Project acronym:	SAPIENT
Project title:	Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies
Project number:	261698
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2010.6.5-2: Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules
Contract type:	Collaborative project
Start date of project:	1 February 2011
Duration:	42 months

Deliverable 5.2: Privacy in Times of Smart Surveillance Proceedings of the SAPIENT final conference, 1-2 July 2014

Rapporteurs:	Nicholas Hernanz (CEPS); Dara Hallinan, Michael Friedewald (Fraunhofer ISI)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due dates:	30 July 2014
Submission date:	10 September 2014

About the SAPIENT project

The SAPIENT project that is expected to provide strategic knowledge on the state of the art of surveillance studies, emerging smart surveillance technologies, and the adequacy of the existing legal framework. In addition to addressing these core research goals, the project will entail the development and validation of scenarios around future smart surveillance systems, and will apply the best elements of existing PIA (privacy impact assessment) methodologies to construct a surveillance related PIA framework.

The work of the project will lead to a practical handbook which will help policy makers, technology developers and other stakeholders to better understand how and when smart surveillance should be used, and apply criteria to assure that such systems respect the privacy of citizens.

Terms of use

Document history

Version	Date	Changes
0.9	08 September 2014	Draft version
1.0	10 September 2014	

Introduction

After 3 years of research on the topics of surveillance technologies, the SAPIENT project came to an end in 2014 and presented its final results during a 2-day Final Conference on 1 and 2 July 2014. This Final Conference, entitled "Privacy in Times of Smart Surveillance", presented the main findings of the SAPIENT project which dealt with the security/rights conundrum, especially in the context of new technologies of surveillance, and bridged the gap between academics and policy-makers on these issues.

The Final Conference was organised as follows: first, a Policy Meeting kicked off the event with relevant policy-makers and stakeholders debating on the new policy agenda on privacy and surveillance at EU level. After the Policy Meeting, the First Panel of the conference presented the findings of the SAPIENT research on EU policies carried out during the last three years on EU security policies, such as Data Retention, Smart Borders and other large-scale information systems including Passenger Name Records. The Second Panel of the conference highlighted the main results of the research on impact assessments' methodologies and guidelines as a tool for a better data protection in the EU.

SAPIENT stands for Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies and is a collaborative research project on the state of the art of surveillance studies, emerging smart surveillance technologies, and the adequacy of the existing legal framework that relates to these technologies. This project is co-funded by the European Commission under the 7th Framework Programme (FP7).

For more information, please visit SAPIENT's website: www.sapientproject.eu

Day 1 – Policy Meeting

Sergio Carrera (CEPS) and **Michael Friedewald** (Fraunhofer) opened the policy meeting by presenting the last stages of the SAPIENT research project and the general policy context of data protection policies at EU level. The first day of the conference, 1 July 2014, coincided with the first day of the Italian Presidency of the Council of the EU. A few days prior, the European Council, in its Conclusions of 26/27 June, defined the strategic guidelines for legislative and operational planning for the coming years within the area of freedom, security and justice.[1] Carrera underlined that it was therefore of key relevance to have the first keynote speech by Luca de Matteis, a representative of the Italian Permanent Representation of Italy to the EU, on the topic of the priorities of the Italian Presidency in the field of data protection.

Luca de Matteis (Permanent Representation of Italy to the EU) started his keynote speech by underlining that the conclusion of the SAPIENT project touched upon fundamental issues for data protection policies in the EU. He presented the Italian Presidency's main data protection priorities for the next six months:

1) The Data Protection package, proposed by the European Commission in January 2012, is still under negotiation between the European Parliament and Member States. The Data Protection regulation has witnessed a difficulty to find compromises between certain member states, but the Italian Presidency will try to move towards a compromise text that will be accepted by all 28 member states. Sensitive chapters such as the one on sanctions, on the one-stop-shop, and the right to be forgotten (following the Google case of the Court of Justice of the EU) are still under discussion. The Data Protection directive on law enforcement is also still under

[1] http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/ec/143478.pdf

negotiation but discussions are linked to further developments in the Data Protection regulation.

2) Ensuring the coherence and Data Protection issues across the action of EU institutions and agencies was the second priority highlighted by De Matteis. This includes data protection matters linked to the Europol regulation as well as Eurojust and the European Public Prosecutor.

3) Transatlantic relations are also high on the Italian Presidency's agenda, especially in the aftermath of the Snowden revelations. This topic includes the umbrella agreements, such as the general agreement on data exchange in the field of judicial and law enforcement cooperation between the EU and the United States. The European Commission is negotiating this general agreement which takes time and which requires a cultural step forward by the US government. The revision of Safe Harbour scheme, which is a mechanism allowing data on EU citizens to be transferred to US companies who commit themselves to abide by a set of data protection rules, is also an important topic. The need to revise the scheme was born from the Snowden affair. 13 recommendations were made by the European Commission to the US government in November 2013 to amend the Safe Harbour use by US companies, but it is yet to be confirmed if and how they will conform to these recommendations.

4) Data Retention, and the consequences of the judgment of the Court of Justice of the EU which annulled the 2006 Data Retention directive, was the last priority identified by De Matteis. The question of data retention for law enforcement purposes was at the centre stage of the debates following Sweden and Austria's decision not to retain data on citizens anymore. De Matteis highlighted that a fragmentation of the continental approach to data retention could be dangerous due to the disappearance of a fundamental tool against serious and organised crime. He also underlined that the consequences on other policies, such as PNR and TFTP, still remain to be clarified.

