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:	36 months

Deliverable 6.4:

More Surveillance, More Security?

The Landscape of Surveillance in Europe and Challenges to Data Protection and Privacy – Policy Report on the Proceedings of a Conference at the European Parliament

Rapporteur:	Nicholas Hernanz with contributions by Elspeth Guild and under the supervision of Sergio Carrera (Centre for European Policy Studies – CEPS)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.1
Due date:	30 September 2011
Submission date:	30 January 2011

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

This document was developed within the SAPIENT project (see http://www.sapientproject.eu), co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (co-ordinator),
- Trilateral Research & Consulting LLP,
- Centre for Science, Society and Citizenship,
- Vrije Universiteit Brussel,
- Università della Svizzera italiana,
- King's College London, and
- Centre for European Policy Studies

Document history

Version	Date	Changes
1.0	30 January 2011	Version 1 of deliverable
1.1	30 January 2011	Minor corrections

Contents

Executive Summary

On 9 November 2011, CEPS and the Privacy Platform, in the context of the SAPIENT project, organised a policy meeting at the European Parliament on the topic of state surveillance in the EU and challenges to data protection and privacy. This report offers a synthesis of the discussions that took place at the policy meeting and highlights the main dilemmas posed by surveillance technologies and private data collection and sharing. Focusing on three main case studies at the centre stage of the debate at the EU level, namely the Passenger Name Record (PNR) mechanism, the practice of collecting and sharing DNA under the Prüm Decisions, and the Terrorist Finance Tracking Programme (TFTP), the policy meeting gathered a range of insights from relevant stakeholders, through which the central controversies have been identified.

First, participants discussed the PNR mechanism, under which third countries request European airlines to send them detailed data of passengers boarding international flights in an effort to prevent terrorism and organised crime. These requests run counter to EU data protection rules and have triggered the negotiation of bilateral agreements on PNR between the EU and the US, Canada and Australia. An EU PNR system is also under development.

Second, on the exchange of DNA data under the Prüm Decisions for the purpose of fighting terrorism and international crime networks, debates centred on the sensitivity and intrusive nature of such data sharing, as genetic data can potentially reveal additional information about an individual, such as health risks.

And third, the TFTP context was examined by speakers, with an emphasis on how access by US authorities to databases of bank transfers and financial transactions of suspected terrorists for the prevention and investigation of terror plots was in line – or not – with EU safeguards for data protection.

From the presentations of the speakers and the discussions that followed, three important issues related to the practices of collecting and sharing personal data emerged:

1) The idea of consent, by which personal data belongs to the citizen and cannot be processed without his or her consent, is enshrined in the EU Charter of Fundamental Rights in its Art. 8. Current practices at the EU level clearly endanger this principle, in that private data may be transferred to third countries without informing the individual concerned.

2) Also of concern is the right to the presumption of innocence, laid down in Art. 48 of the Charter of Fundamental Rights. Increased surveillance activities by law enforcement agencies lead to a general state of suspicion, in which every individual is a potential suspect.

3) Finally, there is the question of democratic accountability, which is essential in the field of security policies and which is being undermined as well. Owing to the specific structure of the Area of Freedom, Security and Justice in the EU, the role of the European Parliament is still not strong enough to provide democratic scrutiny and oversight on matters that are sensitive for privacy and data protection.

These crosscutting concerns appeared in all three case studies. They allowed partners from the SAPIENT project to explore the controversies linked to EU security policies, their intrusive nature for individual freedoms, and the dilemmas and risks associated with privacy and data protection issues from the perspective of the rule of law and fundamental rights. The SAPIENT project is continuing to work on these issues by taking into account the results of this policy meeting and the central position of the Charter of Fundamental Rights in the debates.

1. Introduction

1.1 General background to the meeting

This proceedings report[1] offers a synthesis of discussions that took place at the policy meeting organised on 9 November 2011 at the European Parliament, on the topic "More Surveillance, More Security? The Landscape of Surveillance in Europe and Challenges to Data Protection and Privacy". The report also identifies the dilemmas and controversies posed by surveillance technologies as well as private data collection and sharing in the context of the EU's Area of Freedom, Security and Justice (AFSJ), which was established to ensure the free movement of persons and includes asylum and immigration policies, police cooperation, and the fight against crime. To provide a clear background on the main issues at stake, this analysis anchors the policy debates on surveillance to current research on this topic, including the research done by the SAPIENT project.[2] It is in the framework of this project that the meeting of 9 November 2011 was jointly organised by the Privacy Platform and the Centre for European Policy Studies (CEPS).

- The Privacy Platform is an informal cross-party initiative of MEP Sophie In 't Veld to bring together interested MEPs, Commission and Council officials, and representatives of industry, NGOs, think tanks, academia, data protection authorities and civil society. It aims at sharing information, facilitating debate and fostering better awareness and understanding of privacy issues.
- SAPIENT is a 36-month collaborative project on smart surveillance technologies and their impact on privacy and data protection rights funded under the European Commission's 7th Framework Research Programme. The SAPIENT project is carried out by a consortium of seven multidisciplinary research institutes, among which CEPS provided logistical support for the organisation of the policy meeting. CEPS strives to facilitate the links between the SAPIENT project and debate on data protection and privacy issues at the EU level.

More surveillance, more security? This question guided the overall content of the policy meeting and reflected the need for an in-depth debate at the political level, especially at this crucial time when a number of adjustments are taking place on the EU's justice and home affairs scene. Following the entry into force of the Lisbon Treaty in December 2009, the pillar structure of the EU was abolished and the AFSJ saw its policy fields, which had been spread across the first and third pillars, merged into one fairly consistent legal and institutional framework. The Stockholm Programme,[3] a political roadmap presented in December 2009 that set up a five-year plan for the development of the AFSJ, recommended the establishment of an internal security strategy with a view to fighting organised crime and terrorism. The EU Internal Security Strategy (ISS) adopted in February 2010[4] reflects this approach.

In this renewed institutional setting and against a backdrop of assumed 'threats' to European security, the EU has proposed and adopted a number of instruments that foresee the collection, use and exchange of personal data and information on individuals. The rationale behind this trend is linked to the fight against

[1] The author of this report, Nicholas Hernanz, is Research Assistant in the Justice and Home Affairs section of the Centre for European Policy Studies. This report was drafted under the supervision of Sergio Carrera, Senior Research Fellow and Head of the Justice and Home Affairs section of the Centre for European Policy Studies. The author would also like to thank Elspeth Guild for her comments.

[2] SAPIENT stands for **S**upporting Fundament**A**l Rights, **PrI**vacy and **E**thics in Surveilla**N**ce **T**echnologies (see http://www.sapientproject.eu/).

[3] Council of the European Union, The Stockholm Programme – An Open and Secure Europe Serving and Protecting Citizens, OJ C 115/01, 04.05.2010.

[4] Council of the European Union, *Draft Internal Security Strategy for the European Union: Towards a European Security Model*, 5842/2/10, Brussels, 23 February 2010.

terrorism, which became more salient after the 11 September 2001 attacks in the US and was stepped up following the Madrid and London bombings in 2004 and 2005 respectively. Thanks to technological advances available to EU member states, cooperation based on exchange of information and data processing for intelligence and law enforcement purposes has progressively emerged as a policy priority at the EU level.

