:* Pictures taken with the same camera could be provided with a sort of digital fingerprint. Every camera produces a unique noise pattern, which leads to an image and in this manner you can easily connect different pictures from the same camera.

There are more and more videos instead of pictures, which means a higher level of difficulty for law enforcement agents to analyse the huge amount of material.
It is easy just to get in contact via the internet with the poor family that will let the abuse happen or commit the abuse themselves. The tracing of financial data is an aspect that is becoming more and more important. In a way, there is a sort of normalisation in the web about sexual issues. Children are increasingly on the web and show interest in sexual behaviour. Children of seven, eight and nine years old are at the mercy of grooming and "sextorsion".

- *Grooming* techniques are developing with strategies of trust and manipulation to create trust and affection, encouraging the children to do things that they would not have done otherwise.
- *Sextorsion* is a form of sexual blackmailing. Children are threatened and are forced to be silent about the abuse that they are undergoing.

Dr. Gemma Galdon Clavell
There is enough material to know that a crime is being committed or has been committed and to start to suspect. However, we are facing three important paradoxes:

- The largest amount of funds on security technologies has been invested but citizens are feeling more and more insecure.
- The risk assessment is not correctly done. People are scared about large-scale threats but they are not scared about day-to-day dangers even if the probability of, for example, dying in a car accident is higher than any other risk. It is a matter of trust. People are less and less trusting.
- Most people choose to do "good". The decision-makers do not invest resources to promote good behaviours in new technologies. They focus on that 1% despite improving the behaviour of the other 99%.

In pointing out political efficacy much more than security efficacy, decision-makers and the society, in general, will not succeed in fighting security issues. Good policy-making does not mean implementing more and more CCTV.

Dr. Clavell considers that policies implementing control over the citizens reinforce inequalities. On the one hand, children from wealthy families do not feel affected by CCTV because they think that cameras are looking at the bad guys to protect them. On the other hand, children belonging to poor social backgrounds feel that they are being watched by CCTVs.
In addition, surveillance technologies do not make crime disappear. Criminals adapt their crime depending on the implementation of surveillance technologies. For instance, they commit their crime in another neighbourhood, wear hoodies, etc. CCTV can be useful when it is implemented in the right area. Some are install when it is less of use (*e.g.* in city centres where there is social control). Policemen do not want CCTV any more, but politicians do because the other countries use it. Conversely, CCTV can undermine trust. The governments say, "I do not trust you". The police cannot have the monopoly on technology: if the police use CCTV, citizens use smartphones to control the police (backlash). It is something to take

into account before further technological developments.

Dr. Cavell also considers that tools must be better assessed. Ethics and desirability of technologies should be improved, especially because it has an impact on the acceptability of the population.
Dr. Cavell proposes to move away from fear and look at data when assessing surveillance technologies. Even when responsible technologies are promoted, people do not react in a rational way, people are scared about their privacy.
The choices that are to be made may leave out a lot of considerations such as cost and benefit analysis.

Q&A discussion
Question:
1) **Mr. Edward Beaman**: Should law enforcement agencies allow surveillance projects to establish who is doing "good" or "bad"? And if yes, do they have the technological expertise to do it? Could the resources be invested to assist law enforcement agencies?

Answer:
Mr. Christian Karam: Law enforcement agencies currently have to evolve. The way law enforcement officers used to do cyber investigations is not working any more.

Question:
2) **Ms. Maria Grazia Porcedda**: Do we need to invest in non-intrusive tools? What is Interpol doing in this regard at the moment?

Answer:
Mr. Christian Karam: If you use some technologies that make it impossible to prosecute criminals afterwards, this technology will be suspended. My only concern is the result of a technology used.

Question:
3) **Ms. Maria Grazia Porcedda:** What has changed in the years in connection with prostitution is that we are tackling child pornography but not child exploitation in prostitution in the streets.

Answer:
Ms. Ilana de Wild: These two aspects are two different sides with human traffic, on the one side, and children-related crimes, on the other. This behaviour could be described as hypocrisy but it is important to mention that the definition of prostitution changes depending on the country. It is true that outside Europe this problem is not given much recognition. For some countries, child abuse is not even an issue. There are a lot of factors that have to do with economic and social circumstances. In Europe, the situation changes a lot depending on the area. This is a problem that is often not tackled in an effective way.

Question:
4) **Prof. Joe Cannataci**: The policy approach must be discussed. What are the three projects going to advise the policy-makers to do about it? Are we concerned about the fact that somebody out there is going to make guns? No - because people have been making guns illegally for the past few years. Using the internet is just another way to do that. Given the threats that crowdfunding could represent, what should we do?

It is not new that people try to build guns on their own and they will go on doing so. The most significant issue is not the crowdsourcing and is not about the instructions on how to make guns. The most significant issue is that organised crime does not need crowd sources. Therefore, either Interpol is going to focus on these small crimes or on serious organised crime. If we are looking to discuss a public policy on cybercrime, this is what we should tackle. Petty crimes and threats should not be forgotten but, at the same time, it is necessary to point out the large-scale issues.

Answers:
Mr. Christian Karam: Some points can be said in public, others cannot. Talking about serious organised crime on the internet, I do not agree with you on one point. If you do not think that printing a gun at home by your children or somebody that is not able to understand the use of these items is not a problem you are basically promoting crime. The same thing goes for the dark net. It is becoming easier and easier to access drugs or other illegal and dangerous goods. The dark net is a promotional tool for petty crime.

Dr. Caroline Goemans-Dorny: In Amsterdam, there are CCTVs not for political reasons but for security measures based on quantitative resources. Certainly, it is important to focus on organised crime but, for Interpol, it is also important to figure out how new crimes are developing to deal with them.

PART 5. PANELS ON THE SOCIAL IMPLICATIONS OF SURVEILLANCE

Organised by IRISS with contributions from RESPECT and SURVEILLE.

10:45 – 12:00 | **Panel: Surveillance, Resilience and Democracy**
Principal speaker: Kirstie Ball – Open University (IRISS)
Panel members: Simon Chesterman – National University of Singapore (National University of Singapore), Roger Clarke – Advisory Board (IRISS), Christian Hawellek – Leibniz University of Hanover (RESPECT)
Chairperson: Roger Clarke – Advisory Board (IRISS)

This talk examined the troublesome relationship between surveillance and democracy in Europe. Through a detailed empirical examination of three surveillance practices across Europe – ANPR, Credit Scoring and Neighbourhood Watch – it highlighted, explored and theorised this relationship. The talk's basic theoretical premise was that, while surveillance practices can be deployed to counter threats and risks and to prevent harm occurring, they also create potentially harmful consequences. The reliance of surveillance practices on proprietary information infrastructures can make surveillance processes non-transparent and unaccountable to democratic scrutiny in cases where harm occurs. It is argued that the traditional venues of democracy, where citizens and institutions engage, participate in debate and create governance structures, cannot be mobilised without widespread awareness of the harms and consequences of surveillance practices by both citizens and institutions. This awareness is lacking in most cases. The talk also reveals the deep historical, social, political and legal antecedents of the current state of affairs.

Prof. Roger Clarke introduces the speakers.

Dr. Kirstie Ball
Three surveillance practices across Europe have been taken as case studies and compared one

to another in their relationships with democratic process.

1. ANPR: a form of State-citizen surveillance
2. Credit scoring: a form of crime acceptance citizens' surveillance
3. Neighbourhood watch: a form of horizontal surveillance

Theoretical premise: Surveillance practice deployed to counter risks and threats can be used to protect democracy but can also create harmful consequences.

In terms of democratic process, the level of analysis adopted can be divided into three:

- Governance: the way surveillance practices are regulated.
- Participation: the extent to which surveillance practices are codetermined by different stakeholders.
- Engagement: personal interaction and awareness of people.

Methodology: The case studies are chosen according to protocols that can make them comparable.

Countries analysed:

- Slovakia
- Belgium
- The United Kingdom
- Germany
- Spain
- Austria

Central findings: If the objective is to increase resilience in Europe, it begins with increased public and institutional awareness about costs and benefits. Institutions generally demonstrate satisfaction but issues like human rights violations and privacy violations, environmental harm and a lot more are not taken into account.