Lord John Sharkey (House of Lords, UK) started his presentation by highlighting the role of the EU Sub Committee F - Home Affairs, Health and Education of the House of Lords in the enhanced scrutiny on the Safe Harbour agreement that was conducted in 2014. The Sub-Committee focused its attention on the agreement itself as well as the European Commission's proposal as regards its revision. He provided a short summary of the Safe Harbour agreement, which was signed in July 2000 and allows free transfer of personal information from EU member states to US companies which have signed up to the safe harbour principles, in circumstances where otherwise the data transfer would not be possible due to non-respect of EU data protection rules. The fundamental principles of the safe harbor agreement are transparency of the adhering companies to privacy policies, incorporation of safe harbour principles by companies and enforcement, including by public authorities. The enhanced scrutiny by the House of Lords called on witnesses, among them Mr Connolly and Mr Nemitz who were also speakers of this SAPIENT conference. The scrutiny was concluded in April 2014. The main findings of the scrutiny were the following:

- There exists only limited awareness of safe harbour among EU citizens, and there is a need to do more. National data protection authorities should be more involved to create more awareness among the public. A good example is the US Department of Commerce's website, which offers better explanations and a list of certified companies. Privacy policies should be made more intelligible to lay readers and written in clear language.
- Redress mechanisms surrounding the safe harbor agreement should be improved. Only 7 complaints on the agreement have been received by the EU panel on safe harbour. The US Federal Trade Commission (FTC) has succeeded in reducing to 2 the

number of alternative dispute resolution mechanisms that charge fees, but Lord Sharkey insisted on the need to end fees for all such mechanisms. EU citizens should be able to issue class actions in the US against safe harbour violations. Also, false claims constitute a growing problem: 427 false claims of safe harbour violations (one in seven) have been recorded, which Lord Sharkey presented as unacceptable. The FTC brought claims against 10 companies between 2009 and 2013, and against 14 in 2014 only, which shows an improvement but remains hardly proportionate to the problem. Investigating false harbor claims should be priority, and checks and audits should not be triggered only by false claims. Lord Sharkey deplored the absence of a European Commission evaluation report in recent years – he insisted that a regular evaluation of safe harbour agreement should be done, similar to PNR and TFTP.

- Data access by US authorities was also a main concern, especially for the European Commission and the European Parliament following the Snowden revelations. Safeguards available to US citizens should be also extended to EU citizens who are not resident of the United States. Lord Sharkey insisted however on the fact that the UK government considered that it was not appropriate for the EU to engage in debates with the US over national security issues due to national security being outside of the competences of the EU. However, it would be in the UK interest to conduct a dialogue on these issues with the European Parliament and EU member states to ensure that the UK position is understood.
- On the question of the suspension of the Safe Harbour agreement, Lord Sharkey stated that the agreement should not be suspended. The House of Lords scrutiny identified obvious weaknesses, but found that there were proposals to address these weaknesses. Lord Sharkey concluded by saying that the possibility of suspension should be kept open for the future.

Chris Connolly (Galexia) started his presentation, entitled "A Brief History of Reform and Enforcement of the Safe Harbor", by presenting a timeline of the safe harbor agreement, from its launch in 2000 to the recent actions against 14 false claimants. Galexia, an international consulting firm, has conducted a review on the Safe Harbour agreement in 2008[2] and provided evidence to the European Parliament LIBE Inquiry on Electronic Mass Surveillance of EU Citizens in October 2013. Persistent issues with safe harbor identified by Connolly were false claims (by former members), false trustmarks, no information on dispute resolution and a highly unaffordable dispute resolution. Against false claims, three series of cases were launched by the US Federal Trade Commission (FTC):

- In 2009, the FTC prosecuted 6 organisations for false claims. Connolly viewed this prosecution effort as encouraging, but remarked that it had a limited impact due to the small size of the organisations concerned, the absence of trustmarks involved as well as the absence of sanctions, and the fact that the six companies simply left the Safe Harbour agreement after prosecution.
- In 2011 and 2012, Facebook, Google and MySpace were found to have misled consumers about their privacy practices, and paid fines (but MySpace left the Safe Harbor immediately). According to Connolly, this had a positive impact on Safe Harbour compliance.
- In 2014, the FTC launched actions against 14 companies for false claims (all former members), varying from 6 months to 8 years. In comparison to the 2009 and 2011-12 cases, the 2014 actions concerned larger companies with some trustmarks involved, and about half of these companies stayed in the Safe Harbour. However, no sanctions were implemented.

[2] Connolly C (2008) The US Safe Harbor - Fact or Fiction?, Galexia, December 2008, http://www.galexia.com/public/research/articles/research_articles-pa08.html

Connolly presented the main differences between the US FTC Consent Orders and the existing Safe Harbour requirements, among them the fact that the FTC Consent Orders require an independent privacy compliance assessment every two years while the Safe Harbour requires an annual privacy compliance report.

In November 2013, the European Commission made13 recommendations for improvements in the context of the Snowden revelations, with an emphasis on tightening the national security exemption and making alternative dispute resolution mechanisms more affordable. An agreement appeared to have been reached on all 13 recommendations in June 2014. Connolly considered this as a major milestone in the history of the Safe Harbor, as all prior efforts at reform had failed.