In parallel, the right to the protection of personal data has been enshrined in Art. 8 of the Charter of Fundamental Rights of the EU, which became legally binding after the entry into force of the Lisbon Treaty in December 2009. This is the first time that the right to data protection has been recognised as an autonomous fundamental right in the EU legal order, distinct from the right to respect for private and family life.[5]

In this context, the European Parliament has played an important role in the policy debates surrounding privacy and data protection standards in the fields of police and judicial cooperation in criminal matters. Before the entry into force of the Lisbon Treaty, the European Parliament used its non-binding and consultation-only powers widely in order to elevate the right to the protection of personal data to an autonomous fundamental right in the EU. In the post-Lisbon setting, the European Parliament has acquired the status of a co-legislator and the power to amend or block decisions related to justice and home affairs issues, meaning that it now has a say in almost all recent EU legislative proposals in these fields, as well as in the negotiation of international agreements.[6] The present EU debate on a new legal framework on data protection is crucial for the topic at hand, as one of the directives to be proposed by the European Commission concerns data protection in the areas of police and criminal justice.[7] These legislative developments and the increased role of the Parliament made it all the more important for CEPS and the partners of the SAPIENT project to organise this policy meeting jointly with the Privacy Platform of the European Parliament.

The meeting allowed EU and international policy-makers, academics and practitioners to explore the challenges posed by EU security policies, their intrusive nature for individual freedoms and the dilemmas and risks linked to privacy and data protection issues from the perspective of rule of law and fundamental rights, as well as the necessity and proportionality of such measures.

This proceedings report explores the three main case studies that framed the discussions at the policy meeting: the Passenger Name Record (PNR) mechanisms, the practice of collecting and sharing DNA under the Prüm Decisions, and the Terrorist Finance Tracking Programme (TFTP). The crosscutting nature of these three case studies, as well as the strong stance taken by the European Parliament on each one, allows for a more in-depth analysis of the issues and trends shaping the EU debate.

1.2 More Surveillance, More Security? Contextualising the debate

The welcome session of the policy meeting saw MEP Sophie In ‘t Veld, European Commission official Bruno Mastantuono, as well as SAPIENT members Sergio Carrera from CEPS and Michael Friedewald

[5] The right to respect for private and family life, established in Art. 8 of the European Convention on Human Rights, has been broadened by the case law of the European Court of Human Rights in Strasbourg to include the rights to privacy and partially to data protection. The EU Charter of Fundamental Rights mirrored Art. 8 ECHR in its Art. 7 but created a new Art. 8 on the protection of personal data as a fundamental right.

[6] Examples include the EU–US SWIFT bank data transfer agreement (2010) and the EU–Australia Passenger Name Record agreement (2011).

[7] European Commission, *Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data (Police and Criminal Justice Data Protection Directive)*, COM (2012) 10 final, 25.01.2012.

from the Fraunhofer Institute present the main issues, putting into perspective the latest developments in state surveillance and the research context.

Sophie In 't Veld, MEP (ALDE, Netherlands), Chair of the Privacy Platform in the European Parliament, introduced the topic of the policy meeting by explaining that citizens in the EU are now more and more watched and monitored on cameras, communications, online activities, etc. According to In 't Veld, blanket surveillance of all citizens, as in the novel *1984* by George Orwell, is no longer mere science fiction, but is possible today. Indeed, new technologies and legislation enable governments to monitor every intimate detail of people's lives more closely than "Big Brother" could have ever imagined. In 't Veld set out the two central questions of the policy meeting: Are EU citizens really safer now that surveillance activities are operating in member states and across the EU? And what is the place of the EU Charter of Fundamental Rights and the right to data protection in this debate?

Sergio Carrera, Senior Research Fellow & Head of Justice and Home Affairs Programme at CEPS, presented the work of CEPS on these issues and explained the choice of the three main case studies selected for this policy meeting: the EU PNR system, the DNA sharing under the Prüm Decisions and the EU Terrorist Finance Tracking System (TFTS). One of the key findings of a recent CEPS study for the European Parliament on a new legal framework on data protection[8] is the difficulty of ensuring the practical provision of data protection as a fundamental right. Carrera fully agreed with Sophie In 't Veld that the EU Charter of Fundamental Rights should have priority when dealing with data protection. He also critically addressed the 'balance' metaphor, on the grounds that weighing data protection against state security could only be self-defeating for individual rights.[9] The fact that the European Parliament has acquired new powers in this policy area since the entry into force of the Lisbon Treaty should encourage MEPs to use these powers to push data protection to the forefront of the debate. Independent evaluations of large-scale databases and their costs should also be supported.

Sophie In 't Veld shared Sergio Carrera's concerns about fundamental rights but warned that the European Parliament was operating in a hostile environment for data protection. In her view, a small minority of MEPs is exercising "damage control" in trying to limit the privacy abuses contained in the legislative texts under negotiation.

Michael Friedewald, Coordinator of the SAPIENT project, Fraunhofer Institute, presented the results of the first eight months of work on this project. According to him, surveillance has become so widespread that it raises questions about the role of monitoring technologies, including the precautionary principle.[10] He also referred to the conclusions of a previous EU-funded project on ethics and security, the INEX project,[11] which recommended that an impact assessment be undertaken for surveillance technologies in all future EU legislative proposals. A report on the state-of-the-art in the field of surveillance studies will be published by SAPIENT.

---

[8] See D. Bigo, S. Carrera, G. González Fuster, E. Guild, P. De Hert, J. Jeandesboz and V. Papakonstantinou, *Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament*, Study of the Policy Department C, DG for Internal Policies, European Parliament, CEPS, Brussels, November 2011.

[9] Ibid., p. 100.

[10] The precautionary principle states that if a policy has a suspected risk of causing harm to the public, the burden of proof that it is not harmful shall fall on those taking the action (in the absence of scientific consensus that the action or policy is harmful). For a more detailed definition, see R. von Schomberg, "The Precautionary Principle and its Normative Challenges", in E. Fisher, J. Jones and R. von Schomberg (eds), *Implementing the Precautionary Principle: Perspectives and Prospects*, Cheltenham, UK and Northampton, MA: Edward Elgar, 2006, p. 47.

[11] INEX is a research project funded under the European Commission's 7th Framework Programme on "Converging and conflicting ethical values in the internal/external security in continuum in Europe". For more information about the project, which concluded in August 2011, see the INEX website (http://www.inexproject.eu).

Bruno Mastantuono, Legal Adviser, Research Executive Agency (REA), European Commission, summed up his work as a legal adviser, managing funding opportunities under the 7th Framework Programme for Research and Technological Development (FP7). He noted that some of the proposals submitted for evaluation to the REA may raise ethical concerns as regards data protection or fundamental rights, and provoke debate about how to strike the right balance between security and fundamental rights.

He stressed that legal entities participating in FP7 are bound to comply with the FP7 ethical and legal framework irrespective of their country of establishment. All beneficiaries of EU co-funding shall, therefore, comply with applicable international, EU and national legislation.[12]

In this regard, he highlighted that specific procedures and safeguards have been put into place by the Commission and the REA to ensure compliance with the ethical and legal framework.

In their proposals, FP7 applicants are requested to elaborate on the ethical implications of the research envisaged. Specific guidance is provided in this sense to the researchers in the FP7 guide for applicants. The ethical aspects are thus already considered by the experts in the framework of the scientific evaluation of the proposals that is managed by the REA.

After the scientific evaluation, the projects proposed for EU co-funding and those from the reserve list undergo an ethics screening run by independent ethical experts appointed by the REA, who manage the process. The experts assess the proposals and issue recommendations that may lead to a revision of the proposal or to specific legal commitments in the grant agreements (or both). A second-stage ethical check of the proposals (ethical review) may also be carried out, at the level of the Commission (DG Research & Innovation), for the most sensitive proposals. The decision on the selection of the projects is taken by the Commission.