1. ANPR: This is a digital CCTV camera that captures images of vehicle registration plates. The collection of data could be analysed for multiple purposes. Thus, the use of ANPR covers quite a wide range of organisations, including public and private sectors.

The use of ANPR has mainly been a problem in terms of its regulatory aspects. In Belgium, it is considered that it compromises people's rights. In the UK, the right to protest has been considered compromised. ANPRs were used to register the activity of the vehicle belonging to protesters, which was stopped repeatedly later on. In Slovakia, it is only used to administer roads.

The German case is particular. In 2008, the Constitutional Court decided that the misuse of ANPR infringed the right of information. The use of ANPR is strictly regulated. They could be used only in the case of immediate and concrete risk. If it is not the case, data have to be deleted straight away. Therefore, data retention has to be related to a specific threat. German police may be underestimating the actual threat, making the use of ANPR data basically impossible.

2. Credit scoring: It consists of a rational collection of data about citizens with the explicit intent of using this data to influence which financial products could be offered.

Via credit scoring, financial institutions gather credit information about people and match them using statistical analysis. Even life style information could be registered and could limit your credit score. It is becoming a social issue, influencing people's behaviour and perceptions, particularly in the US.

However, harm can result from this surveillance. It is an administrative tool subject to administrative regulations and it be subject to misuse by financial service employees.
In Austria, some Court staff used the findings of credit score files and sent them to financial services institutions.
In the UK, the phenomenon of *payday lending* is a small, short-term unsecured loan regardless of whether repayment of loans is linked to a borrower's payday. They considerably influence credit scores. In the UK and Norway, the legislation is quite a lot more open and this helps to manage data protection linked to a credit score. In Norway, credit scores are included in data protection law. All citizens have access to them.

3. Neighbourhood Watch: In Anglo-Saxon countries, it is associated with something quite normal. It is different in countries that had a fascist or authoritarian regime in the past.
Perception of authority in Austria, Germany and Spain is extremely different. Surveillance technologies used by neighbourhood surveillance groups are feared because it represented an opportunity for political extremists, in particular for vigilantes that could actually physically harm people. It also stigmatises spaces. It creates the feeling of some spaces being unsafe. It also challenges authority, social beliefs about how the police should be responsible for acting for law enforcement. In particular, in Spain, the emergence of *citizens' patrols* seems to act as a barometer for public insecurity. Community patrols tend to emerge in reaction to threats like broken windows' policies and so on. It developed in the 2000s with police starting to take notice of citizen patrols and taking it as an indication of the areas where they needed to act. However, it was never about recognised community policing. By contrast, in Austria and Germany, there is no real place for neighbourhood watch.

Social and political factors shape the emergence and the use of surveillance technologies:

1. ANPR: It is mostly shaped by legal and political factors.
2. Credit scoring: A wide range of factors seems to be shaping the outcomes. A big issue is the way in which every single country acted towards the issue of data protection (*e.g.* Norwegian experience is seen as completely different from the Italian case). The institutional factors are quite important. Some banks are trying to resist regulation on the use of credit scoring, particularly regarding consumer protection. Finally a really big issue is the fact that, in the UK, credit scoring is becoming a relevant aspect of social life.
3. Neighbourhood watch: Political factors connected to the national political system is of interest in the relationship with the authority. That seems to be one of the most important factors.

What is really interesting is what these outcomes could teach us. Surveillance is first and foremost an organisational principle. The practice of surveillance is a history of how bureaucracy emerged in public and commercial life. The way surveillance practice is shaped explains how the society is conceived, shaped and organised.
One of the noteworthy aspects was the extremely low level of participation by citizens in surveillance practices. There was very little co-determination and that is indeed the key to increase the level of democracy and develop a good relationship with the public.
Dr. Ball concludes in saying that, above all, there is a clear need to improve the level of transparency and accountability. Dr. Ball proposes that a policy outside the conventional venue that could emphasise the engagement and participation of citizens. It is an aspect that could enhance the use of surveillance.

Mr. Christian Hawellek
Mr. Hawellek states that the RESPECT project has reached similar conclusions, especially when it comes to privacy issues and social stigmatisation in the context of surveillance.
Surveillance technologies are protecting the population by preventing crime but they are also creating opportunities for harm. It is therefore fundamental to understand how to combine surveillance practices with adequate protection for citizens.
What the RESPECT project intend to achieve is to categorise surveillance technologies to distinguish target and non-target types of technologies. Also, technical aspects are mainly discussed, including for what matters are the technologies used and the way they are used. There are some factors that need to be changed, such as a certain blur between the private and public sector.
The practice of retaining data can lead to disproportionate use of that data. It is very important to be aware of the consequences of the use of these technologies.

Prof. Roger Clarke
Prof. Clarke points out that it is important to reflect on the five dimensions of privacy:

- Privacy of physical persons
- Privacy of personal behaviour
- Privacy of personal experience
- Privacy of personal data
- Privacy of personal communication.

This model is completely inadequate when it comes to privacy of personal behaviour and privacy of personal experience.
The serious weaknesses of the democratic legitimacy of data surveillance are due to the lack of regulation in the law and in the constitutions. When defining personal rights, the impact of technology assessment on law making is quite limited. In fact, the state of the art in terms of regulation of surveillance technologies is a complete dominance of political processes in the decision-making in the public and private sectors.
There is no simple structure of principles to guide the design of evaluation processes. There is a requirement for justification that the current use of surveillance technologies is not meeting.

Prof. Simon Chesterman
Why should decision-makers and people, more generally, care about law? Why should the law be that important in that process?
Prof. Chesterman considers that the law is important. It can be a legitimising factor and lead to better decisions. Having a legal foundation for something like surveillance, as a technique rather than an organising principle, makes it more legitimate and can actually lead to an expansion of the process and obviously this legitimisation could be read in a good way as in a bad way. The legitimising factor attempts to provide a rational basis for the decision-making.

The law provides a framework of what a community can do, of what a police officer can do.
The law is struggling to catch up with technology. In Prof. Chesterman's opinion, accountability and regulation cannot focus simply on the collection activity.
The society needs structures to avoid too much bad decision-making, especially in regulating these surveillance technologies. And, then, the society needs to give them legitimacy via the law.

Q&A discussion

Question:

1) **Prof. Charles Raab**: Would it not be better to have a principle-based regulation rather than a rule-based regulation? What do you think about the relationship between the two?

Answers:

Prof. Roger Clarke: The problem is that they both lack effective authority. Ethics do not oblige people to do things. The best possible outcome would be to integrate principles into a good law. However, we may not be able to rely on parliaments in this respect.

Prof. Simon Chesterman: Prof. Chesterman is a great sceptic of principles. The concern would be that giving up on hard laws would cause problems of legitimacy because, if there is one thing that law could offer, then it is clarity. And, when we slide into principles, you are actually denying one of the best features of law.

Question:

2) **Prof. John Mueller**: Talking about neighbourhood watch campaigns, are they cost effective?

Answer:

Dr. Kristie Ball: Neighbourhood Watch developed in a social change over the community in Britain. It is very difficult to get figures about how much effectiveness was registered from these campaigns.

Question:

3) **Prof. Roger Clarke:** To what extent has technological progress influenced neighbourhood watch?

Answer:

Dr. Kristie Ball: Nowadays, we are witnessing a massive use of social media in Neighbourhood Watch. For example, in Austria, databases are shared both by the police and citizens.

Question:

4) **Dr. Nils Zurawski**: Talking about resilience, there is a special twist in neighbourhood watch, which is worth mentioning. What do you think about it?

Answer:

Dr. Kristie Ball: Neighbourhood Watch constitutes an example of community resilience facing passive surveillance but also an example of community breakdown as well.

Question

5) Representative of the European Commission: One of the most interesting aspects of your presentation (Kristie Ball's) were the differences between countries and how they were linked to their different historical backgrounds and cultural context. To what extent do you think that resilience could be addressed by a European initiative to find solutions at a European level?

