Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between Human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable 3.1: Draft analysis of privacy and security policy documents in the EU and US

Authors:	Gabriela Bodea, Noor Huijboom, Sander van Oort, Merel Ooms, Bas van Schoonhoven, Tom Bakker, Livia Teernstra (TNO); Rachel L. Finn, David Bernard-Wills, David Wright (Trilateral); Charles D. Raab (University of Edinburgh)

Dissemination level:	Restricted to a group specified by the consortium
Deliverable type:	Report
Version:	1.0
Due date:	30 January 2013
Submission date:	28 March 2013

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

This document was developed within the PRISMS project (see http://prismsproject.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 (Fraunhofer ISI), co-ordinator,
- Trilateral Research & Consulting LLP,
- Dutch Organization for Applied Scientific Research (TNO),
- Vrije Universiteit Brussel (VUB),
- University of Edinburgh (UEdin),
- Eőtvős Károly Policy Institute (EKINT),
- Hogeschool Zuyd and
- Market & Opinion Research International Limited (Ipsos-MORI)

This document may be freely used, copied, and distributed provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The PRISMS partners shall take no liability for the completeness, correctness or fitness for use. This document is subject to updates, revisions, and extensions by the PRISMS consortium. Address questions and comments to: Michael.Friedewald@isi.fraunhofer.de

Document history

Version	Date	Changes
1.0	28 March 2013	

Reading guide

Deliverable 3.1 is the first deliverable of work package 3 (WP3) Policy assessment of security and privacy of the FP7 project PRISMS. It consists of two parts, following the division of tasks in the WP3 research plan, namely:

- Part I entitled "An Overview of Privacy and Security Policy Documents in the EU, six Member States and the United State", which presents the results of research in task 3.1,
- Part II entitled "A discourse analysis of selected privacy and security policy documents in the EU" which presents the results of research in task 3.2, and
- A supplement with bibliographic information about the policy documents analyzed for this deliverable.

CONTENTS

EXECUTIVE SUMMARY viii

PART ONE:
AN OVERVIEW OF PRIVACY AND SECURITY POLICY DOCUMENTS IN THE EU, SIX MEMBER STATES AND THE UNITED STATE

1 INTRODUCTION 3

1.1 Objectives 3

1.2 Context 4

1.3 Criteria for selecting documents 7

1.3.1 Defining policy documents 8
1.3.2 Compiling the long list of policy documents 9
1.3.3 Short analysis 11

2 SUMMARY OF POLICY DOCUMENTS 12

2.1 International organisations 12

2.2 European security and privacy policy documents 12

2.3 Other European policies 13

2.4 United Kingdom security and privacy policy documents 13

2.5 Netherlands security and privacy policy documents 14

2.6 France security and privacy documents 15

2.7 Italy security and privacy policy documents 15

2.8 Germany security and privacy policy documents 16

2.9 Romania security and privacy policy documents 17

2.10 USA security and privacy policy documents 18

2.11 Summary 18

3 HORIZONTAL ANALYSIS 20

3.1 Introduction 20

3.2 Method 21

3.3 Issue analysis by context 21

3.3.1 United Kingdom 22
3.3.2 Netherlands 25
3.3.3 France 27
3.3.4 Italy 31
3.3.5 Germany 32
3.3.6 Romania 35
3.3.7 United States of America 37

3.3.8 The European Union *39*
3.4 Comparative Analysis and Discussion **48**
3.4.1 Security *48*
3.4.2 Privacy, data protection and surveillance *51*
3.4.3 Chronology *58*
4 CONCLUSION **61**
5 INPUT TO THE PRISMS SURVEY **63**

PART TWO:
A DISCOURSE ANALYSIS OF SELECTED PRIVACY AND SECURITY POLICY DOCUMENTS IN THE EU

6 DISCOURSE ANALYSIS – INTRODUCTION AND METHODOLOGY **69**
6.1 Introduction to and review of discourse analysis methodologies **69**
6.1.1 Michel Foucault and the "archaeological" approach *70*
6.1.2 Methods of discourse analysis based on Foucault *74*
6.1.3 Pêcheux's instrument of automatic discourse analysis *75*
6.1.4 Methodologies based on Pêcheux *77*
6.2 Selecting a discourse analysis methodology **78**
6.3 Discourse analysis methodology **78**
7 PRIVACY AND SECURITY DISCOURSES IN SELECTED UK POLICY DOCUMENTS **83**
7.1 Introduction **83**
7.1.1 Methodology *83*
7.2 Key discourses **84**
7.2.1 The surveillance society *84*
7.2.2 Finding a proportionate balance between security and privacy *85*
7.2.3 Surveillance, security and their associated technologies have social benefits *85*
7.2.4 Supporting the security industry *86*
7.3 Key actors and word combinations **87**
7.4 Public interest **90**
7.5 Description of security and privacy discourses **92**
7.5.1 The surveillance society *92*
7.5.2 Finding a proportionate balance between security and privacy *97*
7.5.3 Surveillance, security and their associated technologies have social benefits *98*
7.5.4 Supporting the UK security industry *100*
7.6 General conclusions, reflections and hypotheses **102**
8 PRIVACY AND SECURITY DISCOURSES IN SELECTED DUTCH POLICY DOCUMENTS **103**
8.1.1 Methodology *103*
8.2 Key discourses **104**