It was underlined that REA attributes the utmost importance to the ethical screening/review process, which, in certain cases, may also lead to the exclusion of certain projects from EU co-funding.[13]

2. Determining the challenges for Passenger Name Record mechanisms

2.1 Introducing the topic

The EU Internal Security Strategy, agreed in 2010 by EU member states, called for the establishment of a "European Passenger Names Record (PNR)...for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime"[14] as a prevention and early-warning tool. What is a PNR? A PNR can be defined as a record of the itinerary of a travelling person saved in the database of an airline, usually during the booking process. PNRs started raising concerns after the 11 September 2001 attacks in the US, when the US Department of Homeland Security requested PNR data from airlines in order to prevent and investigate terrorist attacks. Airline companies from the EU had to comply, although EU legislation expressly prevented the transfer of personal data to third countries with a lesser level of

[12] Ethical principles, data protection and the right to privacy are enshrined in several international treaties, such as the Convention on Human Rights and Fundamental Principles, the Lisbon Treaty and the EU Charter of Fundamental Rights.

[13] REA organised a workshop on "Ethical issues in security research" (for material and presentations, see http://ec.europa.eu/research/rea/index.cfm?pg=ethics7fp_workshop2011).

[14] See Council of the European Union, *Draft Internal Security Strategy for the European Union: Towards a European Security Model*, 5842/2/10, Brussels, 23 February 2010, p. 12.

data protection.[15] This situation triggered the negotiation, in May 2004, of the first EU–US PNR agreement. It was subsequently annulled by the European Court of Justice in 2006,[16] due to an action brought by the European Parliament before the Court against the Commission and Council. Another agreement was signed in 2007 and applied on a provisional basis. In May 2010, however, the European Parliament decided – after having been granted negotiating powers by the entry into force of the Lisbon Treaty – to renegotiate bilateral PNR agreements in the form of a 'PNR package' with the US, Canada and Australia. A mandate was given in December 2010 to the European Commission to renegotiate all PNR agreements with these three countries.

Negotiations with the US and Canada are underway,[17] while the EU–Australia PNR agreement was approved by the European Parliament in October 2011. In parallel, the EU is setting up its own internal PNR system, with a directive on PNR[18] having been presented by the European Commission in February 2011. The proposed directive is under negotiation between the Council and the European Parliament, with Timothy Kirkhope, MEP (ECR, UK) as rapporteur. This EU PNR system gives rise to several issues, including questions of the necessity and the proportionality of such a system. As some of the speakers pointed out during the meeting, the uncertainty of the added value of the dissemination of personal data of EU citizens boarding flights to and from the 27 member states triggers debate about whether this system is "appropriate for attaining the objective pursued and does not go beyond what is necessary to achieve it".[19]

2.2 Proceedings of the panel

Timothy Kirkhope, MEP (ECR, UK), chaired the panel and presented the main issues at stake. He noted that four member states[20] already have a PNR system, and posed the question of whether this EU PNR system should only cover flights leaving and entering the EU or also intra-EU flights. He also highlighted the role of necessity and proportionality tests, the costs implied by the system and sensitive questions surrounding the storage of data. In his view, the cost of implementing an EU PNR system would amount to a few cents more on plane tickets for consumers. As for the necessity test, he contended that evidence of multiple arrests of criminals thanks to this system proves that there is a clear need for an EU PNR. Kirkhope discussed his deep involvement in these issues as the rapporteur on the EU PNR directive, and interest as a former Home Office minister of the UK.

The first panellist to take the floor was **Brendan Nelson,** Ambassador of Australia to the EU. He presented the Australian government's point of view as regards the EU–Australia PNR agreement and summarised the main reasons behind this agreement. He highlighted that Australia, as an island continent,

---

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement such data provides, in its Art. 25, provides that transfers of personal data to third countries may take place only if the third country in question ensures an adequate level of protection.

[16] See the Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04, 30 May 2006.

[17] The EU–US PNR agreement has been negotiated and is now awaiting signature – see European Commission, *Proposal for a Council Decision on the signature of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security*, COM(2011) 805 final, Brussels, 23 November 2011.

[18] European Commission, *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, Brussels, 2 February 2011.

[19] The principle of proportionality has been defined in the case law of the European Court of Justice – see for example Case C-58/08, *Vodafone and Others* [2010] ECR I-0000, 8 June 2010, paragraph 51.

[20] These are Sweden and the UK, with a completed PNR system, and France and Denmark, with a PNR system currently being developed.

receives a majority of its visitors by airplane, which involves high security risks. As a result, Australia started collecting PNR data as early as 1998 on a voluntary basis, and made this data collection mandatory in 2004 after a vote in parliament. Airline companies such as Qantas or British Airways found themselves in a situation where an agreement between Australia and the EU became necessary for them to comply with Australian legislation. Nelson stated that since then, not a single complaint regarding privacy issues has been filed. The collection of PNR data in 2009 alone led to the conviction of more than 70 criminals in the field of child pornography, child sex tourism, drug trafficking and terrorism.

Jan Philipp Albrecht, MEP (Greens, Germany) and the Greens' shadow rapporteur for the EU PNR proposal, expressed his doubts about the data protection implications of the future EU PNR system. In his view, the presumption of innocence should be a priority when dealing with the collection of data, as data protection is clearly a part of the fundamental rights framework in the EU. The increasing number of existing large-scale databases in the EU is a worrying trend. While he acknowledged that it is of course useful to collect data in order to stop crime, intrusive data collection must be justified – there is a need to prove that other less intrusive means cannot be used for the same expected results. In this time of crises and debates concerning public expenditure, he does not see how these costly measures could be justified.

The next speaker was **Filip Jasiński**, Justice and Home Affairs Counsellor at the Permanent Representation of Poland to the EU. As a response to participants invoking the EU Charter of Fundamental Rights and its article on data protection, Jasiński started his presentation by stating that the processing of PNR data is covered by both Art. 6 concerning the right to security and Art. 8 on personal data protection. He then presented the Polish Presidency's views on the proposed EU directive on PNR, emphasising its objective to make sure that access to PNR data will only be available to a selected number of officials from law enforcement authorities. The preferred option as regards the scope of the EU PNR system would be to include intra-EU flights, as according to figures cited by Jasiński, 90% of trafficking is carried out on these flights. The GENVAL Working Group of the Council of the European Union is keen to agree on a PNR instrument that will avoid unnecessary costs and be transparent and effective in stopping crime networks.

Wishing to defend the Commission's proposal of February 2011, **Joaquim Nunes de Almeida,** Head of Unit "Police Cooperation and Access to Information", DG Home Affairs, European Commission, stressed the importance and the usefulness of a PNR system to fight terrorism. He acknowledged the principle of the presumption of innocence but recognised that police work would not be the same without the instinct of police officers, who have to guess about suspicious and inappropriate behaviour by individuals. Profiling criteria should not be made public, as criminal networks would be made aware of key information related to police work. Nunes de Almeida also advocated a decentralised system, given the extreme sensitivity of the information collected, which should be stored at the national level. As for the costs, preliminary estimations show that it would amount to €0.10 per plane ticket. Finally, the speaker pointed to the effective use of PNR data in Australia, Canada and the US, where no damage to privacy had been reported.