Outstanding issues with the Safe Harbour agreement include:

- The fact that many Safe Harbor privacy policies still threaten complainants with costs;
- False claims by non members (fraud) are still not acknowledged or addressed;
- Safe Harbor trustmarks have completely escaped enforcement or reform, but have major problems with accuracy and integrity;
- Safe Harbor has been used as a "shield" in some high profile cases – never intended to extinguish EU fundamental rights

Daniel Drewer (Europol) presented the work of the Data Protection Office at Europol, the European Police Office which has its headquarters in the Hague, Netherlands. Drewer underlined the fact that being far away from Brussels meant that Europol was sometimes missing certain details on the Brussels debates as regards data protection issues. Europol hosts top specialists in combating serious crime and terrorism, with over 100 criminal analysts and a network of liaison officers. The information stored in Europol's data centre is composed of the Europol Information System (EIS), the Analysis Work Files (AWF) and the Secure Information Exchange Network Application (SIENA), which hold data on items and persons (suspects, witnesses or victims). Personal data is currently processed in the EIS and the AWF. Europol respects a specific set of data protection rules such as the EU Charter of Fundamental Rights (Art 8), the Europol Council Decision, Regulation (EC) 45/2001 as well as the Council of Europe Convention 108 from 1981. According to Drewer, Europol applies the following fundamental principles as regards the protection of personal data, which ensure quality and proportionality of the data processing:

- Data processing must be based on a legitimate basis laid down by law (Europol Council Decision).
- Data must be processed fairly for specified purposes.
- Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- An independent authority shall control the compliance to these principles (Joint Supervisory Body (art. 34 ECD))

Europol applies very strict time limits - all personal data must be reviewed at the latest after three years. Access to AWF is restricted to participating member states only. Sensitive data, such as political opinions, can only be processed in certain AWFs and only under very strict conditions which have to be agreed with the Supervisory authority prior to the start of the processing. Drewer highlighted the importance of having a tailor-made regime for data processing in the field of law enforcement. He reminded participants about the 1987 Council of Europe Recommendations on the use of personal data in the police sector as well as the Krakow Declaration of 2005 which says that there is the need to adapt general principles in order to meet the specific requirements of the police sector. Drewer finished his presentation by highlighting the future challenges, among them the new legal framework for Europol and

Eurojust and the mandate of the EU Court of Justice as of 1 December 2014, which will have a direct jurisdiction over Europol, as foreseen in the Lisbon Treaty.

Katarzyna Szymielewicz (Panoptykon) started her presentation by highlighting the work of the Panoptykon foundation in Poland, which she co-founded and currently presides. Panoptykon works on European issues related to privacy and data protection, with a basic philosophy rejecting the differentiation between terrorists and law-abiding citizens in the current debates, as she believes fundamental rights should apply to everybody. The themes touched upon by the Panoptykon foundation, and by its partner EDRi, are the Data Protection package, the Passenger Name Records, Smart Borders and other data exchange schemes.

Szymielewicz highlighted her main concerns regarding the state of play of the Data Protection package. According to her, unclear legislative provisions and a general fatigue among negotiators were part of the problem. She insisted on the need to put pressure on the Council to make sure that the current standards of data protection are not diluted. The European Parliament's position should be taken as the minimum standards to achieve.

Szymielewicz presented what, according to her, should be the 6 red lines during the negotiations:

1) The regulation should make clear that companies in the United States should respect the same standards of data protection;
2) Profiling should not be allowed in the regulation – while it can be useful to prevent crime, it is morally unacceptable to judge innocent citizens before they take action;
3) Definitions should be given more weight: what is personal data? What types of identifiers exist? Is pseudonymous data an acceptable alternative?
4) Data transfers: the general consensus reached by Council on Chapter 5 is not acceptable. Codes of conduct or certification mechanisms are new concepts that have been introduced, but challenges may rise if they are not accepted by Data Protection Authorities;
5) Safe Harbour: the agreement cannot be justified in any way;
6) Access to data by foreign authorities (following the NSA scandal and the Snowden affair): Szymielewicz called for the reintroduction of the extra paragraph 42 introduced in the European Parliament's draft article 43a, saying that companies should be prohibited from transferring data abroad unless there is an international agreement with certain standards.

Finally, Szymielewicz warned that the negotiations on the Transatlantic Trade and Investment Partnership (TTIP) should take place in parallel to the negotiations on the Data Protection package. The major challenge lies in the Investor State Dispute Settlement (ISDS) mechanism that would allow companies to sue governments in the future if they introduce stronger legal protection for citizens because it will be perceived as a trade or investment barrier. Delaying the introduction of the new data protection framework would mean that it would be subject to the ISDS mechanism.

Day 1 – Panel 1

Sergio Carrera (CEPS) presented the recent research of CEPS on the data retention challenge in the EU in light of the *Digital Rights Ireland* landmark judgment of the Court of Justice of the European Union (CJEU) on 8 April 2014, which found the Data Retention Directive to be invalid. Carrera first presented the scope and nature of the Data Retention Directive, adopted in 2006. The directive requires service providers to retain details of all telephone, mobile, and internet communications for periods of between no less than six