8.3 Key actors and word combinations 111
8.4 Public interest 111
8.4.1 Description of critical events and the security and privacy discourse 113
8.5 General conclusions and reflections 125
8.6 Hypotheses for the PRISMS Survey 126
9 PRIVACY AND SECURITY DISCOURSES IN SELECT POLICY DOCUMENTS OF THE INSTITUTIONS OF THE EUROPEAN UNION 129
9.1 Introduction 129
9.2 Methodology 129
9.3 Key discourses 130
9.4 Key actors and word combinations 137
9.5 Public interest 137
9.6 Narrative description of the security and privacy discourse 142
9.7 General conclusions, reflections and hypotheses 153
9.8 Hypotheses for the PRISMS Survey 154
10 REFERENCES 155
10.1 Academic Literature 155
10.2 News Reports 157
10.3 Policy Documents 157

EXECUTIVE SUMMARY

The current document, deliverable D 3.1, is the first deliverable of work package 3 (WP3) Policy assessment of security and privacy of the FP7 project PRISMS. It is a draft report presenting an overview of policy documents of the EU and a select sample of Member States (the Netherlands, France, Germany, Italy, Romania and the UK), as well as a discourse analysis of how specific concepts related to security and privacy (technologies) are used; how they frame perceptions, ambitions and expectations concerning security and privacy; and how this correlates with citizens' perceptions, priorities and understandings regarding privacy and security. The document presents the results of study in two tasks of WP3, namely Task 3.1 Overview and first analysis of relevant policy documents and Task 3.2 Discourse analysis of policy documents. The deliverable follows the same structure as the research tasks and is thus divided in two parts: Part I entitled *Security and privacy policy in 21st Century Europe* and Part II entitled *A discourse analysis of selected privacy and security policy documents in the EU.*

The general aim of the study for this report was to gain a better understanding of how policy-makers in Europe conceptualise "security" and privacy" in different contexts (national, international, supra-national) and to capture how security and privacy policies are developed in distinct policy contexts, both on the European and Member State levels. It does so by selecting relevant policy documents of European and Member State as well as policy documents from international organisations and the USA and by comparing and contrasting them to one another, in order to identify commonalities and differences between these contexts. Furthermore, insights from WP3 will be used to shape the PRISMS survey. In their turn, the survey findings will be used to examine further how policy decisions in the field of security and privacy correlates with citizens' perceptions, priorities and understandings. Ultimately, all insights will help shape the decision-support system.

Part I *Security and privacy policy in 21st Century Europe*

The first part of this report produced an inventory of the most relevant policy documents from 2000 onwards within international organisations, the European Union, selected Member States (i.e. the Netherlands, France, Germany, Italy, Romania and the UK) and the USA related to security, privacy and surveillance policy. The result, a "long list" of policy documents (Annex A), provides information about the key issues of privacy, security, data protection and surveillance and potential differences and similarities in the way policy makers in different countries have characterised these issues. From the long list of documents key policy documents from each context were selected. Subsequently these documents were subjected to a "short analysis" to identify key themes within the documents (Annex B).

Horizontal analysis - A more in-depth assessment (chapter 3) of a relevant "set" of policy documents referring to the security and privacy policies of the Commission and selected Member States enabled a better understanding of the manner in which concepts such as "security" and "privacy" are framed in a European policy context, what differences exist between countries and over time, and what dominant approaches frame current discourse and policy activities. This was achieved by means of a horizontal analysis (chapter 3). The horizontal analysis provides a further opportunity to consider how and whether discourses by policy makers influence citizens' priorities and perceptions, as well as how notions of privacy and security might be successfully integrated into a decision support system that protects and provides both privacy and security. Examined closely and compared, the documents yield a

number of insights and hypotheses which will be tested by means of a survey in work package eight. Drawing upon the stated motivations in the analysed texts, there are *six broad categories of drivers* for the compilation and publication of security and privacy texts the horizontal analysis identified. These include: 1) responses to legislative requirements, processes or consultation requests, 2) responses to change security contexts or the emergence of apparent new security threats, 3) responses to particular events or identified public concern, 4) reminders or re-affirmations of principles and clarification of laws, 5) the results of scrutiny, inquiry or evaluation of existing policies and programmes, and 6) responses to increased surveillance practices and technological developments. A first interpretation of the horizontal analysis across the corpus of documents selected would suggest a number of preliminary conclusions. For example, it would appear to emerge that *concepts of security* are heterogeneous across different countries, and across different actors within countries. There are multiple, divergent framings of the concept of security, across European governments, and between different policy actors within individual countries. However, many of these concepts are more expansive than the most traditional concepts of national security, and there is an indication that the scope of security has expanded across all countries in the analysis as more areas of social life are represented as contributing towards security. There would also appear to be a relatively stable core of what are considered to be security threats, although with some alterations of priority and some interests specific to individual states. The texts generally value information exchange between security agencies as an important contributor to security. Economic costs of security are rarely if ever mentioned, even in the context of European economic crisis. The concept of national security is expanding in security policy documents across many countries to include information security, often under the rhetoric of cyber security, critical information infrastructure or cybercrime. In a manner similar to the framing of security, these documents provide ways of framing the problematic of privacy, data protection and surveillance and the appropriate policy, legal, social and economic responses to these issues. The texts provide a perspective on how these issues are represented, as issues, within policy documents. The *combination of privacy and security* documents in this analysis also allows us to reflect upon the way the relationship between the related concepts and practices is presented in public texts. For example, the current EU position on the conflict between privacy and security appears to be that security and fundamental rights (including privacy) are complementary, not in contradiction. Fundamental rights and freedoms are to be "respected" more than "balanced". The language of "balancing" of privacy and security is however still used at national levels. There are variations across the analysed documents in the representation and use of the concept of *surveillance*. Different countries have different sets of *privacy* "threats" – that is, those risks to privacy that are considered to be the most threatening in a particular context. There is a wide and diverse range of privacy problems identified through the documents. These are often shared between countries, but particular issues appear to have increased salience in some countries in comparison to others. There is also a strong thread of technological determinism running through these texts, in which developments in technology have brought about both increased insecurity, but also risks to privacy and data protection. When threats to data protection or privacy arise, they are often portrayed as coming from information technology (such as "databases") or from information sharing practices, more than from "surveillance" as a phenomenon. Furthermore, there is broad agreement across the texts on the broad principles involved in privacy, data protection and surveillance. These principles include proportionality, accountability, transparency, trust, consent, and the rights of the data subject. The analysed documents indicate also that there may be differences in the solutions and responses put forward in response to particular problems of privacy, data protection and surveillance. Few documents were highly supportive or reliant upon technological responses to privacy problems, although as discussed in the