Answers:

Dr. Kristie Ball: Some of the examples that we found to be the best practices in our research

lead us to the question as to whether they could be adopted at European level to promote good practices (*e.g.* the German experience with ANPR and the Norwegian experience with credit scoring). We should work to adapt these experiences to the widest range of uses as possible.

Dr. Gemma Galdon Clavell: With regard to neighbourhood watch online in Spain, we found out different dynamics but one interesting thing is that we found Facebook-based neighbourhood watch and Twitter-based neighbourhood watch to be founded by English citizens resident in Spain. Different contexts deserve different pattern of analysis.

12:45 – 14:00 | **Panel: The Intersection of Surveillance with Citizen's Rights**
Principal speakers: Clive Norris – University of Sheffield (IRISS), Xavier L'Hoiry – University of Sheffield (IRISS)
Panel members: Antonella Galetta – Vrije Universiteit Brussel (IRISS), Claudia Colonnello – Laboratory of Citizenship Sciences (RESPECT), John Mueller – Ohio State University (SURVEILLE)
Chairperson: Ivan Szekely – EKINT Budapest (IRISS)

In the context of surveillance and democracy, the principles of consent, subject access and accountability are at the heart of the relationship between the citizen and the information gatherers. The individual data subject has the right to at least know what data is being collected about them and by whom, how it is being processed and to whom it is disclosed. Furthermore, they have rights to inspect the data, to ensure that it is accurate and to complain if they so wish to an independent supervisory authority who can investigate on their behalf.
This panel presented the results of our multi-partner project on surveillance and democracy as part of the IRISS project. In particular, we focused upon the ability of citizens to exercise their democratic right of access to their personal data. Together with ten partner institutions, we conceptualised a research approach involving auto-ethnographic methods which sought to 'test' how easy or difficult it is for citizens to access their personal data by submitting subject access requests to a range of local, national and supranational institutions across both public and private sectors. We presented the overall findings of the ten country study and considered the strategies used by those who hold our personal data to facilitate or deny us access to what they know about us and how they process it.

Dr. Ivan Szekely introduces the speakers.

Prof. Clive Norris and **Dr. Xavier L'Hoiry**
Question of research: Could we find out what information organisations have about us?

- How do organisations collect information?
- How do they keep it?
- With whom do they share it?
- Do the citizens have the right to know about it and to have their say about it?

There is a piece of socio-legal research concerned with the exercisability of access rights. It is part of ARCO rights (Access, Rectification, Cancellation, Objection).

The Directive 95/46 EC, Article 12, provides that:
"Member States shall guarantee every data subject the right to obtain from the controller:

(a) Without constraint at reasonable intervals and without excessive delay or expense:
- Confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- Communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- Knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) As appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
(c) Notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort."

Prof. Norris and Dr. L'Hoiry consider that exercising access rights is a two-phase process:
1. Locate data controllers: when you make a request, you need to know who collected the data. For this purpose, they have visited 327 websites, including contact details via online platforms, in persons and via telephone.
2. Submit the request to access the data.

In some cases, the response is impossible to get despite the fact that it is actually be guaranteed by law. The best answer came from Italy. The response was very quick in terms of the legal response time. They fully disclosed the data they have. It is a standard example of what can be achieved by organisations. Unfortunately, these organisations were the exceptions and not the rule. Exercising our rights tends to be a race with many obstacles.

Headline findings
- 20% of data controllers cannot be identified before submitting an access request.
- One in five CCTV operators do not display any face.
- 43% of requests did not obtain access to personal data.
- 56% of requests could not get adequate information regarding third party data sharing.
- 71% of requests did not get adequate information regarding automated decisions.
- Subversion of the law: law in books is very different from law in action.

In some cases, they answered positively saying that data was shared with organisations but there was a complete refusal to provide the identities of these organisations.
If you take an informational right perspective, you should be able to know which information an organisation has about you and with whom they shared and for which purposes. However, these results are completely undermined. If the organisation answers, "we share your data with other parts but we are not going to tell you who they are", you loose your power to exercise your rights over data.

Discourse of Denial
Data controllers employ several key discourses of denial to restrict data subjects' ability to exercise their rights:
- Out of sights
- Out of court

- Out of order
- Out of time
- Out of tune
- Out of mind

- **Out of sights:** data controllers render themselves invisible, severely restricting and delaying the access request process.
    - Silence in response to the requests: it is difficult to deal with silence. What can happen to citizens is that, at a certain point they simply give up.
    - Poor content in privacy policies
    - Inability to identify single officer to liaise within an organisation
    - Lack of or poor CCTV footage.

They can use silence as a strategy. You send a letter or an email and you never get a response. Another use of silence was to get an automatic reply: "your request has been taken into account" but then they never replied. Silence is quite difficult to deal with. It leads to a simple reaction by citizens: they give up.
Even when complains have been made to the Data Protection Authority (DPA), sometimes Prof. Norris and Dr. L'Hoiry did not receive any answer. A quite shocking example concerns Oslo, where they still do not know who controls CCTVs in the city.
They even face a bank manager saying that they do not have the right to access data. As a citizen, it is very complicated to respond to that unfounded denial. People do not have the necessary tools.

- **Out of court:** Data controllers and their representatives incorrectly rely on legal exemptions to rule requests out of court:
    - Only the police may access the CCTV footage
    - No right to see the data but only a list of what data is held about you
    - Not possible to view the footage because it would infringe the privacy of others
    - Not a customer, so do not fulfil the category of people having the right to request.

- **Out of time:** Time is used in a variety of ways to restrict and delay access requests:
    - Data controllers respond beyond legal timelines
    - Lengthy delays before receiving disclosure of personal data
    - Data retention period used as a shield to avoid disclosing data

- **Out of order:** Bureaucratic procedures are inadequate and the access request process therefore breaks down:
    - Technical problems
    - Missing information in disclosure of personal data
    - Missing lost letters to and from data controllers
    - Out-dated information on privacy notes
    - Dead telephone numbers (it is not an exhaustive list).

A researcher in Austria tried to submit a request for his mobile phone. He located the number on the internet. He finally succeeded in finding someone to answer but the person in charge of the service answered that he was not aware of any rules related to data protection. The procedures were so strict that there was no actual chance to make a request.

- **Out of tune:** Some data controllers only accept requests using extremely narrow mechanisms restricting our ability to exercise informational self-determination.

- Self-download tolls (restrictive)
- Knowing the unknowable
- Linguistic imperialism

- **Out of mind:** In a minority of cases, data controllers' reactions to access requests give the data subject the feeling that they are out of their minds for making such a request.
  - Abuse of democratic rights
  - Nefarious motives
  - Suspicions and passive aggression.

The exception is that, in Germany, exercising this right is seen as normal. They have a form already prepared to access the data.

In 25% of the requests, Prof. Norris and Dr. L'Hoiry ended up filling in a complaint form, it was actually something completely useless.

The results:

- 39 complaints made across the entire study
- 25 complaints resolved (64%)
- 12 complaints outstanding currently (36%)

Policy recommendations

It should not be necessary to motivate requests. There is no legal definition of what is a justifying right and this makes the actual request meaningless. In addition, data controllers must render themselves more visible.

Ms. Antonella Galetta

The presentation focuses on the legal aspects of the right to access to personal data.
The access to personal data is present in primary and secondary law.
Article 8 of the Charter of fundamental rights of the EU provides that:
"Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority."

The IRISS project has pointed out that there is a massive discrepancy between law in theory and law in practice, so how can it be dealt with that discrepancy?

Legal overview

There are variations across the EU: the data retention period differs from one country to another as the time frames given to data controllers to reply to data subject requests are very different from one country to another (*e.g.* Italy: 15 days, Austria: 45 days).
In some countries, a written request is mandatory while, in others, spoken requests are satisfactory. Some ask for motivation and obligation to pay to have access to personal data. This causes a reflection about accessibility and equality.

European case law

The IRISS project has found that the European law does not really understand when data requests are to be considered legitimated or not (*e.g. Leander* v. *Sweden* - ECtHR 1987, *Gaskin* v. *the UK* 1989, *M.G.* v. *the UK* 2002, *Odièvre* v. *France*).