months and no more than two years from the date of the communication. It involves the collection of bulk metadata – everyone's data is collected without the requirement of any suspicion or the intercession of a judge. The retention itself (storage) is left to individuals and organisations in the private sector. Carrera then went on to explain why the CJEU did find the Data Retention Directive invalid. The issue became one about the role of fundamental rights in the EU legal order – the legally binding nature of the EU Charter of Fundamental Rights – and the consistency of metadata retention for law enforcement purposes with EU citizens' right to respect for privacy (Article 7 EU Charter) and to data protection (Article 8 EU Charter). The reasoning of the Court was as follows: first, the Court confirmed that the amount and precision of the data covered by the Data Retention Directive allowed very precise conclusions to be drawn concerning people's private lives. This was in conflict with the right to respect for private life. Second, any interference with this right needed to be justified through a legality test, answering the following questions: are there adequate grounds/necessity for the interference? And is the justification proportionate? Third, the Court laid down standards to assess the legality test of the Data Retention directive and how it would need to be changed to comply with the right to respect for privacy. Among others, clear and precise rules governing its scope and application, minimum safeguards to protect personal data against abuse, limits on the personal data collected and who can have access to that data, etc. Carrera presented the reactions to the *Digital Rights Ireland* judgment of the Court: the European Parliament issued several parliamentary questions to the Commission and discussed the judgment in its final plenary session on 16 April 2014. Commissioner Malmström advised the EP that the reflection on the need for a new legislative proposal was ongoing but that the decision would be taken by the next Commission. According to Carrera, the implications of the judgment were much wider than the directive and affected other key EU legal instruments and policy tools engaged in mass data collection/processing, such as the Passenger Name Record Agreement (PNR), the Terrorist Finance Tracking Programme (TFTP) and the EU PNR Directive which is still in the legislative process. The implications of the judgment on the Safe Harbor scheme were also still unclear. A confidential opinion issued by the Council Legal Service on 5 May 2014 on the judgment invalidating the Directive confirmed that existing EU measures and proposals which provide for mass data collection, storage of the data of a very large number of unsuspected persons do not stand a serious chance of passing the legality test. Carrera concluded by raising the issues of what the EU should do. His suggestions included

- a full and independent re-assessment of the need for a Data Retention Directive
- a proven justification by Member States that retaining metadata for law enforcement purposes actually helps to address and solve serious crimes
- further discussion is needed on a European 'privacy cloud' where the data of EU residents are stored so that EU data protection supervisors can ensure that they will be treated in accordance with European standards and legal principles
- a careful and thorough independent evaluation of the PNR and TFTP agreements as well as the Safe Harbor scheme with the US is needed in light of the legal standards established by the CJEU

Joanna Parkin (BEPA) presented the Opinion of the European Group on Ethics, part of the Bureau of European Policy Advisors, on the Ethics of Security and Surveillance Technologies. The European Group on Ethics, a multi-disciplinary group composed of 15 experts, provides independent advice to the European Commission on ethical aspects of science and technologies since 1991. The Group published its Opinion 28 in June 2014 in the context of the digital revolution and rapid expansion of surveillance, especially following the 2013 surveillance disclosures which emphasised that there is a serious ethical crisis with severe political repercussions. There is a need for the EU to make clear where it stands ethically speaking. The Opinion is divided in four chapters:

- **Technological trends**: trends such as miniaturisation, automation, or ubiquity show us that there seems to be a technology lock-in – 'no going back'. Technology is perceived as a 'universal security enabler' but also presents limits.
- **Governance challenges**: challenges include outdated regulatory frameworks (e.g. telecommunications, CCTV) and fragmented global regulatory landscapes. The national security exemption lacks clear articulation.
- **Ethical considerations**: the core ethical principles that underpin the EGE's recommendations are privacy and freedom, autonomy and responsibility, and justice. Its procedural principles are accountability and transparency as well as efficacy and proportionality.
- **Policy recommendations**: the Opinion suggests policy recommendations as regards accountability and oversight mechanisms (a system of judicial oversight for surveillance for criminal investigations, adequate powers and resources for oversight authorities or comprehensive whistleblower protection mechanisms), data protection and privacy (EU code of conduct for big data analytics, a constant evaluation of underlying algorithms and their parameters, and vesting data protection authorities with sufficient legal powers and resources) and design and development (establishing necessity and value added of security technologies, such as new border surveillance systems, as well as devise privacy impact assessment procedures).

Els de Busser (Max Planck Institute) started her presentation by pointing out a research conducted by the Max Planck Institute and published in 2012 on Data Retention. This research was based on statistics and interviews with police authorities, prosecutors and judges at federal and state level in Germany. The main conclusion of this study was that the storage of data does not raise clearance rates for serious crimes.

From her personal point of view, she considered important that in the discussions on data retention for criminal investigations one has to be very careful when making the distinction between blanket retention and specific requests. Another point was not to overrate the value of retained data as the only form of evidence. In this regard, she highlighted that no prosecutor would start a prosecution based only on one type of evidence.

Furthermore, she continued her presentation by focusing on two recent rulings from the Court of Justice. The first ruling was the *Digital Rights Ireland* judgment, previously explained by Dr. Carrera. In this regard, de Busser considered that the decision by the Court was certainly not on data retention as such (as a tool) either on the use of personal data for the purposes of criminal investigations. According to her, this was a decision on blanket data retention as described in the Directive of 2006 or on a lack of description. It was a decision on the proportionality concept and what is strictly necessary. In the PNR and TFTP discussions it has been proved the difficulty to describe such concepts. From de Busser's point of view, this decision was a miss opportunity for the Court to give few indications on how to deal which such difficult concepts such as necessity and proportionality.

Looking at a bigger picture, de Busser explained that when seeing the recent developments in the EU, how Member States are dealing with cooperation in criminal matters and exchange of information, and how Member States are implementing EU legal instruments, she could see a general trend on the lack of trust. She brought these points up as she considered that everyone was looking at the Court of Justice for guidance and finally the Court did not provided it.

The second ruling she mentioned was the Judgment on *Google* and the right to be forgotten (which according to her it should be reframed for the right to be erased). In line with the previous judgment, she thought that Google should not have been the target. This ruling was about somebody's information which was available online for a longer time while Google is just a channel that brings the information available in a link. Thus, the real issue was the

fact that national legal rules are not providing a maximum time period for which the information could be posted. For this reason, de Busser considered that the Court should again have gone a bit further and focused more on the national legal rules.

Going back to the general theme of the Conference, de Busser concluded by saying that one has to be careful to don't expand to a right to convenience and give the people the right to have erased the information that could not be convenient for them.