previous section on information security, information security was seen as highly important. There were occasional mentions of privacy enhancing technologies and introducing privacy by design, but these were presented as solutions much less frequently than legal, regulatory and compliance responses across all countries. These texts also feature representations of the interactions between countries, and between countries and international organisations. For the EU Member States the EU is a significant actor in privacy and data protection. Several texts provide representations of these relationships. Across most of the documents the *representation of the EU* is nuanced. It is both a (necessary) source of security, and a support for privacy and data protection rights, but also brings with it membership costs and its measures can have impacts upon both security and the exercise of rights. In general external influences upon policy process are downplayed. The non-US documents do not describe any post-9/11 security or surveillance measures as being driven by US expectations regarding speedy security cooperation, but rather frame these measures as a required response to the revealed security problematic of terrorism or global instability. Recent concerns about industry lobbying around data protection reforms are not reflected in these documents. It is possible to suggest that 9/11 preceded a range of texts that directly responded to the attacks and to the security measures brought in response. Also, if we look at the long-list documents from the European Commission, Council and Parliament, there are generally more documents focused on security than on privacy, apart from in 2012.

A *general hypothesis* emerging from the horizontal analysis is that there will be significant differences between the ways in which members of the public in different Member States understand privacy and security. Different countries appear to focus on different aspects of security. Furthermore, different countries appear to have different relative levels of concern about issues such as privacy, data protection and surveillance.

Part II ***A discourse analysis of selected privacy and security policy documents in the EU***

The preliminary conclusions and hypotheses formulated by the horizontal analysis and briefly presented above appear to be supported by the findings of the discourse analysis performed in Part II of this report. This part of the report is dedicated to a discourse analysis of selected Dutch, British and EU policy documents. Together with the results of the horizontal analysis, the discourse analysis should offer a more detailed understanding of exactly how concepts of privacy and security are discussed, contested and negotiated within specific (inter)national contexts. The aim of this multi-dimensional methodology is to enable PRISMS to understand the manner in which concepts such as security and privacy are framed in policy circles, what differences exist and what dominant approaches frame current discourse and policy activities.

Discourse analysis – also referred to as 'critical analysis' – can be understood as a scientific approach (a manner of deconstructive reading) to analysing (written, vocal or sing) language use or any relevant communicative event. The analysis enables access to the ontological and epistemological assumptions behind a (legal) statement, strategy, policy or programme. Moreover, discourse analysis reveals the motivations, ideas and interests behind a text, statement or conversation. For our discourse analysis we have adopted and adapted the methodology proposed by Maarten Hajer and tested it first on a limited selection of policy documents (the UK case, chapter 2) so well as on a more extensive selection of policy and other types of documents providing context to the policy documents (the case of the Netherlands and the case of the EU institutions, chapters 3 and 4 respectively). The methodology will be refined further in part two of our research and input from interviews will

be added, resulting in the final deliverable 3.2. A summary of the findings of the discourse analysis is presented below.

For the *UK case* (chapter 2), the discourse analysis examines how select UK policy documents, and thus some British policy-makers, conceptualise security and privacy. It is based on an examination of five recent UK policy documents: a 2006 report by the Surveillance Studies Network, entitled *Report on the Surveillance Society*; a 2008 report from the House of Commons Home Affairs Select Committee, entitled *A Surveillance Society?*; a 2009 report from the House of Lords Constitutional Committee, entitled *Surveillance, Citizens and the State*; a Joint Committee on Human Rights examination of the proposed Protection of Freedoms Bill from 2011; and, a Ministry of Defence *White Paper* on national security from 2012. The analysis of these five UK policy documents identified four key discourses: "The surveillance society"; Finding a proportionate balance between security and privacy; Surveillance, security and their associated technologies have social benefits; and, Supporting the security industry. Although the analysis is based on a very small sample of UK policy documents, they reveal that British policy appears to be more concerned than other countries with the relationship between surveillance and privacy, the benefits that surveillance technologies can bring to society and the provision of security using new technologies. However, like other countries, UK discourse primarily relies upon the trope of providing a "balance" between security and privacy, which are often constructed as oppositional. Different actors appear to be aligned with particular discourses, in that government actors, by and large, seek to capture the benefits of security technologies and balance these against privacy, while academic and civil society representatives support foregrounding privacy and human rights considerations, possibly at the expense of new surveillance and security programmes.