The final panellist was **Margreet Lommerts,** Manager of Security and Cargo at the Association of European Airlines (AEA). She presented the work of the AEA, representing 35 member airlines that ensure the transportation of more than 400 million passengers annually. On the issue of PNR, airline companies support the Commission's proposal in its purpose of harmonising PNR systems across the EU, as there is a high risk of diverging rules among member states, which could in turn lead to increased costs for airlines. The main concerns of the AEA relate to the costs of such a system and the additional burdens involved. PNR was first introduced among airline companies to facilitate the transfer of passengers during flight changes. The data exchanged among companies included the name, contact details and itinerary of the passenger. Today, more and more state authorities are requesting the disclosure of airlines' passenger data. According to the AEA, the costs of financing data collection and transfer in the EU should be borne by requesting member states; she quoted estimates placing the cost of PNR measures at €0.17 per passenger. Finally, she highlighted that PNR data transfers requested by third countries, such as Japan,

South Korea and Saudi Arabia, put the AEA in a difficult situation, because airlines may only transfer personal data if the third country in question can ensure an adequate level of protection of such data. Until agreements with these countries are negotiated by the EU, airlines will not be in a position to comply with such requests and will face the risk of not being able to operate in these countries.

2.3 Conclusion of the panel and open discussion on PNR

In his role of discussant, **David Wright**, Managing Partner and Co-Founder of Trilateral Research and Consulting, identified several questions linked to the PNR system. Among them was that none of the comments made by the Article 29 Working Party, the Office of the European Data Protection Supervisor, the European Parliament or the European Commission's Legal Service have been taken into account. Furthermore, there was the inevitable fact that the use of large databases will lead to mission creep and not be limited to their original purpose. There is the issue of assessing the cost-effectiveness of a PNR mechanism, and the need to consider whether there are better and cheaper alternatives. Finally, there is the danger of transforming innocent citizens into suspects, which Wright identified as the biggest danger. His questions sparked many reactions during the open discussion with participants, and reflected the main challenges posed by the establishment of an EU PNR mechanism, which the SAPIENT project will analyse.

The central question that arose during the panel concerned the necessity and proportionality tests linked to the PNR system. Is this system the optimal solution to achieve the objective of fighting terrorism and serious crime? Could less intrusive means accomplish the same goal? The impact assessment undertaken by the European Commission that accompanied its PNR proposal[21] has been criticised by several stakeholders for its weak analysis of the cost-effectiveness of such a system, its impact on fundamental rights and its use of the 'balance' metaphor on striking a right balance between security and privacy.

Another issue connected to the previous one is the purpose of using PNR data, and the possible 'function creep' identified by several participants in this panel. According to the European Commission's proposal, the purpose of PNR data is limited to the "prevention, detection, investigation and prosecution of terrorist offences and serious crime", but it has been argued that the database might be used for other purposes in the future, especially as the definition of "serious crime" varies across member states.[22]

A key aspect identified by participants was the idea of consent: personal data belongs to the citizen and cannot be processed without his or her consent, as enshrined in the EU Charter of Fundamental Rights in its Art. 8. This aspect becomes problematic when sending PNR data to third countries without informing the citizen in question.

Also of concern was that more surveillance would lead to more suspicion, especially in the case of airplane travellers. This poses a challenge to the fundamental right to presumption of innocence (Art. 48 of the Charter of Fundamental Rights) as well as non-discrimination (Art. 21), as generalised suspicion leads to increased profiling by law enforcement authorities.

Questions also arose as regards such technical details as the storage of data – data retention has been limited to five years in the Commission proposal, and law enforcement authorities must depersonalise the data one month after the flight. Likewise there questions about the costs incurred by establishing such a system, with estimations ranging from €0.10 to €0.17 per ticket.

---

[21] European Commission, *Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes*, Commission Staff Working Document, Impact Assessment, SEC(2007) 1453, Brussels, 6 November 2007.

[22] See E. Brouwer, *Ignoring Dissent and Legality – The EU's proposal to share the personal information of all passengers*, CEPS Liberty and Security in Europe paper, CEPS, Brussels, June 2011, p. 2.

Finally, the role of the European Parliament and the principle of democratic accountability were horizontal issues throughout the discussions. Several speakers emphasised the key role of Parliament in safeguarding citizens' rights in the face of new security and surveillance proposals, especially after acquiring new powers with the entry into force of the Lisbon Treaty.

Most of the issues raised during the discussions are horizontal ones that recur throughout the rest of this report. Moreover, they constitute an excellent basis for the SAPIENT project in its work towards understanding the dilemmas posed by the collection, storage and exchange of personal data.

3. DNA collection and sharing under the Prüm Decisions – Context and challenges

3.1 Introducing the topic

The second case study chosen in the framework of the SAPIENT policy meeting deals with the issue of collecting and exchanging DNA profiles at the EU level for the purpose of investigating and preventing criminal offences, and more specifically with the provisions included in the Prüm Treaty and the subsequent Prüm Decisions. Signed in 2005 by seven EU member states,[23] the Treaty of Prüm provides for the facilitated exchange of data concerning DNA files, fingerprints and vehicle registration for law enforcement purposes. Why Prüm? As stated in the Preamble, the objective of the Treaty is "to play a pioneering role in establishing the highest possible standard of cooperation especially by means of exchange of information, particularly in combating terrorism, cross-border crime and illegal migration". It was signed outside the EU framework as a purely intergovernmental form of cooperation.

The Treaty of Prüm contained an explicit statement in its Preamble foreseeing the content of the Treaty being incorporated into the legal framework of the EU. In this context, a proposal to integrate Prüm was presented as early as January 2007 by the German Presidency of the Council. Certain provisions that would have come under the ex-first pillar were left out of the German initiative, which consequently prevented the European Parliament from participating in negotiations as a co-legislator. The Parliament was asked to deliver a non-binding opinion, one of the weakest of the institution's engagements in law-making, with a mere three months to prepare it.[24] Another consequence resulting from the accelerated adoption of the Council's text was the lack of a proper impact assessment of the measures proposed. The Council adopted a Decision and its implementing provisions in 2008,[25] thus extending certain measures of the Prüm Treaty, including the DNA exchange system, to 27 member states. As of October 2011, however, only 12 EU member states have integrated the Council Decision into their national legislation.

Along with provisions facilitating the exchange of fingerprints and vehicle registration data, the Council Decisions incorporating Prüm into the EU framework provide for automated searches on DNA profiles by EU member states. These searches are performed through national contact points by comparing DNA samples that are present in the database, for individual cases and on a hit/no-hit basis only. In the case of a hit, the national contact point carrying out the search receives confirmation but no information whatsoever on the DNA sample found. This means that the requesting authorities are required to trigger the pre-existing bilateral or multilateral agreements on DNA exchange, to which national data protection

[23] The signatories are Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain.

[24] The Council's "lettre de saisine", sent on 1 March 2007, asked the European Parliament to deliver an opinion before 7 June 2007.

[25] Council of the European Union, Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210/1, 06.08.2008 and Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210/12, 06.08.2008.

rules apply. Individuals may turn to their national data protection supervisor to enforce their rights concerning the processing of personal data.

The Prüm system on collecting and exchanging DNA still poses difficulties regarding data protection, as genetic data is one of the most sensitive forms of personal data given the specific characteristics of DNA, which can potentially reveal additional information about the genetic code of an individual, such as health risks. Other questions concern the extent of the parliamentary and democratic oversight of the Prüm system as well as the technical feasibility of establishing national DNA databases in all EU member states.

3.2 Proceedings of the panel

As the chair of the panel, **Carlos Coelho**, Portuguese MEP from the EPP Group, introduced the speakers and presented the general context behind the Prüm Treaty and the exchange of DNA among member states. He emphasised the centrality of the principle of proportionality in this domain, and presented statistics on the risk of false matches when searching DNA databases, mainly owing to the minimum number of locations on a chromosome (loci) that are compared when conducting a search.[26] The question of whether to destroy DNA samples if they do not lead to the conviction of a criminal was also raised.