Didier Bigo (KCL) started his presentation by asking the audience: how can we re-think the impact of surveillance following the Snowden revelations in 2013? He presented a paper that he co-authored recently with academics working on the field of surveillance.[3] The themes of Bigo's presentation were the definitions of intelligence and national security, the impact on international relations, the relation between intelligence agencies and politicians, and the privatisation of intelligence.

What is intelligence? Bigo called for a clearer definition of the term "intelligence" especially in the context of the logic of intelligence in the US and in other countries across the world. The transnational logic of the organisation of intelligence services, and the fact that they all work together, proves that the divide between US and Europe, "us" vs "them", is a myth. Also, the terminology as regards national security and global citizenship needs to be revisited. The term "National security" in the sense of one country protecting its own citizens is now outdated: we are not in a world where threats come from another nation, now it comes from a globalised source. Global threats and global insecurity mean that there is a need to share information, as national intelligence agencies cannot rely on their own information anymore. Transnational alliances take place between secret services that have been socialised through the lens of national security. Bigo pointed out the disjunction between the cooperation between national intelligence agencies and their discourse.

What does surveillance mean for our understanding of international relations? It is a question of understanding the term "alliance" which has lost its meaning following the globalisation of security and the globalisation of intelligence. An alliance between different countries on the topic of intelligence does not necessarily mean that all components of this alliance have an equal say – the right word may be "networks" where certain parties are at the centre of the network (nodes), others are at the edge, thus creating an asymmetry.

As regards the relation between the professional of security and the politician, which is supposed to have an oversight and control over intelligence, the traditional boundaries are also shifting. How far do the politicians control the sensitive information? National security professionals are supposed to just obey to the national interests as identified by the politicians, but the question is whether they are not the ones deciding on the national interests. The term "Reason of state" has been encapsulated behind the notion of national security, but prior to the 1960es, the term was seen as the first stage of a police state. The difference between law enforcement and intelligence has been made clear in EU affairs, but now the two notions seem to be intertwined. Intelligence agencies manage to find a loophole to get information on their own citizens thanks to the transnational nature of the intelligence-sharing networks, which leads to what Bigo calls "privacy shopping".

Finally, Bigo mentioned the privatisation of intelligence, which is the current trend of private companies getting more and more involved in intelligence issues. Most of the analysis of intelligence has been outsourced to private companies. Leaks and whistleblowers are not a coincidence: they appear more often due to these private companies. The question of trust and mistrust is central here, especially with the concerns of data mining revealing information about consumer attitudes and political opinions.

[3] Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the Impact of Surveillance. International Political Sociology, 8(2), 121-144.

Bigo concluded by calling for a transformation of the understanding of surveillance via the right of data protection for all Internet users, moving from a role of data subject (passive) to data citizen (active). Good examples in Brazil, Germany and the UN could be highlighted.

Paul Nemitz (European Commission) concluded the first day of the Conference by presenting the priorities of the European Commission in relation to Data Protection. According to Nemitz, the main priority of the Commission is to fulfill the promise that the Charter of Fundamental Rights holds out to the EU citizens. Thus, private data should be protected by independent authorities. He highlighted the significance of the fact that this right is protected independent authorities, as it makes it different to the other rights.
He continued by explaining that the inclusion of this right into the Charter showed the maturity on this issue from the societal point of view. The efforts of the Commission to update and complement Data Protection regulation into a digital future brought the Commission to draft a Proposal which was preceded from a consultation with civil society organizations. This newer resolution was agreed by the European Parliament with a vague majority because of two-fold:

- The Members of the Parliament understood the importance of the matter. The big efforts from the Rapporteur (Jan Albrecht) and Co-rapporteur brought various debates and in-depth analysis on the subject.
- The wisdom of the law-maker: Nemitz described it as being technology neutral, to allow the law to develop in the time and use the consensus (not based on one business model).

Nevertheless, a consensus was not reached within the Council and the debate of Data Protection is still on-going.

Focusing on the inter-institutional debate, Nemitz considered that the European Parliament would continue maintaining its position and he considered that the final outcome would be largely what the Commission more or less proposed (although taking long time).

To conclude his speech, Nemitz highlighted his belief that this new regulation would make an important step forward for promoting trust within the society. Nonetheless, in order to reach a good level of Data Protection, it is not only important to work in Europe but also in the transatlantic relations. For this, the Commission is currently working on two projects:

- **The Umbrella Agreement** related to data exchange in police and judicial cooperation.
- **Safe Harbour**. In this regard, he explained that the negotiations are in progress and that the crucial and problematic point is the one related to the 'national security exception'. According to Nemitz, it is important that this point remains an exception and therefore that the collection of data is proportional and never becomes a routine. For the U.S. this entails a Mosaic Theory that consists on the following:
    - Develop tools for targeted and tailored purposes. For the moment the compilation of data is limited on the use but not on the collection.
    - Specific commitments on the Safe Harbour.
    - White spots.

Regarding the latter, the Safe Harbour, the Commission hopes that these regulations will be fulfilled as they count with the support of various enterprises and civil society organisations.

Day 2 – Panel 2

The second day of the conference focussed more specifically on the SAPIENT project. It provided a platform for the summary of the project's results and for a discussion as to how

the project's findings and outcomes could be used moving forward. There were three presentations on the project's themes and findings, followed by a round of expert commentary, followed by a question and answer session, followed by a final summing up of the work, of, and lessons learned from, the project.