Enforcement of access rights

- Bring access rights violations before DPAs: powers and action of DPAs depend on their independence, neutrality, lack of financial and human resources, etc.
- Bring violations to courts: only a very limited number of cases are brought before courts. It is very unlikely that a complaint is actually admitted.
- Possibility for NGOs to address data subjects but distinctions must be made based on a national level and on the role played by NGOs in national contexts. There are countries where NGOs are very active on data protection issues and some others where the scenario is almost empty.

Data protection reform

According to Ms. Galetta's analysis, the legislator tends now to be more accurate about the definition and procedures to protect personal data. However, some aspects are still not addressed in the reform and still need to be taken into account.

Conclusions

From a European perspective, the access to data is not harmonised. It really depends on national laws. More is going to come. The reform gives the opportunity to NGOs to submit a sort of class action. In the end, we will probably see more in terms of gains in access.

Ms. Claudia Colonnello

Title: "Research of the social costs of surveillance and building a map of the social cost of surveillance"

The general aim of RESPECT's research is to identify and examine every possible harm caused by the use of surveillance systems involved in the implementation of identifying surveillance technologies and providing an empirical basis for the analysis of the social cost of surveillance.

Following are the key points of the social scenario of the genesis of social costs:

- Growth of human subjectivity and its relationship with the use of information communication technologies in today's society.
- Emergence of new social threats related to the use of ITC.
- Surveillance policies: Response necessary for security demands, which tends to produce new dangers that must constantly be investigated.
- Privacy dynamics: The sociological value of privacy structuring human subjectivity in a social context, which makes the results much more complicated.

Individual side identities:

- Identity: Capacity for individuals to control reality online and offline without suffering from discrimination.
- Autonomy: Decision-making power and freedom of action and movement without being constantly monitored.
- Reputation as a way of protecting the social relations of individuals.
- Trust
- Quality of democracy tested in the access to participation.

- Justice could be really damaged by these social relations.

Ms. Colonello concludes with three points she considers important to stress:
- Gap between the declaration of rights and how to exercise them.
- Relationship between our work areas.
- The relevance of the knowledge regime. Actors suffer from a lack of information.

John Mueller
Prof. Mueller makes a reference to the International conference on the ISO 31000 Risk Management Standard about the use of risk analysis.

Prof. Mueller asks what should be taken into account when considering a security measure (focus on terrorism).
- **Benefit** from a security measure:
  - Losses sustained in a successful attack
  - Probability of a successful attack
  - Reduction of the risk due to the security measure: security measures can reduce the losses or tools such as CCTVs reduce the actual risk of an attack.
- **Total benefit** of a security measure: benefit + co benefit
- **Total cost** of a security measure: direct cost + privacy cost

All these variables need to be put together and, if the total benefit still exceeds the total cost, the security measure is cost effective. There are security programmes that are not cost effective even if privacy costs are not taken into account (and this could be the case of the NSA data programme, which had only costs and no benefits). He considers that policy-makers and all competent authorities involved have to figure out a way to reduce security costs.

In considering a break-even analysis, the objective is to set the total cost equal to the total benefit.

Q&A discussion
Question:
1) **Ms. Ilana de Wild**: In terms of the enforceability of rights, how much do you believe that the introduction of a possibility to file a collective complaint, which is a new option, could change the scenario?
One of the few problems people are facing when approaching courts is that judges have not enough knowledge about data access. What kind of recommendation would you make to EU policy-makers?
Ms. De Wild makes a technical remark clarifying that individual rights are NOT citizens' rights because they are not linked to nationality.

Answers:
Ms. Antonella Galetta: There is a new possibility with the regulation package in discussion, but it would be linked to the role played by national NGOs in protecting data. It is very hard to foresee how this possibility will be exercised in the future.

Prof. Clive Norris: The key feature is clear that, in every single country, you can exercise your rights just because you decide to.

Question:
2) **Mr. Jens Kremer:** Do you find any relationship between data responsiveness and DPA capacities?

Answer:
Prof. Clive Norris: If you want national DPAs to respond, they need to have a report written in the national language. The Italian report did not make a good reading for the data protection authorities. So they now want to discuss our results with us.

Question:
3) Member of the audience: Have you sent the report to the DPAs of the country where you conducted the report?

Answer:
Dr. Chiara Fonio: They did, and they received an invitation to Rome to present the findings of the research.

Question:
4) Member of the audience: The balance between risk analysis and cost benefit analysis is very rational. There are some events that are so terrible that they must be prevented even if they are not cost effective. So what would you respond to that argument?

Answer:
Prof. John Mueller: Saving life from terrorism is not an infinite good. There are a lot of ways in which people die. People in charge of public safety should approach it in a responsible way as much as possible and not focus all the investments on non-cost effective measures such as investing extra money on terrorism when there are sectors that are most of the time underestimated by comparison with their importance.

Mr. Sebastian Sperber: Mr. Sperber underlines that when talking about the fact that citizens' calls are not answered, the opposite situation also happens to some services offered by public authorities. There is also a problem relating to citizens who do not exercise their rights. There is also somebody who waits for the phone to ring and this does not happen.

14:00 – 15:30 | **Panel: Citizens attitudes towards surveillance**
Principal speaker: Chiara Fonio – Catholic University of Milan (IRISS)
Panel members: Noellie Brockdorff – University of Malta (RESPECT), Sandra Appleby-Arnold – University of Malta (RESPECT), Elisa Orru – University of Freiburg (SURVEILLE)
Chairperson: Reinhard Kreissl – Institute for the Sociology of Law and Criminology (IRISS)

The IRISS project Working Package 4 (WP4) was devoted to collecting citizens' views on surveillance through both interviews and informed debates on the topic. This presentation focused on the everyday experience of European citizens in five countries: Austria, Germany, Italy, Slovakia and the United Kingdom. Emphasis is given on how they perceive their status of being techno-social hybrids and how technology affects their daily lives when they, e.g. shop, share information on social networks, are "watched" in the workplace or actively engage in security. The core of the analysis is the variety of situations that citizens deal with,

comply with, negotiate with and/or resist, pertaining to the pervasiveness of technology and control.

Prof. Reinhard Kreissl introduces the speakers.

Dr. Chiara Fonio
The IRISS project has adopted a bottom-up approach to understand citizens' attitudes towards surveillance.
The everyday experience of European citizens is to ask how the pervasive use of modern technology shapes their lives and how they perceive their status as being surveyed data subjects. The word surveillance is avoided to understand the point of view of the person being watched.
Individuals were asked what their relationship with technology is without mentioning surveillance. They were encouraged to use an active mode of narration to give them the opportunity to define the concept of surveillance themselves. This qualitative approach led to the possibility to collect a rich range of aspects. Narrative interviews are focused on the reconstruction of experiences.

Methodology:
- 217 interviews: open and elaborate personal interviews from 20 minutes to 1 hour
- Five countries.
- After the interviews, informal debates were held, formed partly by interviewees and partly randomly in order to investigate the reactions before and after having reflected on the issue.

Topic:
- Consumer advocacy
- Crime prevention
- Data protection
- Workplace surveillance
- Random control group: citizens not recruited on the basis of any particular experience (the largest)

The narratives were structured around five dilemmas:
1. Privacy and convenience: Assuming that they have no other choice, they perceive they are surrounded by data collection. There is a sort of readiness to give up privacy, especially in online shops. Online fraud is also perceived as less intrusive than other types of crime.
2. Privacy and security: The idea is that privacy depends on where people are. In public areas, privacy is more and more perceived as lost. The constant regime of visibility is not always welcome and accepted. Many citizens have raised issues of proportionality and effectiveness. Therefore, not everyone simply accept that they are watched in public.
3. Privacy and sociality: The response is a use of privacy tools on social media to protect themselves. There is an introduction of the concept of *security fatigue* connected to the constant and growing effort required to protect privacy.
4. Asymmetry of power and erosion of trust: Introduction of technologies in the workplace. In this context, trust is an issue as a surveillance employer has replaced the supervisor with cameras and microphones, initially to detect thieves. This completely undermines the trust between employers and employees. The notions of

duty and fairness were involved to describe scenarios connected to surveillance technologies.