Joaquim Nunes de Almeida, Head of Unit "Police Cooperation and Access to Information", DG Home Affairs, European Commission, started his presentation by underlining the fact that DNA exchange under the Prüm system only takes place on a hit/no hit basis. This means that authorities of one member state checking the database of the 26 other member states will only receive confirmation – or not – that there is a match with another strain of DNA in one or more member(s) state(s). If the identity of the suspect or any other information is required, the requesting authorities must use the pre-existing bilateral or multilateral agreements on DNA exchange, to which data protection rules apply. As regards the state of implementation, only 12 member states[27] have transposed the Prüm Decisions into national law despite the elapsed deadline of August 2011, but no infringement mechanism is applicable by the European Commission because this is a purely intergovernmental instrument from the former third pillar. The speaker stressed that Prüm is one of the most important developments in the establishment of a common area in fighting crime.

Robert Żółkiewski, Chair of the Working Party on Information Exchange and Data Protection (DAPIX) at the EU Council, presented the views of the Polish Presidency on the challenges of data protection. After recalling the important hit/no hit approach of DNA data exchange under the Prüm system, as well as that all electronic transmissions were encrypted through a secured communication network (called 's-TESTA') to ensure full anonymity of the data, he explained that DNA samples also had to comply with EU standards as well as Interpol standards.[28] In his view, matches found by the system still need to be confirmed by experts in order to avoid errors on the hits due to fault rates intrinsic to the technology used. On the state of implementation by member states, Żółkiewski announced that according to a Prüm post-deadline questionnaire sent by the Polish Presidency to all member states, 14 of them were operational in the field of automated DNA data exchange as of November 2011. Various reasons may explain the delay in transposing the Council Decisions into national legislation – problems include IT and financial

[26] According to statistics presented by Coelho, searches of a DNA database based on 6 loci led to 86 matches, of which 57 later turned out to be false positives (66% false matches). A similar DNA search based on 7 loci led to 276 matches of which 15 later turned out to be false positives (5% false matches). The fact that the Prüm Treaty sets the minimum number of loci to be used for DNA searches to 6 is a cause for concern (laboratories typically look at 10 loci in the UK and at 13 in the US).

[27] As of October 2011, 12 member states were operational for DNA information exchange: Bulgaria, Germany, Spain, France, Luxembourg, Latvia, the Netherlands, Austria, Romania, Slovenia, Slovakia and Finland; not all of them were interconnected to the others.

[28] These are the European Standard Set (ESS) and the Interpol Standard Set of Loci (ISSOL).

difficulties, logistical, legal and political decision-making problems at the level of national parliaments as well as a shortage of human resources, especially in the case of experts who are in charge of confirming the DNA hits. The Polish Presidency was assured by the member states concerned that they would intensify their efforts.

Peter Hanel, from the Austrian Ministry of Interior and also a member of the Prüm Mobile Competence Team, recalled the main purpose of exchanging DNA among member states, which is to solve unsolved crimes. He stated that DNA samples are much more precise than names for identifying criminals operating across borders (citing as an example the different spelling of Russian names as an obstacle to identifying possible criminals by name alone). His presentation then focused on the technical details of DNA samples and the comparison of DNA strains. He pointed out that only 10% of DNA is understandable and used to identify individuals, and highlighted the difficulties posed by the necessity of comparing DNA strains with multiple other strains in order to confirm a hit and to avoid a mismatch.

3.3 Conclusion of the panel and open discussion on DNA exchange under the Prüm Decisions

As the discussant for this panel**, Rocco Bellanova,** researcher at the Vrije Universiteit Brussel and the Facultés Universitaires Saint-Louis, drew attention to the central role of technology when understanding the full implications of DNA data exchange under the Prüm Decisions, and the challenges for data protection and privacy when the technical systems involved become highly complex – as under Prüm. He also underlined the importance of ensuring democratic scrutiny for systems such as Prüm.

His intervention sparked several discussions among the audience, and questions were put to the panellists about the latest available technical developments on DNA use as well as the risk of mismatch. A 2009 news story in Germany on DNA contamination in several crime scenes[29] was used as an example showing the limits of DNA profiling. Other questions concerned the purpose of collecting DNA, with one participant explaining that in the Netherlands, DNA samples are taken from children who are simply falling in the schoolyard. Officials from the Commission and from member states reminded the audience that as an intergovernmental initiative, the Prüm data sharing remains allegedly in member states' competence – it is up to the member states to decide the kinds of crimes for which DNA samples will be used.

These questions remain at the core of the dilemmas posed by an EU framework for DNA collection and exchange. The persisting high risk of mismatch when comparing DNA strains can have consequences for the principle of the presumption of innocence, especially when police databases are no longer restricted to identifying criminals, but are now also mapping and profiling all citizens. As developed in section 2 on PNR, this becomes problematic when considering the fundamental rights of presumption of innocence and non-discrimination (Arts. 48 and 21 of the Charter of Fundamental Rights).

Discussions among participants also revealed a need to clarify how long DNA samples may be kept and when they should be destroyed, so as to prevent law enforcement agencies from keeping the DNA data of a suspect after s/he has been proven innocent by judicial proceedings. The European Court of Human Rights addressed a similar problem in its case *S. and Marper v. the United Kingdom* in 2008.[30] The Court found against the UK and for the two applicants who had requested that their DNA samples be removed from the police database.

These issues coincide with the data protection and privacy concerns that were addressed throughout the presentations. Speakers underscored the hit/no hit approach used for DNA comparisons under the Prüm

[29] See the *Spiegel online* article, "Police Fear 'Serial Killer' Was Just DNA Contamination", 26 March 2009 (http://www.spiegel.de/international/germany/0,1518,615608,00.html).

[30] See Case 30562/04, *S and Marper v. United Kingdom* [2008] ECHR 1581, 4 December 2008.

Decisions, which provides law enforcement agents with access solely to reference data and not to personal data. The application of data protection principles is thus left to national law. The argument that the hit/no hit approach and the limitation to anonymous DNA are sufficient safeguards for the protection of privacy rights can be critically challenged by the fact that a hit already reveals to a requesting body that data about a person related to the same DNA profile exists in another member state. This can already be considered sensitive information, and becomes problematic when looking at the right of consent of individuals as regards their personal data, enshrined in Art. 8 of the Charter of Fundamental Rights (see section 2 on PNR).

Finally, the question of democratic accountability and the role of the European Parliament were tackled by speakers and identified as a core concern. The European Parliament was hastily consulted in under three months, and the amendments proposed in the resolution drafted by Rapporteur Fausto Correia were not taken into account due to time constraints at the Council level.[31] The Prüm initiative did not benefit from an open discussion involving relevant actors, among them MEPs and national data protection authorities. Similarly, the absence of impact assessments on privacy and data protection raises the question of whether the Prüm Decisions, having been integrated into EU law, respect all the fundamental rights standards contained in the EU Charter of Fundamental Rights.

These open reflections and points for consideration are very important in guiding the future work of the SAPIENT project on the issues surrounding DNA collection and sharing under the Prüm Decisions. In a similar vein, MEP **Carlos Coelho** concluded the panel by stressing that the European Parliament, although not having many powers in this field, would not stop following this matter.

4. Assessing the challenges of the Terrorist Finance Tracking Programme and the EU Terrorist Finance Tracking System

4.1 Introducing the topic

The third panel focused on the Terrorist Finance Tracking Programme and the future EU Terrorist Finance Tracking System, examining the state of play of negotiations on global data transfers to third countries for the purpose of fighting terrorism, the difficulties with such global data transfers and the potential for establishing an EU equivalent.

The TFTP is an instrument set up by the US Department of Treasury after the 11 September 2001 attacks to access databases of bank transfers and transactions of suspected terrorists, in order to facilitate the prevention and investigation of terror plots and to freeze the assets of persons suspected of being terrorists or having links to terrorist organisations.