The first speaker was **David Wright** from Trilateral Research and Consulting. He began by elaborating the three phases of the SAPIENT project: 1. Research into, and the eventual construction of, a taxonomy of surveillance technologies. 2. The development of a set of scenarios and engagement with project relevant stakeholders. 3. The development of the Surveillance Impact Assessment (SIA) methodology.
He continued by elaborating on the specificities of a SIA. In particular, David described the differences between a SIA and other forms of impact assessment – especially Privacy Impact Assessments (PIA). PIAs are of course useful, but they are limited. In the first instance, PIAs only take into account privacy impacts. A SIA takes into account a much broader scope of impacts, including legal, psychological, ethical and financial impacts. Further, PIAs are only focussed on the individual. SIAs include consideration of a much broader scope of parties who might be impacted by a surveillance technology, including groups and even society as a whole. David demonstrated this breadth by giving a number of examples of questions from the SAPIENT methodology which would be asked in the SIA process, but which would be unlikely to appear in a PIA process.
David finished by considering the benefits of a SIA, both to the surveilled public and to an organisation conducting the SIA: 1. Greater public accountability. 2. Greater public awareness of the consequences of surveillance. 3. Reduction in unwarranted surveillance. 4. A SIA can function as an early warning system for privacy risks. 5. This early warning can help to avoid costly and/or embarrassing privacy mistakes. 6. A SIA can be used as evidence that organisation tries to avoid harm in advance. 7. A SIA can help enhance informed decision making.

The second speaker was **Inga Kroener**, also from Trilateral Research and Consulting. Inga gave an overview of the hands on experience gained from conducting SIAs to trial the methodology developed in the SAPIENT project.
She began by discussing the original methodology developed in the project. This was a lengthy document of 40 pages, including 10 pages of questions. It included an extensive risk assessment process, including multiple steps on the description of the surveillance system, the identification of risks, their assessment and mapping, and on eventual recommendations and approaches to risk treatment. This methodology was sent to 140 companies, inviting them to take part in a trial run of the developed SIA. However, only 3 of these companies responded, and all 3 commented that the process outlined in the methodology seemed too long and complex to undertake. All 3 stated that something simpler would be welcome.
The project consortium took this advice, and reviewed and simplified the SIA process. The simplified process included the same steps but was much reduced in size and complexity. This simplified process was then tested on three European projects – DEPET, ADDPRIV, ANON. (the third project could not be named due to confidentiality) – and one company which had developed technology for a European Project – Mirasys.
This simplified version was generally welcomed by participants in the SIA process – although it was observed that there may still be the need to conduct the more extensive process in certain cases. However, even with this simplified process, there were issues which arose, and certain lessons to be learned moving forwards. 1. Even the light version was seen, at times, as too complex – for example, questions often required clarification from the researcher present. In this regard, it seems that having a specialist present when conducting the SIA remains a good idea. 2. Participants wanted a more open discussion, rather than a formulaic approach. The SIA methodology should thus not be used as a strict and rigid framework, but should allow the flexibility for participants to discuss, and think freely about

issues that come up. 3. Group discussions were far superior to one on one interviews (which was how the ADDPRIV case study was done). Ideally, these group discussions should include representatives from various disciplines/parts of the project. Such group discussions allowed a cross-fertilization of ideas, and a collaborative understanding of problems and meanings which was not possible in one on one discussions. 4. One size does not fit all. Tailored approaches will be needed depending on a number of factors – for example, who is conducting the SIA or how far the technology has already been developed 5. Contacting external stakeholders is essential in the SIA process. Within a project/technology development team, it is impossible to presume the considerations and concerns of the range of different external stakeholders.

The third speaker was **Raphael Gellert** from the Vrije Universiteit Brussel, who gave a presentation entitled: The future of EU Personal Data Protection: The risk management of nothing: Analysing data protection as a risk management regime, pitfalls and potentials.
The founding thesis of this presentation was that, as opposed to the traditional rights based conceptualisation of data protection law, one could also conceive data protection as risk management regulation – in particular, as an attempt to tame and regulate technology to avoid the perceived future risks it poses to individuals.
Raphael considered this possibility firstly through an historic analysis of data protection regulation, attempting to trace references to the idea of risk in data protection law. He observed that the area of law known as data protection was overtly born from the perception that certain forms of new technology came with risks, and that these risks would need to be controlled to ensure social trust. He observed that the concept of risk is explicitly mentioned in many core data protection texts – including the OECD guidelines, Council of Europe texts, the German Data Protection Regulation and others.
Having established the relevance of risk as a concept behind data protection law, he considered how well current data protection law could be classified under risk management frameworks. He elaborated that risk management approaches were characterised be three pillars: 1. Defining what is, and what is not, a risk to be considered. 2. Gathering information on these risks. 3. Approaches to mitigate and control these risks. He concluded that the approaches taken in European data protection law, up to and including the Data Protection Regulation, fit very easily within such a framework.
From this, he sought to draw some further conclusions. If data protection can be conceived of as risk regulation, then perhaps lessons about the benefits and pitfalls of risk regulation, drawn from other areas of law and society, could be of benefit? First, this might allow a better understanding of data protection law, which in turn would allow a better understanding of the direction in which data protection law should go. Second, this would allow a better understanding the correct role of, and approach to, the concept of risk in data protection law. He considered that comparisons between data protection and environmental law – as an area of law with a long history of risk regulation – could be fruitful. He also observed that the history of the flaws of the risk management approach – citing particularly the problems with the New Public Management approaches in the UK in the 80s and 90s – could be important as indicators of problems to avoid in data protection law.