5. Relationship between citizens and State power: This relationship is asymmetric and frequently mentioned. Surveillance measures are acceptable only up to a certain level.
6. Engagement and security citizens watching citizens: Surveillance carried out by neighbourhood watch is frequently not associated with any consent. The lost of anonymity consists of a huge struggle connected to these practices. When surveillance comes from a neighbour, it is perceived as not accepted if it is not negotiated.

Dr. Fonio concludes in claiming that a very complex picture emerges. The complexity stems from the variety and the ambivalent feelings towards surveillance. There are citizens who fear the destruction of their privacy but, at the same time, they share private thoughts online. The "nothing to hide, nothing to fear" statement is rarely cited. A high level of awareness around surveillance is present, resilience tend to miss. Many citizens underlined personal responsibilities to feel safe in a public environment.

Dr. Noellie Brockdorff and **Dr. Sandra Appleby-Arnold**
Title: "Citizens' attitudes towards surveillance"
In the framework of the REPSECT project, Dr. Brockdorff and Dr. Appleby-Arnold have adopted a quantitative approach with quota samples representing populations in thirteen partner countries.
They have adopted two methods to collect the data:

1. An online survey
2. Face to face questionnaires

The overall sample characteristics are the following: 5.361 respondents, including 49% being female 49% and 51% being male.

For the purpose of their study, five different types of surveillance were taken into account: CCTV, databases, social networking, financial transactions and geo-location surveillance. This choice is based on three specific purposes, being detection of crime, reduction of crime and persecution of crime.

Feelings about surveillance and security: Generally, the presence of surveillance makes people feel insecure. In particular, male respondents are more insecure.

Differences between countries: Austria and Germany are significantly more insecure in the presence of surveillance. By contrast, Malta, Spain and Romania are marginally more secure in the presence of surveillance.

Feelings of security and perceived effectiveness: There is only a medium to weak connection between the perceived effectiveness of surveillance and the perception of security (exceptions: Sweden and the UK). This leads to one conclusion, which is that the efforts to increase effectiveness of surveillance may not make feel citizens more secure.
The question asked is: how happy do you feel about the following types of surveillance? The majority of the population feels unhappy with the different types of surveillance and much more unhappy if they have no awareness of the presence of surveillance (exception for CCTV; but in Austria and Germany, they are unhappy in general also with CCTVs).

Privacy v. security: There is not so much evidence of citizens thinking of a trade-off between

them. A large majority of people would not accept a reward for giving up privacy (the small part who would accept it would prefer CCTV). In Sweden, there is a relationship between feeling secure/insecure and surveillance having a negative impact on privacy.

Awareness: There is actually a rather high awareness of surveillance. There is a large portion of people who do not know what type of surveillance they undergo. There are even two strong opposites: 5% of Romanians think they are under surveillance whereas 95% in the UK think they are. Also, female respondents appear to be substantially less aware about surveillance in their countries.

Acceptance: There is a similar level of acceptance. CCTV was the most accepted; with the highest level in the UK, Malta and Italy. Acceptance depends on the place where surveillance is taking place, with hospitals at the top of the list. There is no relationship between acceptance and perceived effectiveness of surveillance. Therefore, where does this acceptance come from? The relationship found was between acceptance and happiness. This relationship is strong in several countries whereas it does not exist in others.

Dr. Elisa Orru
The SURVEILLE's analysis presents the relationship between surveillance and security as it is perceived by respondents. The SURVEILLE project has actually seen three contexts emerging:

1. Trade in privacy v. security: people consider they exchange privacy for security. People are not willing to give up privacy to gain security.
2. Efforts to feel safer: surveillance threatens security.
3. False sense of security provided by surveillance tools: a trade-off between feeling secure and actual security.

Security and perceptions

- Security dilemma: It emerged from the first two examples. Security measures introduced to increase security result in a perception of insecurity by people due to the association between security measures and threat.
- Perceived security and actual security: To give people the feeling of being safe, it is not only part of people's perceptions but also a part of surveillance effectiveness.

Q&A discussion
Dr. Chiara Fonio responding to Elisa Orru's comments: Dr. Fonio does not think that a qualitative analysis can be compared to a quantitative one. There are some topics that emerge from all the research, such as awareness and trust. Also, the false sense of security is a significant point and requires resources. It is very important from a sociological point of view to focus on citizens' perspectives.

Question:
1) Member of the audience: What is the methodology used for the surveys? How many people were surveyed in each country?

Answer:
Dr. Noellie Brockdorff: A part of the interviews were done online and another face to face in countries with a population of over 2 million, minimum 500 interviews were carried out and countries under 2 million population, 200 interviews.

Question:
2) **Dr. Kristie Ball:** Surprisingly, there was no trust relationship between acceptability and trust. We actually found out the complete opposite so how did you measure trust?

Answer:
Dr. Noellie Brockdorff: We did not measure trustworthiness in the sense of trust in the government. It was about data protection trust.

3) Member of the audience: Could you say a few words about the samples criteria used to collect the surveys? And how did you extract the assumptions from the surveys?

Answer:
Dr. Elisa Orru: The three projects did not want to compare the existing surveys with one another. The objective was to highlight common points emerging from several interviews. Around 65 existing surveys were investigated. Twenty of them were selected on the basis of their relationship with surveillance in public spaces and law enforcement agencies. In addition, these surveys were selected because they used transparent methodologies.

4) Member of the audience: How do you come to the conclusion that people interviewed make a difference between surveillance and security and what do they mean by that?

Answer:
Noellie Brockdorff: The idea comes from the 'Smart project'. People generally do not mind that there is a trade-off between security and privacy.

Comments:
Prof. Charles Raab: There was a project called *Prison* that covered a very large survey (16.000 interviewed). It is worth pointing out that the terms of the question were not about the trade-off but about presenting people with clear scenarios to explain the results clearly.

Ms. Maria Grazia Porcedda: Despite the different methodologies adopted, if the three projects come together with some similar results, we can make a strong case when advocating policy measures.

POLICY BRIEF

15:45 – 17:00 | **Joint Policy Brief**
Principal speakers: Reinhard Kreissl – Institute for the Sociology of Law and Criminology (IRISS), Joe Cannataci – University of Groningen (RESPECT), Martin Scheinin – European University Institute (SURVEILLE)
Panel members: David Wright – Trilateral Research & Consulting (IRISS), Maria Angela Biasotti – National Research Council / ITTIG (RESPECT), Simon Chesterman – National University of Singapore (SURVEILLE)
Chairperson: Bogdan Manolea – ApTI / RESPECT EAG

Mr. Bogdan Manolea introduces the speakers.

Prof. Joe Cannataci
Prof. Cannataci explains that the RESPECT project has tried to set out a scale of actions that

can be taken by the policymakers *(see p. 4 policy brief report)*. What he considers would be interesting is whether the audience and policy-makers agree with RESPECT's suggestions.

Prof. Martin Scheinin

Prof. Scheinin considers that f selected points in the SURVEILLE section need to be presented:

- On recommendation 8: regarding the legislative process, decision-makers have to make sure that there is a proper legal basis for every form of surveillance. And the important lesson from the ECJ rulings and the data retention cases is that if the EU is going to regulate it must be regulating in a complete sense.
- On recommendation 7: privacy by design is important and its conceptual relatives are too. These notions are important because, by including privacy protection features in surveillance technology measures, usability of surveillance (its cost-efficiency) can be increased at the same time and the impact on fundamental rights of these measures can be reduced. Therefore, it would constitute a win–win scenario.
- SURVEILLE assessment of surveillance technologies is based on three dimensions: Technological usability, including effectiveness and cost-efficiency, 2) Identification and assessment of moral risks, and 3) Analysis of the intrusion into fundamental rights. Combining the three assessments enables SURVEILLE to rank surveillance technologies..
- On recommendation 2: A choice must be made to move from mass to targeted surveillance.