For the analysis of the discourse on privacy and security in *the Netherlands* (chapter 3), we have chosen to use a more extensive selection of policy documents than for the UK. Additionally, we tried to include also other types of documents and sources of information likely to add more context to both the discourse(s) and the analysis thereof. The purpose of the slightly different approach in analysing the situation in the Netherlands as compared to that in the UK was to test the methodology we had chosen, its strengths and its limitations.
The framing of security and privacy by media and politicians in the Netherlands appeard to have been highly influenced by various critical events, both national and international. In the aftermath of the attacks of 9/11 in the United States of America, and the Theo van Gogh assassination in the Netherland, strong statements were made about (the balance between) security and privacy in various political debates and in the media. Often times, these discourses described security and privacy in terms of a trade-off, with security generally given precedence over privacy. Various incidents (e.g. the assassination of Pim Fortuyn, rowdy youths causing neighbourhood nuisance) were seen and presented through a "terrorism" lens (i.e. described in strong terms such as "terrorist attack" and "street terror"). Terrorism functioned as an emblematic issue; it was an emblem for many forms of (potential) disruptions of the Dutch society. In addition, it seemed that privacy and security were two separate discourses and that only in some rare instances an integrated debate about these subjects took place. A break with this discursive tradition seem to emerge around the year 2007 when several actors pointed to the perceived misbalance between privacy and security. From that moment on, the discourses on privacy and security appear to converge and privacy and security seem to undergo a conceptual shift. Whereas in the wake of 9/11 and the Theo van Gogh assassination, privacy and security were perceived to be rival values, now these subjects were increasingly mentioned as matching and reciprocally reinforcing values. In

addition, security was increasingly mentioned as a precondition for privacy. From this perspective, (technological) security measures were recommended in order to protect citizens' (online) privacy. Over the past few years, the discourse focused strongly on specific security and privacy topics, such as online data protection and cybercrime.

The EU discourse analysis is presented in the final chapter of this report, chapter 4. One preliminary conclusion of the analysis is that in the past decade, the EU security and privacy discourse has been highly influenced by the 9/11 attacks in the United-States of America (US). In the aftermath of the 9/11 terrorist attacks, the US played a dominant role in the framing of security issues which influenced strongly policies adopted in the EU. The documents examined would indicate that the European Commission found itself several times in the difficult position (to mediate) between the US and the European Parliament (EP) in matters of international cooperation in the fight against terrorism. One of the key storylines emerging from the discourse analysis of documents of the European Parliament is that European citizens' rights are likely to be violated by the US anti-terrorism measures as these measures would provide the US with disproportionate access to (sensitive) personal data. The dominance of the US in the security and privacy discourse is further revealed by several EU policy documents and EU-US agreements in which multiple metaphors and statements of the US administration(s) are adopted and reproduced in one form or another. In the past years however, the EU discourse on privacy and security appears to have become more balanced with more room for a more rational and in-depth discussion on the security and privacy balance. The same chapter on the EU discourse analysis includes a brief preliminary cross-country analysis. This will be developed further in the final deliverable D3.2. Similarly to the previous two chapters, the chapter on the EU discourse analysis formulates a number of hypotheses to be tested during the pan-European survey undertaken in work package eight.

Final remarks. Whereas the current deliverable includes only preliminary conclusions with each of the main chapters, the final deliverable D 3.2 will finalize the analysis, take into account any new relevant policy developments, conduct a round of expert interviews meant to validate the results and formulate general conclusions regarding the framing of the privacy and security debate from a policy perspective.

PART ONE

An Overview of Privacy and Security Policy Documents in the EU, six Member States and the United State

1 INTRODUCTION

This report presents an overview of various international, European and Member State policy documents, their contexts and the main perspectives they cover in order to gain a better understanding of how policy-makers in Europe conceptualise "security" and privacy". In this overview, European and Member State policy documents are compared and contrasted to one another, as well as to policy documents from International organisations and the USA in order to identify commonalities and differences between these contexts.

A continuous debate about the objectives of European security policy and safeguarding human rights (amongst others, the right to privacy) is apparent in these security policies. Over the past 10 to 20 years, the stock of surveillance-related technological resources (e.g., biometrics, DNA profiling, etc.) has steadily grown and has influenced the security and policy agenda. The policy documents reveal how security and privacy technologies are perceived by policy-makers, how they reflect certain expectations and ambitions. Reciprocally, the policy agenda also influences the development and deployment of specific technologies and practices, such as camera surveillance, biometrics and DNA profiling. These security and privacy policies are also interrelated with other policy domains such as transportation, immigration, health and immigration policies. Policies concerning security and privacy also integrate other key concepts, including trust, citizens, terrorism, and criminal behaviour. Reflecting social and human-rights values such as security and privacy, they focus upon these key concepts, and they relate them in ways that make assumptions about how technology might help in overcoming certain societal needs and challenges.

An analysis of the meanings, expectations and ambitions with regard to the fulfilment of policy ambitions and the use of security/privacy technologies will assist in developing two key aspects of the PRISMS project. First, the analysis will enable PRISMS to use the Europe-wide survey to consider whether policy-makers' constructions and concerns mirror those of citizens, and whether they are consistent or divergent across different national contexts. Second, the policy analysis combined with the survey findings will contribute to a better design for the PRISMS decision support system that will assist decision-makers in evaluating security and privacy technologies and practices before they are procured or deployed.

1.1 OBJECTIVES

The purpose of this review of privacy and security documents at the international level, EU level, in six Member States and the USA is twofold. First, the PRISMS project wishes to understand how security and privacy policies, priorities and initiatives are developed within different political contexts. This includes national contexts, e.g., in Member States and the USA, as well as supra-national contexts, e.g., the UN or the European Union. Second, this review also seeks to understand how "security" and "privacy" are conceptualised by different policy-makers. As mentioned above, this will be used in conjunction with the PRISMS survey findings to examine how well this correlates with citizens' perceptions, priorities and understandings.