The existence of the TFTP was revealed in the US in 2006 after several newspapers published articles on a secret counter-terrorism system used by US intelligence to access financial transaction databases. The TFTP was used to access data from a Belgian-based company, SWIFT (Society for Worldwide Interbank Financial Telecommunication), which operates a financial messaging network for worldwide bank transfers and financial operations used by a vast majority of companies and organisations across the world. Gaining access to these data allegedly allowed US authorities to capture several individuals linked to terrorist groups.

[31] See R. Bellanova, "The 'Prüm Process:' The Way Forward for EU Police Cooperation and Data Exchange?", in E. Guild and F. Geyer (eds), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Farnham, UK: Ashgate, 2008, p. 207.

The TFTP presented a cause for concern in the EU as regards the risks it posed to data protection. Under the German Presidency of the Council, in 2007, a first set of agreements[32] was negotiated between the European Commission and the US Department of Treasury to clarify how EU-originating personal data would be processed under the TFTP and what data protection commitments applied.[33]

Data were requested by US authorities, in the form of subpoenas to SWIFT offices located on US territory that had access to all SWIFT transaction messages from the transatlantic zone. As of 1 January 2010, however, a change in the architecture of the SWIFT system separated the financial data stemming from the American continent on the one hand from data originating in Europe on the other, which as a consequence prevented US-based SWIFT offices from accessing European data. An EU–US agreement was therefore necessary to ensure that the TFTP would continue to have access to EU-originating financial data. An interim agreement negotiated with the European Commission in November 2009 was rejected by the European Parliament in February 2010 on the grounds that it failed to protect the privacy of EU citizens. The European Parliament had just been granted new powers by the entry into force of the Lisbon Treaty, which gave MEPs the right to veto specific international agreements.

A new EU–US TFTP agreement was thus re-negotiated and approved by the European Parliament in June 2010, and entered into force two months later. Europol, the EU law enforcement agency, has been put in charge of receiving the US requests and assessing their compliance with the agreement. Under the agreement, data are sent in bulk to the US, since SWIFT does not possess the technical capabilities to perform a targeted search for precise data. This has sparked serious criticism by several independent bodies,[34] notably on the necessity and proportionality of bulk data flows. A report on the inspection of the first six months of Europol's work by its own Joint Supervisory Body, published in 2011,[35] concluded that data protection was not ensured in light of several oral requests from the US Department of Treasury, which were too general and abstract. Nevertheless, a joint review of the implementation of the agreement, performed by experts from the European Commission and from the US Department of Treasury according to Art. 13 of the EU–US TFTP, took place in March 2011 and gave an overall positive picture of data protection compliance.[36]

Art. 11 of the EU–US TFTP agreement paves the way for a future EU TFTP mechanism, to provide the EU with a legal and technical framework for the extraction of data on EU territory. This EU TFTP has been repeatedly asked for by the European Parliament and by the Council. Originally, the purpose was to avoid the sending of bulk data to the US as a proper EU system would establish a prior filtering of data, but another reason is that EU member states are interested in the results of such a system as well. This is

[32] Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes – 'SWIFT' (2007/C 166/09), OJ C 166/18, 20.07.2007.

[33] Data protection commitments were provided by the representations of the US Department of Treasury, including limiting the purpose exclusively to the fight against terrorism, strictly forbidding any form of data mining, deleting the data after a maximum period of five years and appointing an "eminent European person", working in Washington, to verify these data protection commitments.

[34] See the Letter of the Article 29 Data Protection Working Party to Ms Melissa Hartmann, US Treasury, on the TFTP Agreement, Document D(2011) 612638, Brussels, 7 June 2011, as well as the opinion of the European Data Protection Supervisor on the TFTP II Agreement between the EU and the US, Brussels, 22 June 2010.

[35] See Europol Joint Supervisory Body, *Report on the Inspection of Europol's Implementation of the TFTP Agreement, Conducted in November 2010 by the Europol Joint Supervisory Body*, JSB/Ins. 11-07, Brussels, March 2011.

[36] See European Commission, *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program 17-18 February 2011*, Commission Staff Working Paper, SEC (2011) 438, Brussels, 30 March 2011.

expressly stated in the Commission Communication of 13 July 2011 on a European TFTS,[37] which examines the options available for its establishment. Obviously, setting up an EU TFTS gives rise to several questions in common with the debates that occurred during the negotiation of the current EU–US TFTP agreement. Among these are data protection and privacy issues, the necessity and proportionality of such a system, the possible impact of a future EU TFTS on the existing EU–US TFTP agreement, as well as the key role of Europol in verifying and authorising requests to provide data. Moreover, difficulties might arise from the simple fact that the EU and the US have different organisations listed in their Terrorist Lists.[38]

The European Parliament plays a key role in the negotiation of both the EU–US TFTP and the EU TFTS, with the legislative input by the rapporteur for both files (German MEP Alexander Alvaro, ALDE) at the centre of attention of the EU policy debate on terrorism.

4.2 Proceedings of the panel

The third and last panel of the policy meeting, chaired by **Sergio Carrera** (CEPS), was attended by high-ranking officials from Europol, the Council and the European Commission, as well as a representative of the US Mission to the EU, who offered insight on the American point of view on these issues.

Representing Europol, a central body in the current TFTP and proposed TFTS system, its Director **Rob Wainwright** emphasised that the TFTP had been an intensely debated issue within the European Parliament. MEPs approved the recent EU–US TFTP agreement in June 2010 and this agreement has been running for more than a year, which enables a first assessment of the programme. In Europol's view, the procedures established in Art. 4 of the EU–US TFTP agreement are operating properly – US requests to obtain data are processed only if they are necessary, and this necessity test is always performed by Europol, which receives an additional copy when the data is transferred. A dedicated unit was specially created to deal with the TFTP within Europol's secretariat. Wainwright recognised the concerns expressed in the opinions of the Article 29 Working Party and of the European Data Protection Supervisor[39] about the sensitivity of data transfers, but stressed that in taking on this new role, Europol had managed these activities with high standards. According to Wainwright, the NGO Statewatch had even praised Europol's work during a high-level conference on data protection in Warsaw in September 2011. He contended that the benefits in terms of security gains are clearly measurable: thanks to this agreement, investigations on the terrorist attack in Norway in July 2011 were facilitated and US financial data on the suspect were transferred to Norwegian authorities. Nevertheless, fundamental issues remain with Art. 4 of the agreement and its ambiguity on how US requests should be treated. The possibility of establishing a TFTS at the EU level was seen as a positive initiative in Wainwright's opinion – he welcomed the Commission's Communication and the strong data security of the proposed system.

The EU Counter-Terrorism Coordinator, **Gilles de Kerchove,** started his presentation by highlighting the added value of an EU TFTS. He underscored the counter-terrorism relevance of such a system and pointed out how effective the TFTP had been for the prevention and investigation of terrorist attacks – citing once again the example of the Norway attack in July 2011. He also referred to reports such as those of French judge Jean-Louis Bruguière,[40] which emphasise the usefulness of the TFTP. The speaker welcomed the Commission's Communication on the EU TFTS of 13 July 2011, which adopts a four-step approach: the selection of messages, the management of the database, the extraction of the messages and

[37] See European Commission, Communication on a European terrorist finance tracking system: Available options, COM(2011) 429 final, Brussels, 13 July 2011.

[38] One example being Hizbullah in Lebanon, considered a terrorist organisation by the US but not by the EU.

[39] See note 34.