Prof. Reinhard Kreissl

Prof. Kreissl explains that, in the policy brief, the IRISS project included some very precise and very clear recommendations. The key questions driving the project were:

- What are the effects of surveillance?
- How can society become more resilient? Two headlines could be used to label the results of the project:
  - The social sorting process is something really important that should be considered also at a policy level.
  - Surveillance is shaping citizens perceptions so how will new social media shape the public's thinking? How can resilience be developed in this context? Unfortunately, citizen's perception on security is always the final point addressed.
- How can citizens be approached and consulted in this sense?

Privacy can no longer be conceived as something detached by social perception.

Dr. Maria Angela Biasotti

Before commenting on the policy brief, Dr. Biasotti makes a preliminary remark in defining legal informatics as a discipline dealing with the application of ICT to a legal scenario. It gives the public access to information. It aims to provide information in advance to render information to the general public not only more accessible but also more understandable.

What is a policy brief? By definition, it is a summary of a particular issue of the policy options that can be given to policymakers to assess and regulate a policy issue.
Keeping this definition in mind, Dr. Biasotti considers that the *DEMOSEC Policy Brief* tries to create awareness on surveillance and on the need to regulate surveillance. Indeed, it attempts to give, on the one hand, awareness of the gaps created by the surveillance and, on the other hand, the potentiality that these technologies could offer. Furthermore, the policy brief also gives a huge amount of information to policymakers. It is a very good starting

point. The content is rich and useful but it is not structured in a way that it could be fully understood by policy makers. She specifies that the three projects have to bear in mind that policy makers do not have an academic background.
Dr. Biasotti invites the coordinators to find a *fil rouge* that can guide policymakers towards the context. Linking one content to another might help to make the situation clear.

Which are the common points and the differences between the three projects? What is the benefit for policymakers to receive all these contents in one policy brief?

Dr. Biasotti is more specific in giving some specific key words that might help:

- For the IRISS project: societal behaviour and resilience
- For the RESPECT project: rules, law enforcement agencies, involvement and technologies
- For the SURVEILLE project: rules, tools, technologies and ethics.

To conclude, Dr. Biasotti thinks that the content of the policy brief needs to be restructured using common frameworks. She makes some suggestions:

- The impact of surveillance on fundamental rights: competent national authorities must communicate to citizens that protecting their data is also protecting their safety.
- Privacy by design.
- Data protection authorities.
- Social and ethical cost of surveillance.
- Need to advise policy makers that surveillance might keep citizens away from certain technologies.
- Thinking about taxation in the use of data by the private sector might be a strong point to improve in this report.

Dr. Biasotti concludes by saying that policymakers are busy people and are not experts. Therefore, a policy brief needs to be attractive, appealing and interesting and, above all, short and easy to read.

Mr. David Wright
Mr. Wright primarily asks what can be done about mass surveillance. Mr. Wright considers that aspects that need to be addressed in connection with mass surveillance could be:

- Mandatory surveillance and impact assessments made public.
- Independent, third party audit.
- Parliamentary oversight committees that are adequately resourced.
- No secret laws.
- Civil society organisations.
- Clear division between mass and targeted surveillance.

<u>Surveillance impact assessment</u> (SIA)

- Need to take into account that it impacts other rights than just privacy: ethical, political, social and economic impacts.
- Need to engage a wider range of stakeholders.
- Need for independent third party review.
- Publish the SIA reports.
- Need to maintain a registry of SIA for organisations.
- Regulator needs to see SIA where there are significant impacts.

Economic value of personal data: Mr. Wright is quite sceptical about assigning a fix value to data. He considers that this value changes depending on circumstances - context-specific. The individual may assign a high or low value depending on many criteria.

Privacy seals: A privacy enhancing technology is a pretty good idea, at least in theory. Article 45 of the proposed directive on data protection refers to privacy seals. It requires further research about what could be done.

Prof. Simon Chesterman
Prof. Chesterman asks three questions:

1. Does an EU policy actually make sense in this area? What is the impact of variations within European countries? There are differences in experiences, histories and cultures that could point to different policies depending on the areas.
2. What is the relationship between targeted and mass surveillance? The suggestion would be for governments to give up mass surveillance but it could be quite tricky because they will probably be reluctant to give up on mass surveillance. And if they refuse, is it less bad to do profiling or mass surveillance?
3. What will change in the next ten years? Which one of your recommendations will actually make a difference?

Discussion
Mr. David Wright: The utility of SIA is really high but this depends on how these tools are structured and used.

Prof. Joe Cannataci: Prof. Cannataci answers Simon Chesterman's questions:

1. A European policy actually makes sense because it keeps the policymaker involved in the issue, continuing to stimulate the debate at a European level.
2. When choosing mass surveillance and targeted surveillance, the most important aspect would be about constant vigilance regarding the impact of the surveillance.
3. The debate started thirty years ago and will increase in the next ten years. Hopefully, there will be a more structured debate than the current one.

Prof. Reinhard Kreissl: Prof. Kreissl also answers Simon Chesterman's questions:

1. A European policy is necessary partly because the EU has a regulatory authority and partly because data does not know any borders. However, it is not enough. A regulation should be promoted at the United Nations level.
2. Mass surveillance goes hand in hand with profiling. If mass surveillance is rejected, profiling will also be. Therefore, can it be suggested to governments that surveillance should be based on information that does not come from mass surveillance but from police investigation? It is a possibility but the adoption of a compromise about these definitions is the better method.
3. (No answer is given to the third question asked).

Prof. Martin Scheinin**:** Prof. Scheinin also answers Simon Chesterman's first question:
Yes, it must be a European approach to define exactly what States need to do.

Prof. Charles Raab: First, Prof. Raab declares to be confused about the policy brief, as he thought this should be addressed to people who work in the EU institutions. However, what seems to have happened in the policy brief is that some issues are addressed to States. Second, he also remarks that it seems to be a mismatch between the work of the IRISS

project and what it is in the policy recommendation, which does not relate in any way to the concept of trust that have been developed in the project.

Dr. Gemma Galdon Clavell: We cannot ask policymakers to become experts. Specific solutions should therefore be provided.

Prof. Joe Cannataci: In the case of RESPECT, there is a tool kit that will give operational information and directions depending on issues. All three projects have three different briefs. What we should focus on is what best suits the persons who receive the brief.

Member of the audience: In talking about impact assessment, we avoid what is an impact and what it is effectively impacting?

Mr. David Wright: Mr Wright says that he used them as a general reference to the impact of surveillance over society.

The European Commission representatives then made several remarks on the policy brief and thanked the three projects for organising this event.

Last question from **Prof. Reinhard Kreissl** to the audience: If you had the choice between taking a very cheap flight ticket but without thorough security measures and a more expensive one with all the security measures applied, which would you buy? Audience members were invited to raise their hands to indicate their preference: most of the audience would take the cheap ticket.

17:00- 17:15 **Closing remark**
The panel thanked the audience for attending and for participating in the joint final event.