In order to achieve these aims, this report produces an inventory the most relevant policy documents from 2000 onwards within international organisations, the European Union, selected Member States and the USA related to security, privacy and surveillance policy. We then selected key policy documents from each context and subjected these to a "short

analysis" to identify key themes within the documents. These "short analyses" were combined into a horizontal analysis that sought to gain an understanding of how security and privacy were conceptualised by policy-makers in different national or regional contexts, and to understand how security and privacy were conceptualised across these different categories. This horizontal analysis will be supplemented, in a separate deliverable, by a discourse analysis of selected Dutch, British and European policy documents in order to gain a further detailed understanding of exactly how these concepts are discussed, contested and negotiated within specific national contexts. This multi-dimensional methodology will enable PRISMS to understand the manner in which concepts such as security and privacy are framed in these policy circles in preparation for conducting the PRISMS survey as well as for designing the decision support system.

1.2 CONTEXT

This review of policy documents is part of a multi-faceted approach that the PRISMS project is taking to understand how privacy and security are conceptualised in a range of different sectors, including the media, the legal sphere and the technology domain. Such a multi-faceted review is necessary because both privacy and security are complex and contested concepts, particularly across different national and language contexts.

Academics have found that the concept of privacy is notoriously difficult to define. Privacy is often understood to be a social value and a public good as well as an individual value.[1] Although a widely accepted definition of privacy remains elusive, many academics have argued that privacy comprises multiple dimensions. For example, Daniel Solove asserts that privacy is best understood as a "family of different yet related things"[2]. Roger Clarke outlined, in 1997, a taxonomy of privacy that included four different types of privacy: privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication.[3] More than a decade later, Finn, Wright and Friedewald updated Clarke's categories to include seven types of privacy:

- *Privacy of the person* encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private.
- *Privacy of behaviour and action* concerns activities that happen in public space and private space.
- *Privacy of communication* aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages.
- *Privacy of data and image* includes protecting an individual's data or image from being automatically available or accessible to other individuals and organisations and ensuring that people can "exercise a substantial degree of control over that data and its use".

[1] See Gutwirth, Serge, *Privacy and the Information Age*, Rowman & Littlefield, Lanham, MA, 2002; Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, MA, 2006; Regan, Priscilla, *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, NC, 1995, Chapter 8; and Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge, MA, 2008.
[2] Solove, 2008, p. 9.
[3] Clarke, Roger, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997. http://www.rogerclarke.com/DV/Intro.html

- *Privacy of thoughts and feelings* includes individuals having the right to think whatever they like.
- *Privacy of location and space* argues that individuals have the right to move about in public or semi-public space without being identified, tracked or monitored, and to designate private spaces that are free from intrusion.
- *Privacy of association (including group privacy)* is concerned with people's right to associate with whomever they wish, without being monitored.[4]

However, others have argued that the complexity of privacy as a concept has legal and ethical benefits. The European Court of Human Rights (ECtHR) has ruled that it is neither possible nor necessary to determine the content of privacy in an exhaustive way.[5] Furthermore, maintaining flexibility in a conceptualisation of privacy could ensure that a wide range of issues such as integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data, wiretapping, gender, health, identity, sexual orientation, protection against environmental nuisances and so on are covered by the law.[6]

However, in a policy context, the focus is often on protection of personal data more than on the protection of privacy. Although the Charter of Fundamental Rights of the European Union 2000 treats privacy and data protection separately in Articles 7 and 8 respectively,[7] the first European Directive related to privacy was the 1995 Data Protection Directive (95/46/EC) that is focused on organisations that process personal data.[8] In the past few years, an intense process of stakeholder consultation has led to a recently published Proposal for a Regulation to update the existing regulatory framework.[9] This document foregrounds data protection elements such as supporting "privacy by design" technologies that integrate privacy features throughout the entire development process of a system from its earliest conception, and mandating that organisations appoint data protection officers and implement "data protection impact assessments". However, developments in security and surveillance technologies have created new practices that threaten the privacy of individuals without actually processing their personal data. Indeed, when using the various ICTs, individuals leave a vast number of electronic traces that may not be personal data in the sense of the relevant Directives, but which nonetheless become the resources of extensive profiling activities that entail several

[4] Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Yves Poullet et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 3-32.

[5] *Niemietz vs. Germany* and *Pretty vs. UK,* Judgment of 16 December 1992, § 29 [these are 2 separate cases. Which one is being quoted?]: "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However, it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there from [does the original say "therefrom" or "there from"?] entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."

[6] See Gutwirth, 2002 and Sudre, Frédéric, Jean-Pierre Marguénaud, Joël Andriantsimbazovina et al., *Les grands arrêts la Cour Européenne des Droits de l'Homme*, Presses Universitaires Française, Paris, 2003.

[7] European Commission, Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities*, 2000/C 364/01, Brussels, 18 December 2000. http://www.europarl.europa.eu/charter/pdf/text_en.pdf

[8] European Commission, 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 of such data, *Official Journal*, L 281, 23 November 1995, pp. 31-50.

[9] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 January 2012. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

risks for the privacy of the persons concerned.[10] Therefore, the equation of privacy with data protection does not adequately address infringements that are not directly linked to the processing of personal data.