[40] The first Bruguière report on the processing of EU originating personal data by the US Treasury Department for counter-terrorism purposes was issued in December 2008 and the second in January 2010.

the need to control the system. He indicated that it was up to the member states to decide which agency or agencies should be tasked with these four functions (Europol, Eurojust, the future IT Agency,[41] Financial Intelligence Units' network, etc.), but he pointed out that Europol should play a role at two levels:

- At a strategic level, Europol – as it currently does when analysing US requests – is well equipped to collect requests from member states and to examine whether they meet the requirements of the system.
- At a more operational level, Europol could be authorised to quarry the databases for its own need and to execute US requests.

As for the impact of the new TFTS on the TFTP, while welcoming increased data protection safeguards de Kerchove expressed two concerns. One is ensuring that the TFTS is not less effective than the TFTP, and another is ensuring complementarity between the TFTS and the TFTP. He also called for the establishment of criminal sanctions against law enforcement agents who violate data protection provisions.

Dick Heimans, Head of Sector in the unit "Crisis Management and Fight against Terrorism" in DG Home Affairs of the European Commission, presented the Communication of the Commission on the EU TFTS and the steps leading to it. After many debates on the very sensitive issue of the EU–US TFTP agreement, the European Parliament finally agreed to sign it under the condition that the Commission should start working on the establishment of a similar EU-wide system. A consultative firm was asked to deliver a study on the matter, which led to the drafting of the Commission Communication. This document describes the functions of an effective TFTS and the added value needed, as well as the safeguards that must be provided. The costs of such a system – whether it should be borne by the Commission or by member states – and the scope of application are pending issues that still need to be discussed. On the question of data protection, inspiration is drawn from the existing TFTP agreement with a clear will not to go below data protection standards that already exist in this agreement. Heimans concluded his presentation with the hope that the debate between the Council and Parliament would inspire more ideas, while at the same time acknowledging that the level of support for the EU TFTS was stronger in member states than in the European Parliament.

Sergio Carrera reacted to the presentations by raising the question of the compatibility of this new police model being established by the EU with the rights enshrined in the EU Charter of Fundamental Rights. He highlighted problems of legal and democratic accountability in the working practices of Europol, citing a recent CEPS study for the European Parliament.[42]

As a legal counsellor working with the US Mission to the EU, **Kenneth Propp** outlined three aspects that are relevant to the discussions of this panel:

- First is the importance of the EU–US TFTP agreement, which has increased the protection for EU and US citizens through the conduct of effective investigations on major terror plots. Examples include the Norway attacks (2011), the Nigerian Independence Day car bombings (2010), the hijacking actions of the Al-Shabaab militia (2009), the Jakarta hotel attacks (2009), the Mumbai attacks (2008), a foiled plot by the Islamic Jihad Union to attack sites in Germany (2007), the London bombings (2005) and the Madrid train bombings (2004).

[41] The future IT Agency, which is due to start operations at the end of 2012, will be responsible for the operational management of large-scale IT systems in the area of home affairs (EURODAC, the Visa Information System (VIS) and the second-generation Schengen Information System (SIS II)), and other systems in the future (such as the TFTS, if established). The main seat of the Agency will be in Tallinn. (See http://ec.europa.eu/home-affairs/policies/borders/borders_it_agency_en.htm for more information.)

[42] E. Guild, S. Carrera, L. Den Hertog and J. Parkin, *Implementation of the EU Charter of Fundamental Rights and its Impact on EU Home Affairs Agencies*, Study for the Directorate-General for Internal Policies of the European Parliament, CEPS, Brussels, 2011.

- Second is the large array of safeguards provided in the agreement. Notable in this respect are data storage in a stand-alone and secured computer, very limited possibilities to search data (only for counter-terrorism measures and only if a TFTP investigator has separate leads), an independent overseer from the EU who is situated in Washington and who can block the search if s/he has doubts about the respect of safeguards, and the existence of periodic joint reviews of the implementation of the agreement. Personal protection is also available to citizens, both EU and US nationals, who have the possibility to obtain information about data that concern them. To date, there have not been any administrative or judicial complaints brought in relation to the 2010 TFTP agreement.
- And third is the EU's decision to set up its own equivalent system of TFTP. This move is supported by the US Department of Treasury, especially given the existing clause in Art. 11 of the 2010 agreement providing that US authorities shall cooperate and provide assistance and advice to the EU if an EU TFTS is established. Propp highlighted that the TFTS was an EU debate and he pointed to the successes achieved by EU–US cooperation in the field of counter-terrorism.

4.3 Conclusion of the panel and open discussion on the EU–US TFTP agreement and the establishment of an EU TFTS

Elspeth Guild, Senior Associate Research Fellow at CEPS, took up the role of discussant for this panel. She made two observations that are indicative of the general state of mind among policy-makers in this debate.

First, she argued that the real underlying subject matter of the panel discussion had become lost. She reminded participants that the TFTP involved the exchange of data concerning financial transactions and the private bank history of individuals, which covers an extraordinarily wide range of information about people's lives and which should provoke real concerns over its impacts on privacy.

Second, she noted that the only person mentioning the Charter of Fundamental Rights in this panel was Sergio Carrera. The Charter is all the more important to take into account as it now contains basic human rights that were derived from secondary law and principles before the entry into force of the Lisbon Treaty.

Guild went on to raise very important questions that in her view require further debate:

- The issue of consent by an individual is central – if EU authorities interfere with the personal data of a person, this person has to give his or her consent. This right of consent, as presented above, is enshrined in the now legally-binding EU Charter of Fundamental Rights. Instruments such as the TFTP displace that consent. Therefore, if EU citizens have to give up their right to privacy for increased security, there needs to be a consistent and coherent rationale behind this. Furthermore, safeguards have to be provided in the form of a purpose limitation and a complete array of controls. On these controls, the question that needs to be raised is whether the fragmentation of monitoring is justified – a multiplication of supervisory bodies that check the respect of data protection safeguards may decrease the level of protection.
- The idea to put in place criminal sanctions against law enforcement agents who violate data protection provisions, as suggested by Gilles de Kerchove, incorrectly addresses the problem, as the objective is to prevent misuse rather than punish the agents who abused the system. By the time the damage is done, sanctions seem unnecessary.
- Finally, Guild examined the issue of the displacement of responsibility. It is very difficult to know the operational aspect of the system in the US and even more difficult to control and monitor data protection across the Atlantic. The joint review, which has already taken place once and should take place again in 2012, has been highly criticised by the European Parliament.

5. Final remarks

The conclusion of the panel on the TFTP and TFTS highlighted several challenges that are connected to those pointed out by the other panels on PNR and DNA exchange under the Prüm Decisions. By focusing on the three main case studies taking centre stage of the debate at the EU level, this policy meeting, organised by the European Parliament's Privacy Platform, CEPS and supported by the SAPIENT Research Project, gathered a range of insights from relevant stakeholders, through which the central controversies have been identified.

The key horizontal issue across all three case studies is the respect of fundamental rights as recognised in the EU Charter, which was given a binding legal effect equal to the Treaties after the entry into force of the Lisbon Treaty in December 2009. The protection of personal data, enshrined in Art. 8 (from which the notion of individual consent stems), the right to non-discrimination (Art. 21, which is at risk when law enforcement authorities use the collected bulk data for profiling purposes) and the right to presumption of innocence (Art. 48) are all crucial elements that need to be taken into account in the current policy debates taking place in the AFSJ. The SAPIENT project will continue to work on these issues under the general assumption that the Charter of Fundamental Rights is not only a catalogue of rights, but also a practical tool to make the actual provision of fundamental rights to the individual citizen a reality applicable to EU policy-making processes.