ANNEXES

1. Joint Final Event Schedule
Agenda DEMOSEC: **IRISS-RESPECT-SURVEILLE** Joint Final Event
Title: DEMOCRACY and SECURITY

Time	**Day 1: Wednesday 29th October** ***Agenda***
8.30-9.00	Registration
09.00 - 09.15	1.1) Welcome and introduction
09:15 – 09:45	1.2) Presentation of the projects by coordinators
09:45 – 10:45	2.1) Keynote on Surveillance and Democracy
10:45 - 11:15	COFFEE BREAK
	RESPECT PANELS
11:15 – 12:00	3.1) Panel: Surveillance technologies in society
12:00 – 13:00	LUNCH BREAK
13:00 – 14:15	3.2) Panel: Use of Technologies in Society
14:15– 15:15	4.1) Panel: Reconciling human rights protection and security: the roles of European norms and discretion of competent national authorities in using surveillance technologies
15:15 – 15:30	COFFEE BREAK
	SURVEILLE PANELS
15:30 – 16:45	4.2) Panel: Data retention and fundamental rights – the CJEU Judgment of 8 April 2014
16:45 – 18:00	4.3) Panel: Targeted use of surveillance technologies to control individuals considered as dangerous
18:00 - 18:30	Drinks in the lobby
18:30 - 20:30	Conference Dinner at venue

Time	**Day 2: Thursday 30th October** ***Agenda***
8.30-9.00	Registration
09:00 – 10:30	3.3) Panel: The role of Law Enforcement Agencies in Surveillance
10:30 - 10:45	COFFEE BREAK
	IRISS PANELS
10:45 – 12:00	5.1) Panel: Surveillance, Resilience and Democracy
12:00 – 12:45	LUNCH BREAK
12:45 – 14:00	5.2) Panel: The Intersection of Surveillance with citizens' rights
14:00 – 15:30	5.3) Panel: Citizens' attitudes towards surveillance
15:30 - 15:45	COFFEE BREAK
15:45 - 17:00	6.1) Policy Brief
17:00 – 17.15	Closing remarks

Draft Schedule – Joint Final Event
IRISS-RESPECT-SURVEILLE

- Day 1: Wednesday 29th October 2014 -

REGISTRATION
08:30 – 09:00

PART 1 - Welcome and Introduction

1.1) Welcome and Introduction
09:00 – 09:15

Speakers:	Graham Willmott - Head of Unit - Policy and Research in Security
Content:	Welcome and Introduction by the European Commission (EC)
Duration:	15 minutes

1.2) Brief presentation of the projects by the project co-ordinators
09:15 – 09:45

Speakers:	Reinhard Kreissl - IRKS (IRISS) Joe Cannataci - University of Groningen (RESPECT) Martin Scheinin - European University Institute (SURVEILLE)
Duration:	30 minutes

PART 2 – Keynote

2.1) Keynote on Surveillance and Democracy
09:45 – 10:45

Keynote speaker:	Helen Nissenbaum - New York University
Panel members:	Charles Raab - University of Edinburgh (IRISS) Nikolaus Forgo – Leibniz University of Hanover (RESPECT) John Mueller – Ohio State University (SURVEILLE)
Chairperson:	Nikolaus Forgo – Leibniz University of Hanover (RESPECT)
Content:	Keynote lecture and discussion
Duration:	60 minutes

10:45 - 11:15 Coffee Break

PART 3 – Panels on the technological aspects of surveillance

Organised by the RESPECT project with contributions from IRISS and SURVEILLE

3.1) Panel: Surveillance technologies in society
11:15 – 12:00

'Balancing society needs with the use of surveillance technologies'

Principal speaker: Tony Porter - Surveillance Camera Commissioner UK

Panel members: Michelle Cayford – Technical University Delft (SURVEILLE)
William Webster - University of Stirling (IRISS)

Chairperson: Caroline Goemans-Dorny – INTERPOL (RESPECT)

Duration: 45 minutes

12:00 – 13:00 LUNCH BREAK

3.2) Panel: Use of Technologies in Society (Social Media and CCTV)
13:00 – 14:15

'Security and surveillance practices are informed by a range of technologies, many of which are currently trialled and used by law enforcement, security and intelligence agencies on a global scale. These technologies, including closed-circuit television networks (CCTV) and social network monitoring and analysis systems (SNMAS) are developed in both the private and public sectors. This panel will highlight key findings from the RESPECT project that consider the uptake and integration of these technologies, in particular relating to cost versus convenience, proportionality issues and privacy and the data protection impact assessment.

Principal speakers: Daniel Trottier – University of Westminster (RESPECT) and Caroline Goemans-Dorny - INTERPOL (RESPECT)

Panel members: Mathias Vermeulen – Free University of Brussels (SURVEILLE)
Richard Jones - University of Edinburgh (IRISS)

Chairperson: Simon Dobrišek - University of Ljubljana (RESPECT)

Duration: 75 minutes

PART 4 – Panels on the legal aspects of SURVEILLANCE

Organised by the SURVEILLE project with contributions from RESPECT and IRISS

4.1) Panel: Reconciling human rights protection and security: the roles of European norms and discretion of competent national authorities in using surveillance technologies
14:15 – 15:15

In the European Union, human rights are protected at both the national and European level. While the use of surveillance technologies for security purposes engages both, European norms and national legal frameworks may conflict. Such contrasts remain topical and are of interest in the development of surveillance technologies. Indeed, European institutions have an increasing focus on the potential harmonisation of the use of surveillance technologies. Thus, it is important to achieve clarity as to the application of protective mechanisms vis-à-vis fundamental rights. In this context, we consider whether Member States retain a margin of appreciation. Furthermore, to what extent should the European Union further legislate on this matter?

Principal speaker: Hielke Hijmans - VUB- University of Amsterdam

Panel members: Ivan Szekely – EKINT Budapest (IRISS)
Jeanne Mifsud Bonnici - University of Groningen (RESPECT)
Christiane Höhn - Adviser to the EU Counter Terrorism coordinator

Chairperson: Francesca Galli - University of Maastricht - IEE/ULB (SURVEILLE)

Duration: 60 minutes

15:15 - 15:30 Coffee Break

4.2) Panel: Data retention and fundamental rights: the CJEU Judgment of 8 April 2014
15:30 – 16:45

The Data Retention Directive aimed to harmonise Member States' provisions concerning the retention of certain data generated or processed by providers of publicly available electronic communications services or of public communications networks. In April the Court, declaring the Directive invalid, took the view that by requiring the retention of data and by allowing the competent national authorities to access it, the Directive breaches the fundamental rights to the respect for private life and to the protection of personal data. We consider in this panel the implications of the decision, taking into consideration that Member States adopted legislation to ensure compliance with the Directive. Discussion shall further debate how issues raised by the ruling will be resolved by European institutions and Member States.

Principal speaker: Paul Nemitz - Director Fundamental and Union Citizenship - EC

Panel members: Paul de Hert – Vrije Universiteit Brussel(IRISS)

Erich Schweighofer - University of Vienna (RESPECT)
Walter Coenraets (Director Federal Cybercrime Unit, Belgian Federal Police)*TBC
Tuomas Ojanen - University of Helsinki (SURVEILLE)

Chairperson: Martin Scheinin – European University Institute (SURVEILLE)

Duration: 75 minutes

4.3) Panel: Targeted use of surveillance technologies to control individuals considered as dangerous
16:45 – 18:00

Surveillance technologies have long been developed to prevent and investigate offences. Dealing with terrorism and organised crime, States have extended this use for security purposes more generally. Suspicion may be a pretext for conducting targeted surveillance of specific individuals or groups. In this respect, monitoring may involve a plethora of different technologies. With respect to criminal justice procedure, distinct issues arise that will be addressed in this panel. For example, competent national authorities are using information gathered more generally against suspects and potentially infringing their rights (gathering information may interfere with the right to data protection): practices may challenge the presumption of innocence, which is said to have been increasingly replaced by a presumption of guilt. Furthermore, administrative measures in the spheres of immigration and post-detention monitoring are increasingly implemented using surveillance capabilities due to the risk an individual is believed to represent. What is the legal basis for such activities? Are such measures as implemented in compliance with human rights standards?

Principal speaker: Michele Panzavolta - University of KU Leuven

Panel members: Nils Zurawski - University of Hamburg (IRISS)
John Guelke - University of Warwick (SURVEILLE)
Antonis Samouris - Counterterrorism specialist – future Europol Counterterrorism specialist
Ilana de Wild (National Police of The Netherlands/INTERPOL – Human Trafficking and Child Exploitation team)

Chairperson: David Wright - Trilateral Research & Consulting (IRISS)

Duration: 75 minutes

18:00 – 18:30 Drinks

18:30 – 20:30 Conference Dinner at the Venue

- Day 2: Thursday, 30th of October 2014 -

REGISTRATION
08:30 – 09:00

3.3) Panel: The role of Law Enforcement Agencies in Surveillance
9:00 – 10:30

'Criminal trends have rapidly evolved in the last twenty years mainly due to the fact that criminal innovation pools its resources directly from society and is able to flexibly adapt to technological changes with few legal restrictions. Moreover, new technologies enable and facilitate the perpetration of criminal acts and, as a consequence, law enforcement agencies need to step up the level of appropriate tools to combat those crimes with a view to protecting the security of citizens. This panel will discuss challenges that law enforcement agencies are currently facing'.