Individuals in the European Union also have a right to security, and like privacy, there have also been difficulties in establishing a comprehensive definition of security. Lucia Zedner has argued that security is often defined as the absence or mitigation of threats, thus it depends on these very threats in order to have conceptual clarity.[11] Other researchers, such as David Brooks, argue that the "multidimensional nature of security results in both a society and industry that has no clear understanding of a definition for the concept of security. Moreover the current concepts of security are so broad as to be impracticable."[12] Given this difficulty, it is not surprising that different European languages have different words and different connotations for the meaning of security. In English, words such as security, safety and continuity are used for different aspects of being and feeling secure.[13] The German word *Sicherheit* refers to both security and safety while the Dutch and French use a different word for each (*veiligheid* and *zekerheid*, *sécurité* and *sûreté*). Furthermore, security is applied to a range of different contexts, from social security to technologically secure systems. Cyber and information security is a distinct branch which refers to secure handling of information, preventing unauthorised access and use of data. Secure communications are communications which function as expected and which are robust and vital, able to resist attacks on their functionality. Within the policy context of the European Union, security relates to the integrity of the European Union as a whole, the protection of its outer borders and the fight against criminality, terrorism, fraud and illegal immigration. The first PRISMS work package developed a taxonomy of "security" that broke security down into seven different types.

- *Physical security*: That part of security concerned with physical measures designed to safeguard the physical characteristics and properties of systems, spaces, objects and human beings.
- *Political security*: That part of security concerned with the protection of acquired rights, established institutions/structures and recognised policy choices.
- *Cultural security*: That part of security concerned with measures designed to safeguard the permanence of traditional schemas of language, culture, associations, identity and religious practices while allowing for changes that are judged to be acceptable.
- *Environmental security*: That part of security concerned with measures designed to provide safety from environmental dangers caused by natural or human processes.
- *Radical uncertainty security*: That part of security concerned with measures designed to provide safety from exceptional and rare violence/threats.
- *Information security*: That part of security concerned with measures designed to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

[10] De Hert, Paul, and Serge Gutwirth, "Regulating Profiling in a Democratic Constitutional State", in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, pp. 271-291.
[11] Zedner, Lucia, *Security*, Routledge, London, 2009.
[12] Brooks, David J., "What is security: Definition through knowledge categorization", *Security Journal*, Vol. 23, No. 3, 2009, pp. 225-239. http://www.palgrave-journals.com/doifinder/10.1057/sj.2008.18
[13] Bauman, Zygmunt, *In Search of Politics*, Polity Press, Cambridge, 1999.

- *Socio-economic security*: That part of security concerned with economic measures designed to safeguard the economic system, its development and its impact on individuals.[14]

Significantly, the right to privacy is often linked with an individual's right to security, as security measures often involve the increased use of surveillance technologies that have significant privacy implications. Over the past decade, the Tampere Programme (1999-2004), the Hague Programme (2005-2009) and most recently the Stockholm Programme (2010-2014) form the basis of the internal security strategy of the Commission, and deal with the protection of individual rights, the fight against terrorism, criminality, immigration and fraud. Various events (the attack on the World Trade Centre in New York, the bombings in Madrid and London) contributed to the request for new measures to safeguard Europe and its Member States from terrorist attacks and opened the door to a variety of measures which were potentially intrusive in relation to privacy (such as visual surveillance, location determination, communication monitoring, biometric identification, dataveillance and sensor technologies[15]). For example, in its 2010 Communication, the European Commission presents an overview of European initiatives to safeguard the security of its citizens by combating criminal and terrorist behaviour and fighting illegal immigration.[16] It identifies 18 different initiatives some of which were established several years ago (e.g., the Schengen Information System) and some are the result of the heightened threat alerts in recent years. Furthermore, the European Security Research Advisory Board (ESRAB) has stated that more security is only possible at the price of collecting more information and increased surveillance which immediately raises questions of privacy and data protection.[17]

These complex and contested definitions were fed into the selection criteria for policy documents in order to ensure a comprehensive inventory of policy documents across different contexts.

1.3 CRITERIA FOR SELECTING DOCUMENTS

Because this report describes both the document collection phase and the first analysis of policy documents, in the pages below we define our understanding of policy documents and describe the criteria for selecting documents for the long list of documents as well as the short analysis process.

[14] See also, Lagazio, Monica, *Report on research approaches and results,* ETTIS project, Deliverable 2.2, 31 June 2012.

[15] Bellanova, Rocco, Matthias Vermeulen, Serge Gurwrith, Rachel Finn, Paul McCarthy, David Wright, Kush Wadhwa, Dara Hallinan, Michael Friedewald, Julien Jeandesboz, Didier Bigo, Merveyn Frost and Silva Venier, *Smart Surveillance – State of the Art*, SAPIENT Deliverable 1.1, SAPIENT, 23 January 2012. http://www.sapientproject.eu/deliverables.html

[16] European Commission, "Overview of information management in the area of freedom, security and justice", COM(2010) 385 final, Brussels, 2010.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF

[17] ESRAB (European Security Research Advisory Board), "Meeting the challenge: the European Security Research Agenda. A report from the European Security Research Advisory Board", Office for Official Publications of the European Communities, Luxembourg, 2006.
http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

1.3.1 Defining policy documents

The core concern of this report is to examine how privacy and security are understood, enacted and constructed in policy processes. Although the PRISMS project has not defined "policy" or "policy document", we do not believe it is necessary or helpful for the purposes of this document to theorise "policy" as a concept in order to fulfil our aim of analysing how "privacy", "security", and other terms are manifested in policy processes.