Appendix 1. Programme of the policy meeting

09.00 – 09.30 Welcome

- **Sophie In 't Veld**, MEP (ALDE, Netherlands), Chair of the Privacy Platform, European Parliament
- **Sergio Carrera**, Senior Research Fellow & Head of Justice and Home Affairs Programme, Centre for European Policy Studies
- **Michael Friedewald**, Fraunhofer Institute, Coordinator of the SAPIENT project
- **Bruno Mastantuono**, Legal Adviser, Research Executive Agency, European Commission

09.30 – 11.30 Panel I: Assessing the challenges of the EU Passenger Name Record system

Chair:

- **Timothy Kirkhope**, MEP, European Parliament

Panellists:

- **Jan Philipp Albrecht,** MEP (Greens, Germany), European Parliament
- **Brendan Nelson,** Ambassador, Australian Mission to the EU
- **Filip Jasiński,** JHA Counsellor, Permanent Representation of Poland to the EU
- **Joaquim Nunes de Almeida**, Head of Unit "Police Cooperation and Access to Information", DG Home Affairs, European Commission
- **Margreet Lommerts**, Manager, Association of European Airlines

Discussant:

- **David Wright**, Managing Partner and Co-Founder of Trilateral Research and Consulting

Open discussion

11.30 – 12.30 Lunch break

12.30 – 14.30 Privacy Platform: More surveillance, more security? The landscape of surveillance in Europe and challenges to data protection and privacy

Chair:

- **Sophie In 't Veld**, MEP (ALDE, Netherlands), Chair of the Privacy Platform, European Parliament

Panellists:

- **Didier Bigo**, Professor, King's College London/Sciences Po
- **Wil van Gemert**, Director, General Intelligence and Security Service of the Netherlands
- **Quirine Eijkman**, Senior Researcher and Lecturer, Centre for Terrorism and Counter Terrorism (CTC), Leiden University

Open discussion

14.30 – 14.45 Coffee break

14.45 – 16.00 Panel II: Assessing the challenges of DNA collection and sharing under the Prüm Decisions

Chair:

- **Carlos Coelho**, MEP (EPP, Portugal), European Parliament

Panellists:

- **Joaquim Nunes de Almeida**, Head of Unit "Police Cooperation and Access to Information", DG Home Affairs, European Commission
- **Robert Żółkiewski,** Chair of the Working Party on Information Exchange and Data Protection (DAPIX), EU Council
- **Peter Hanel**, Senior Project Manager, Ministry of Interior of Austria & Prüm Mobile Competence Team

Discussant:

- **Rocco Bellanova**, Researcher, Vrije Universiteit Brussel & Facultés Universitaires Saint-Louis

Open discussion

16.00 – 16.15 Coffee break

16.15 – 17.30 Panel III: Assessing the challenges of the Terrorist Finance Tracking Programme and the EU Terrorist Finance Tracking System

Chair:

- **Sergio Carrera**, Centre for European Policy Studies

Panellists:

- **Rob Wainwright**, Director, Europol
- **Gilles de Kerchove**, EU Counter-Terrorism Coordinator, EU Council
- **Dick Heimans,** Head of Sector in the unit **"**Crisis Management and Fight Against Terrorism", DG Home Affairs, European Commission
- **Kenneth Propp**, Legal Counsellor, US Mission to the EU

Discussant:

- **Elspeth Guild,** Senior Associate Research Fellow, Centre for European Policy Studies

Appendix 2. Minutes of the Privacy Platform meeting from 12.30 to 14.30

Privacy Platform: More surveillance, more security? The landscape of surveillance in Europe and challenges to data protection and privacy

Chair:

- **Sophie In 't Veld**, MEP (ALDE, Netherlands), Chair of the Privacy Platform, European Parliament

Panellists:

- **Didier Bigo**, Professor, King's College London/Sciences Po
- **Wil van Gemert**, Director, General Intelligence and Security Service of the Netherlands
- **Quirine Eijkman**, Senior Researcher and Lecturer, Centre for Terrorism and Counter Terrorism (CTC), Leiden University

This meeting took place from 12.30 to 14.00 and focused more generally on the challenges posed by security policies and intelligence services for the privacy of citizens. MEP **Sophie In 't Veld** (ALDE, Netherlands), Chair of the Privacy Platform, welcomed the three speakers: **Didier Bigo**, Professor from the King's College of London and Sciences Po Paris, **Wil Van Gemert**, Director of the IEVD – Intelligence and Security Service of the Netherlands, and **Quirine Eijkman**, Senior Researcher at the Centre for Terrorism and Counter-Terrorism of Leiden University.

Didier Bigo started his presentation by asking what 'more security' meant: Is it understood as a 'right to security'? Surveillance practices allow member states to gather and analyse data for the purpose of profiling individuals, but as he recalled, 78% of individuals who are arrested are found not guilty. Bigo expressed his concerns about the evolution of the logic of prevention into one of suspicion, as well as the function creep from personal safety to state security. One example of the worrying trend in considering the global society more important than the individual was the introduction of heat scanners at the US airport in San Diego, which were supposed to detect the temperature variations of passengers. A high temperature indicated a state of fear and thus led to the assumption that the passenger was a possible terrorist. As Bigo noted, the only results of this action were the increased arrests of pregnant women. In conclusion, he stressed the need for impact assessments prior to introducing new surveillance systems.

Wil Van Gemert briefly presented the work of the Dutch Intelligence Service and assured the audience that its powers were very limited, as his organisation constantly needed a clear mandate from various supervisory bodies. He answered positively to the main question of this meeting: Does more surveillance lead to more security? He explained that balanced surveillance always leads to more security. In his view, the security paradox lies in the need for governments to protect citizens while at the same time prevent the misuse of their personal information. This is possible through a strong legislative framework with checks and balances and an evaluation of threats on a case-by-case basis. Van Gemert recalled the necessity and proportionality tests, which make sure that each action taken is the best available in terms of security and privacy.

Sophie In 't Veld immediately reacted and criticised Van Gemert's use of the 'balance metaphor', which implies the idea of a balance between privacy and security. Security being a collective issue and privacy an individual one, she wondered how it was even possible to compare and to balance the two, as the obvious result would be that the individual would lose against society.

Quirine Eijkman presented the challenges that arise through more and more pervasive surveillance activities. She defined the notion of privacy as the right to be left alone, and underlined that checks and balances provided by decision-makers allowed for individuals to complain before judicial bodies. In her view, more transparency is needed on surveillance activities so that citizens can be aware of them and help out. She concluded her intervention by highlighting the main dilemma in security issues today: the difference between law in theory and law in practice. More specifically, citizens have confidence in the law, but less confidence in bureaucracy.

The **discussion** that followed focused on certain specific issues, such as the impossibility of knowing for sure whether surveillance is really efficient, the context of counter-terrorism in Europe, the use of the 'balance metaphor', the question of accountability of law enforcement agencies and the global shift from intelligence to law enforcement that is currently taking place. Questions by participants were primarily aimed at trying to understand the difference between data collection by private companies for advertising purposes and data collection by governments for security purposes. The question of trust in governments was also raised; **Sophie In 't Veld** concluded the meeting on this issue, saying that one should not have the illusion that any government is immune to abuses and authoritarianism. She maintained that proper checks and balances are the essence of democracy.

Addendum: Sophie In 't Veld's report on the main achievements and future challenges of the EU's counter-terrorism policy was adopted by the European Parliament during its plenary session on 14 December 2011.[43]

[43] See European Parliament, Resolution of 14 December 2011 on the EU Counter-Terrorism Policy: Main achievements and future challenges (2010/2311(INI)) (http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0577&language=EN&ring=A7-2011-0286).