Principal speaker:	Christian Karam - INTERPOL – Digital Crime Officer
Panel members:	Brian McNeill – Merseyside Police (SURVEILLE)* Gemma Galdon Clavell - University of Barcelona (IRISS/RESPECT) Ilana de Wild - National Police of The Netherlands /INTERPOL – Human Trafficking and Child Exploitation team
Chairperson:	Edward Beaman- University of Central Lancashire (RESPECT)
Duration:	90 minutes

10:30 - 10:45 Coffee Break

PART 5 – Panels on the social implications of surveillance

Organised by the IRISS project with contributions from RESPECT and SURVEILLE

5.1) Panel: Surveillance, Resilience and Democracy
10:45 – 12:00

This talk examines the troublesome relationship between surveillance and democracy in Europe. Through a detailed empirical examination of three surveillance practices across Europe – ANPR, Credit Scoring and Neighbourhood Watch - it highlights, explores and theorises this relationship. The talk's basic theoretical premise is that, while surveillance practices can be deployed to counter threats and risks and to prevent harm occurring, they also create potentially harmful consequences. The reliance of surveillance practices on proprietary information infrastructures can make surveillance processes non-transparent and unaccountable to democratic scrutiny in cases where harm occurs. It is argued that the traditional venues of democracy, where citizens and institutions engage, participate in debate and create governance structures, cannot be mobilised without widespread awareness of the harms and consequences of surveillance practices by both citizens and institutions. This awareness is lacking in most cases. The talk also reveals the deep historical, social, political and legal antecedents of the current state of affairs.

Principal speaker: Kirstie Ball - Open University (IRISS)

Panel members: Simon Chesterman - National University of Singapore (SURVEILLE)
Roger Clarke (IRISS Advisory Board)
Christian Hawellek - Leibniz University of Hanover (RESPECT)

Chairperson: Roger Clarke (IRISS Advisory Board)

Duration: 75 minutes

12:00 – 13:00 Lunch break

5.2) Panel: The Intersection of Surveillance with Citizen's Rights
12:45 – 14:00

In the context of surveillance and democracy, the principles of consent, subject access and accountability are at the heart of the relationship between the citizen and the information gatherers. The individual data subject has the right to at least know what data is being collected about them and by whom, how it is being processed and to whom it is disclosed. Furthermore, they have rights to inspect the data, to ensure that it is accurate and to complain if they so wish to an independent supervisory authority who can investigate on their behalf.
This panel will present the results of our multi-partner project on surveillance and democracy as part of the IRISS project. In particular, we have focused on the ability of citizens to exercise their democratic right of access to their personal data. Together with ten partner institutions, we conceptualised a research approach involving auto-ethnographic methods which sought to 'test' how easy or difficult it is for citizens to access their personal data by submitting subject access requests to a range of local, national and supranational institutions across both public and private sectors. We will present the overall findings of the ten-country study and consider the strategies used by those who hold our personal data to facilitate or deny us access to what they know about us and how they process it.

Principal speakers: Clive Norris – University of Sheffield (IRISS) and Xavier L'Hoiry – University of Sheffield (IRISS)

Panel members: Antonella Galetta – Vrije Universiteit Brussel (IRISS)
Claudia Colonnello – Laboratory of Citizenship Sciences (RESPECT)
John Mueller - Ohio State University

Chairperson: Ivan Szekely - EKINT Budapest (IRISS)

Duration: 75 minutes

5.3) Panel: Citizens attitudes towards surveillance
14:00 – 15:30

The IRISS project Working Package 4 (WP4) was devoted to collecting citizens' views on surveillance through both interviews and informed debates on the topic. This presentation focuses on the everyday experience of European citizens in five countries: Austria, Germany, Italy, Slovakia and the United Kingdom. Emphasis was placed on how they perceive their status of being techno-social hybrids and how technology affects their daily lives when they, e.g. shop, share information on social networks, are "watched" in the workplace or actively engage in security. The core of the analysis is the variety of situations that citizens deal with, comply with, negotiate with and/or resist, pertaining to the pervasiveness of technology and control.

Principal speaker:	Chiara Fonio - Catholic University of Milan (IRISS)
Panel members:	Noellie Brockdorff and Sandra Appleby-Arnold – University of Malta (RESPECT) Elisa Orru – University of Freiburg (SURVEILLE)
Chairperson:	Reinhard Kreissl
Duration:	90 minutes

15:30 – 15:45 COFFEE BREAK

PART 6 –Policy Brief

6.1) Policy Brief
15:45– 17:00

Principal speakers:	Reinhard Kreissl (IRISS), Joe Cannataci (RESPECT), Martin Scheinin (SURVEILLE)
Panel members:	David Wright – Trilateral Research & Consulting (IRISS) Maria Angela Biasiotti – National Research Council (CNR) - ITTIG (RESPECT) Simon Chesterman – National University of Singapore (SURVEILLE)
Chairperson:	Bogdan Manolea (ApTI/RESPECT EAG)
Content:	Presentation of the Joint Policy Brief and open discussion
Duration:	30 minutes for the Joint Policy Brief and 30 minute discussion

6.2) Closing Remarks
17.00-17.15

2: List of SURVEILLE attendees:

NAME	AFFILIATION
Martin Scheinin	European University Institute
Jonathan Andrew	European University Institute
Maria Grazia Porcedda	European University Institute
Mathias Vermeulen	Vrije Universiteit Brussel
Tom Sorell	University of Warwick
John Guelke	University of Warwick
Chris Nathan	University of Warwick
Heather Draper	University of Birmingham
Gregory Moorlock	University of Birmingham
Mikael Johansson	Lund University
Karol Nowak	Lund University
Elisa Orru	University of Freiburg
Gian Guido Nobili	EFUS
Sebastian Sperber	EFUS
Eck Ralf	Fraunhofer IOSB
Erik Krempel	Fraunhofer IOSB
Michelle Cayford	TU Delft
Claudia De Concini	European University Institute
Brian McNeill	Merseyside Police
Margaret Gorman	Merseyside Police
Claudia Diaz	University of KU Leuven
Simon Chesterman	National University of Singapore
John Mueller	Ohio State University
Michele Panzavolta	University of KU Leuven
Antonis Samouris	Counter Terrorism Specialist - future Europol Counter Terrorism Specialist

NAME	AFFILIATION
Tuomas Ojanen	University of Helsinki
Céline Cocq	Université Libre de Bruxelles
Francesca Galli	Université Libre de Bruxelles
Paul Nemitz	European Commission
Christiane Höhn	Council of the European Union
Jens Kremer	University of Helsinki
Anne Weyembergh	Université Libre de Bruxelles
Yasuo Kasuto	Canon Research Centre France SAS
Raminta Sulskute	Human Rights Monitoring Institute
Federico Fabbrini	University of Tilburg
Brooks Tigner	Security Europe
Teri Schultz	Security Europe
Chris Dalby	Security Europe
Emile Dejehansart	Comité P - Belgium
Nicolas Dubois	European Commission
Gerburg Larsen	European Commission
Michael Vanfletere	European Commission
Katrin Huber	European Parliament
Annieke Logtenberg	European Commission
Graham Willmott	European Commission
Antoine Cahen	European Commission
Clodagh Quain	EU Institute for Security Studies
Gordon Lennox	former EU Commissioner
Niklas Creemers	Center for Technology and Society
Oronzo Daloiso	Paragon Europe
Maurits Martijn	journalist - De Correspondent

NAME	AFFILIATION
Vivian Linssen	European Commission
Anita Nappo	EU-logos Athena organisation
Marie Anne Guibbert	EU-logos Athena organisation
Ana Daniela Sanda	EU-logos Athena organisation
Valeria Serra	Edisfera
Diego Naranjo	European Digital Rights
Claudia Scharl	Bavarian Research Alliance GmbH
Fabio Feudo	Laboratorio di Scienze della Cittadinanza
Peter Ide Kostic	European Parliament STOA