We understand policy processes as including policy formation, policy implementation and policy evaluation, although these are only analytical categories and not clearly defined, discrete, or sequential empirical stages. Textbooks of political science and policy studies[18] provide lengthy debates over the meaning of "policy" as either "an attempt to define and structure a rational basis for action or inaction",[19] or as something more decentralised, dispersed, and far less coherent; we do not regard it as necessary to take a stand on this question. Nor do we have to arbitrate between alternative views concerning the distribution and exercise of authoritative decision-making power[20] in which the production of policy documents by a variety of participants and actors may serve purposes and have meanings and impacts that vary, depending upon how power relations are configured in any state or in any sector of policy. We have made a pragmatic choice to take "policy" to mean a decision or intention of government or other authoritative body to pursue a course of action, whether by means of legislation or through other executive or administrative means.

In a similar vein, for present purposes we adopt a relatively unburdened and straightforward approach to identifying the sources to be used in this analysis. Thus we take 'policy documents' to be documents that relate to one or more aspects of policy processes in various sectors in which issues of security and privacy play a major part. We adopt a broad approach towards policy documents in which we accept policy advice, policy papers, policy evaluations and policy analyses as relevant documents, presuming that they all may have an impact on policy processes. Thus we consider a very wide range of published materials related to decision-making, whether these are produced by the authoritative body itself or by other official participants in the policy- or decision-making process. These include parliaments and parliamentary bodies (e.g., committees), regulators, government and intergovernmental agencies, and others. The documents themselves are similarly heterogeneous: policy statements, reports, opinions, commentaries, published speeches, descriptive papers, and many other kinds. Given the purpose of compiling a list of policy documents – to create a master inventory from which to select documents for further analysis, including discourse analysis – we have tended to exclude actual pieces of legislation or bills on the grounds that their close analysis would not be fruitful because of their nature and the language in which they are written, although we have not kept strictly to this criterion in the case of certain very prominent governmental or intergovernmental promulgations that have had great influence over the field of this project (e.g., certain EU Directives or proposals for Directives, in which there is explanatory prose that is amenable to analysis). We also excluded the vast number of

[18] For example, Parsons, Wayne, *Public Policy: An Introduction to the Theory and Practice of Policy Analysis*, Edward Elgar, Aldershot, 1995; Sabatier, Paul (ed.), *Theories of the Policy Process*, Westview Press, Boulder, CO, 1999; Hill, Michael (ed.), *The Policy Process; A Reader*, 2nd edn., Prentice Hall/Harvester Wheatsheaf, Hemel Hempstead, 1997.

[19] Parsons, Wayne, *Public Policy: An Introduction to the Theory and Practice of Policy Analysis*, Edward Elgar, Aldershot, 1995, p.14.

[20] For example, Dunleavy, Patrick and Brendan O'Leary, *Theories of the State: The Politics of Liberal Democracy*, Macmillan, Basingstoke, 1987.

policy-related documents such as academic articles, newspaper stories, and papers from civil-society bodies on the grounds of convenience and time limitation.

1.3.2 Compiling the long list of policy documents

We used the following process for compiling the long list of documents. First, we decided to focus on select international organisations' policy documents, European policy documents, policy documents from six Member States and the USA. The six European Member Sates we focus on included the Netherlands, France, Germany, Italy, Romania and the UK. These countries were selected to provide a geographical and political mix of perspectives. For example, the UK has often been described as prioritising security over privacy, particularly in relation to the introduction of surveillance technologies and devices and their close relationship with the United States.[21] In contrast, recent debates around the introduction of the Data Retention Directive in Germany suggest that the German government focuses heavily on the data protection and privacy considerations of proposed security policies.[22] Romania, as a former totalitarian state, provides another unique perspective on privacy and security issues. Finally, despite the focus of this research on Europe, partners included international organisations and the USA as additional examples because of Europe's participation in organisations such as the UN, the Organisation for Economic Cooperation and Development, etc., and because of the USA's prominent role in shaping security discourse internationally, particularly after the events of September 2001.

The 983 documents selected for the long list were subject to some practical restrictions. First, we only collected documents which were published, since we had no systemic outside knowledge about unpublished documents. Second, the partners only collected documents that were publicly available and free to access. This strategy was adopted because PRISMS is interested in public opinion, and this report is interested in how policy documents might eventually relate to public opinion. Third, we focused on documents published from 2000 onwards; however important documents from before 2000 were occasionally included if they were especially relevant.

Documents were searched within different international, EU and national government agencies, departments and oversight bodies. For the international examples, the report examines five major bodies or organisations, including the UN, the Organisation for Economic Cooperation and Development (OECD), the North Atlantic Treaty Organisation (NATO), the International Conference of Data Protection and Privacy Commissioners and the International Telecoms Union. Because of the size and breadth of these organisations, the report lists key documents and major policy initiatives that relate to privacy and security, rather than producing an exhaustive list.

In relation to Europe, the report focuses on legislative bodies, executive bodies and a number of specific agencies and oversight bodies. Legislative bodies were represented by the Council of Europe, the European Parliament and the Council of the European Union, while the executive branch was represented by the European Commission (EC). The report also includes documents from agencies, departments and institutions relevant to security and privacy such as the European Security Research Advisory Board (ESRAB), the European

[21] Lyon, David, *Surveillance after 9/11*, Polity Press, 2003.
[22] DeSimone, Christian, "Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive", *German Law Journal*, Vol. 11, 2010, pp. 291-318. http://www.germanlawjournal.com/index.php?pageID=11&artID=1240

Security Research and Innovation Forum (ESRIF), European Network and Information Security Agency (ENISA), Frontex, the European Union Agency for Fundamental Rights, the Article 29 Data Protection Working Party and the European Data Protection Supervisor (EDPS). Each of these agencies shape policy either by issuing recommendations, reviewing proposed policies, setting priorities and initiatives or implementing policies.