The first of the respondents was **Rocco Bellanova** from the Peace Research Institute Oslo. Rocco had a number of comments to make. 1. He observed a professionalization of data protection and a continuing move towards formalised, one size fits all solutions. As part of one of the SIA test projects, his experience with the inclusion of different disciplines and the integration of their perspectives in the SIA process, was very positive. 2. He wanted to reiterate the importance of the involvement of external stakeholders, to get internal participants to reflect upon, and reconsider their own positions. 3. He observed that data protection assists with governance, and that they are not, as often perceived, two separate entities. 4. He observed the difficulty in developing metrics for surveillance. There is a need

for conventions on such metrics, but such are still lacking. However, he suggested that the different perspectives which may come forward when people are asked to put numbers on surveillance impacts (as they are in the mapping exercise in the SAPIENT SIA) can themselves serve to trigger discussions which can then move toward building communally understood meanings. 5. He wondered about the future of SIAs, and how, when and to what extent they might be included in research moving forward. He particularly referenced their relevance to Horizon 2020. 6. He thought it valuable to keep considering which, and how stakeholders could be included in the process. Asking the question: How can people be empowered to use data protection in their own way? 7. He was complimentary to the project as he saw that, in continual reflexive reference to data protection, perhaps other issues, and approaches to issues, could be obscured. The breadth of the approach of SAPIENT, beyond simply data protection, was a valuable contribution in reopening such discussions. 8. Finally, he considered Raphael's presentation, and reflected on the significance of defining, and redefining, data protection, before using it as a tool from which to advocate.

The second commentator was **Jens-Henrik Jeppesen** from the Centre for Democracy and Technology (CDT). Jens commented on the continuing importance of data protection issues on the CDT's agenda and how important the reigning in of 'rampant' electronic surveillance was. He also commented on the continuing need for discussion and consideration of both US, and European state surveillance, which often function collaboratively.
With respect to David's presentation, Jens commented that there remained a lack of response from government in engaging with surveillance reform. He considered that there was often an implicit assumption that an impact assessment, balancing all relevant interests had taken place, although he questioned to what extent a number of interests were truly taken into account by governments engaging in surveillance practises. In this regard he recognised PIAs and SIAs as important tools, but also saw them as limited in what they could achieve. He noted that it was still the job of the regulators to set out concrete privacy rights. He followed this point up with a consideration of the risk of formalisation of PIAs and SIA. He noted that, whilst it was essential that such assessments be made public, there was a risk that, because they were to be made public, they might become formal box ticking exercises: this would run counter to their goal.
With regard to Raphael's presentation, Jens wanted to reiterate the point that the rights at stake are human and fundamental rights. In this regard, he wanted to highlight that a risk approach, which focuses on harm mitigation rather than concrete prohibition, should not always be seen as the best approach.

The third person to comment was **Reinhard Kreissl** from the Institute for the Study of Law and Criminology. Reinhard began by discussing the relevance of the work done in the IRISS project, and its alternative approach to considering surveillance – from the perspective of how citizens understand and use surveillance.
He then remarked on the limitations of a SIA if it is done as a one off exercise. He noted that such an approach does not take into account the evolution of technology, nor could it take into account the assemblage of systems which eventually define a surveillance system.
He also observed that the logic of the SIA was to focus on the technology and its impact on users. However, he remarked that impact cannot be accurately assessed *a priori*. He suggested an alternative approach might move away from the humans v. technology approach, toward a techno-social hybrid approach. This approach would rest on the premise that, as citizens in modern society, we are already tied into many technology based systems, and are co-constructors of the eventual function and consequence of surveillance systems. Accordingly, in a techno-social hybrid approach, users would be integrated into the SIA process beyond simply considering them as 'impacted'.
He concluded with some broader observations about the development of data processing technologies and what this means for the core concepts we use to frame it. He observed a

move from being able to consider data as single pieces of isolated information, remarking on the ability of social research to transform trivial data into interesting personal information which tells the possessor much about the individual. He also considered that the idea of being 'machine readable' as constituting a novel ontology in itself. With this in mind, it may be insufficient to rely on concepts developed in a context where this ontology was not present. Accordingly, a reconceptualisation of concepts such as privacy, and autonomy, may be necessary.

The last commentator was **Elspeth Guild** from the Centre for European Policy Studies. Elspeth generally welcomed the SIA concept and methodology, and was positive about the project and what it had achieved.
However, following this, she noted an important issue which she felt had been absent from the discussion up to that point. She felt that questions of surveillance could not be detached from questions of the knowledge that surveillance produced, and in turn, this knowledge could not be detached from the power relations it served (and created). She felt that the issue of power had largely been missing from the discussion. Using the example of the anthropologist studying a remote Chinese village, who then published a paper with knowledge which was then used, on the one hand, by a civil rights lawyer to help a refugee, but on the other hand by the Chinese secret service to crush dissidents, she observed that surveillance could be turned into different types of knowledge and different types of power. Using the example of the Hoover files, she highlighted the potential power of knowledge and the importance, when considering surveillance, of asking questions such as: For whom is knowledge being made? About whom? Who will this knowledge be given to? She observed that we are all constantly in the process of the co-production of data, but that the real issues lie with who gets this data, and what they want to do with it.

Following these comments, **David Wright** made the point that the SAPIENT project was proud of what had been achieved with the SIA methodology, but that institutions often found even the shorter version to be too detailed. He called on **Chris Connolly** from Galexia (a speaker on the previous day) to comment from his wealth of practical experience.
Chris commented from his experience with PIAs. He started by observing that, when they started, they were long, complex and comprehensive. However, that in the last 2 or 3 years, there had been a push back against long PIAs. The focus now seemed to be on shorter PIAs, perhaps even only focussing on one or two issues. He observed, however, that although these PIAs were faster, shorter and cheaper, they were still often used to justify projects and technologies in exactly the same way as the more comprehensive PIAs.

Raphael Gellert followed up by responding to **Rocco Bellanova** agreeing about the significance of conceptualising data protection. He added to this by stating that, when one looks at policy principles, these may differ in style and quality of protection depending on which conceptualisation of data protection one takes.
He also added that there was a continuing need to consider the scope of data protection – what does it apply to, when etc. Such definitions can pose serious legal hurdles to the protection offered. However, he also observed the necessity of looking beyond data protection – for example to the rich body of law on discrimination – to make up for the shortfalls and limits of data protection.

Inga Kroener followed next, in principle agreeing with Reinhard about people as co-producers in a techno-social hybrid model. However, she wondered what a SIA which used this as a start point might look like in practise.

Reinhard Kreissl responded by considering the facebook psychology experiment – which has recently received much media coverage. He observed that there were a number of

unexpected surveillance practises occurring. He saw that we might go deeper into the structure of the surveillance system, and from there create completely new ways of assessing technologies.

Erik Josefsson, a representative of the Greens, questioned whether an impact assessment, even if done within the bounds laid out by the impact assessment procedure, would not often result in a green light for a project which ought, on more substantive grounds, to be stopped. He gave the example of the Data Retention Directive as an example of this – the Directive passed the Commission's impact assessment, but was substantively ruled illegitimate by the ECJ.
He followed this question up by wondering, in relation to Reinhard's presentation, how such a conceptualisation of surveillance might impact the balancing of power, and interests, done by the courts.

Else Boekesteijn, a representative from the European Association of Co-Operative Banks, then asked Raphael how, in relation to his presentation, it was possible to match legal certainty when processing data, with a risk based approach.

Didier Bigo, from King's College London, asked – in relation to Reinhard's conception of the socio-technical hybrid – about responsibility. He commented that we would never put a computer on trial. He wondered how far legal responsibility and sociology could go together. He commented that methodology is interesting, but that responsibility remained a central question. He finished by commenting that we may be involved in the co-production of surveillance, but that we are rather intent on self-exposure, which does not necessarily invite surveillance – for example when a person writes a facebook post, that is directed at their facebook friends, rather than inviting the surveillance of third parties.

Sergio Carrera, from the Centre for European Policy Studies, asked about the role of impact assessment and power in the EU. He observed that the results of SAPIENT will be put at the disposal of those in power. He wondered how to take the impact of power relations into account, and whether the current methodology was able to do this.

Raphael Gellert responded to the Greens representative and observed that system, impact and consequence were dynamic and constantly being created. Accordingly, impact assessments, including PIAs and SIAs should be done reflexively and continuously through the life cycle of a project.
In response to Else Boekesteijn he commented that the question of legal knowledge is really central, and that it was imperative to integrate legal categories into risk tools and methodologies.

In a final comment in response to the questions, **David Wright** observed that the final responsibility lies on the organisation which wants to introduce new technologies. If this organisation wants to take the impact assessment to the regulator, then that is their choice. However, he added that the process states that there should always be a third party reviewer regarding the adequacy of a PIA or a SIA – this might be the regulator.
David observed that the Commission has been studying impact assessment methodology for the last 20 years and that their guidelines are very detailed. However, he observed that the actual impact assessments can differ greatly in quality.
He observed though, that the Snowdon revelations had driven home how necessary it was to have oversight over surveillance and the organisations which conducted surveillance and he hoped that SIAs could make a positive impact in this regard.

The concluding speaker was **Michael Friedewald**, from the Fraunhofer Institute for Systems and Innovation Research, who gave a recap of the journey of the SAPIENT project, and some insight into where the work of SAPIENT might go from here.

He noted that, throughout the course of the project, there was much technological change, and much change in the attitudes of citizens to surveillance. He recalled that the worst thing imagined in 2009, was the deep packet inspection for advertising conducted by the company Phorm. The reality in 2014 is much worse. There is of course the NSA, and other intelligence services' mass collection activities. However there is also a proliferation in everyday surveillance technology and an increasingly fast development of novel types of surveillance technologies – for example, the internet of things, face recognition technologies, brain computer interfaces etc.

He commented on the initial idea behind 'smart' surveillance, as surveillance which would be able to avoid blanket surveillance by focussing on only that which should be surveilled. He recalled that, at the start of the project, there were high hopes from the Commission that smart surveillance could be tailored to be targeted at the 'critical parts'. However, reality dashed these hopes. The reality is rather that 'smart' surveillance is used for both broader, and deeper surveillance by both the state and private organisations.

Michael noted a number of general lessons learned through the project. 1. That precaution is needed in the development and deployment of surveillance technologies. 2. That there is a constant need to monitor the development of technologies. 3. That citizens' attitudes change, and this should be borne in mind. The Eurobarometer results pre-Snowden would almost certainly look different if the same survey was conducted today. 4. That there are increasing protests against the infringement of human rights through surveillance. 5. That citizens' engagement is crucial. The trust of the public is hard to gain, and easy to lose. Michael suggested that an approach to surveillance for the future should be based on transparency rather than secrecy, on the early involvement of stakeholders and on accountability mechanisms. PIAs and the SIA methodology developed in the SAPIENT project are one piece – albeit a small piece –in regaining control over surveillance.

He concluded by noting that there was still a lot of work to do. Noting that Article 33 of the Proposed Data Protection Regulation would make doing a data protection impact assessment law, he observed that there was still no consensus on a number of issues. Questions remain as to how assessment methodologies should look and be used – is a data protection impact assessment adequate – which approach they should take – risk v. compliance – how to make them practicable and scalable and how to make them compatible with other types of assessment – for example technology assessments.

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de