Other European agencies that performed similar functions or were also relevant to privacy and security were not in the list of policy documents for various practical reasons. These included the European Committee on Standardization (CEN) as well as the International Standards Organization (ISO) because their documents were not publicly available and could only be accessed via purchase. Europol was also excluded because this organisation primarily produces reports on activities rather than policy documents or recommendations for policy. Researchers encountered a similar situation in relation to Eurojust, in that this organisation tends to produce reports or agreements on data sharing with other countries or organisations, but no policy documents as described above. Finally, although we considered Global Monitoring for Environment and Security (GMES), this agency primarily produces research related to establishing a space satellite system, not producing policy papers or making policy recommendations. However, GMES was managed initially by the European Commission and the EC documents relevant to GMES and dealing with policy issues have been included with the other EC documents.

For the European countries and the USA, the report identifies documents from a similar range of bodies, departments and agencies. For each country, researchers focused on legislative bodies (i.e., both legislative houses or bodies as appropriate), executive bodies (e.g., the Cabinet Office, the Office of the Prime Minister, etc.), department of defence, immigration agencies, data protection authorities and other relevant institutions as appropriate for each country. We focused on policy documents in English as well as the official language(s) of each country, with many titles “unofficially” translated into English by members of the research team.

In all cases, search functions on particular websites were used when possible to identify relevant material. Terms such as “privacy”, “security”, “cybersecurity”, “data protection” and “surveillance” were searched in the English language countries and documents. Because of the use of local languages in some European countries, we adjusted the word searches to reflect different languages and contexts, and these are described in the introduction to each country, as appropriate. In other cases, it was necessary to trawl through websites, long libraries of documents or tens of thousands of search results in order to identify potentially relevant policy materials. In these cases, we relied on the titles of the documents to determine whether the material was worth exploring further. Judgement was used to decide whether a policy document focused on privacy and/or security, rather than simply mentioning these issues in passing. In all cases, the research team prioritised documents that discussed both privacy and security. The long list of policy documents in presented in Appendix A.

However, because the selection of documents involved considerable methodological and practical constraints as well as potentially significant divergences between countries, any conclusions drawn from this exploration of policy documents must be viewed as preliminary and partial, rather than exhaustive. Despite this limitation, the long list of policy documents do reveal some interesting differences between Europe and its Member States, as well as between different States themselves.

1.3.3 Short analysis

For the short analysis of key documents, partners used a consensus building workshop to select documents that would be subject to short analysis. Partners involved in the work package gathered for an internal workshop, each one having previously selected approximately 80 documents from the long list that, in their opinion, were key policy documents. Individual selections were compared, and those selected by three or more partners were automatically included in the short list. Overall, the partners prioritised major policy documents (e.g., the Stockholm programme), key policy changes after September 2001 and national defence strategies in Europe, Member States and the USA. In order to fill the remaining slots, partners were then invited to argue for the inclusion of other documents they had selected. Overall, 56 documents across the international organisations, Europe, the six Member States and the USA were subject to short analysis. The short analysis for each of the sampled documents contained six fields. These included the domain addressed by the document; its target audience; its stated purpose, its context, including any other documents referenced; its key points; and an assessment of its importance or significance. The short analyses provide a glimpse of privacy, data protection and security issues in particular countries. Each short analysis is included in Annex B.

2 SUMMARY OF POLICY DOCUMENTS

2.1 INTERNATIONAL ORGANISATIONS

The chapter on international organisations includes supra-national organisations that are relevant to different countries and different continents or regions across the globe. Many of these organisations are world-wide, in that they include members from across the world, although, in many cases some countries, such as the USA or China in the case of the United Nations, carry more weight than other countries. Often these organisations make pronouncements that are generally applicable across the world or which prioritise national, regional or ethnic equality and equity.

Researchers selected the following organisations for the document search: the United Nations, the Organisation for Economic Cooperation and Development, the North Atlantic Treaty Organisation, the International Conference of Data Protection and Privacy Commissioners and the International Telecommunications Union. The purpose of this selection was to contextualise the position of the European Union as well as the European Member States within this larger, supra-national structure. Thus, some relevant international organisations, for example the Association of South East Asian Nations (ASEAN), have been excluded because they do not involve European members. Furthermore, other relevant international organisations, for example Interpol, were not included either because the documents they produced were too numerous to effectively search, or because they did not fit the criteria outlined in the methodology section above (e.g., they were not publicly available).

Researchers identified 33 key policy documents from international organisations specifically related to security and privacy, utilising the following terms when searching for policy documents: security, privacy, surveillance and data protection. Issues related to defence, security and protection from various threats, including terrorism and cyber-terrorism, featured in approximately 66% of all international policy documents, particularly NATO documents, and including a small sub-set of UN documents that explored strengthening privacy protections while effectively combatting terrorism. The remaining 33% of focused on privacy, data protection and other human rights, with a specifically strong discussion of these issues originating in the UN as well as the International Conference of Data Protection and Privacy Commissioners.

2.2 EUROPEAN SECURITY AND PRIVACY POLICY DOCUMENTS

As part of this work we have included a long list of policy documents from the European Union and European context due to PRISMS' focus on Europe. European policies are central to the linkage between security and privacy and often refer to the hypothesis that privacy and security must be balanced against one another. However, Europe may also be considered an important avenue through which the balance metaphor can be disrupted and security and privacy can co-exist. In the European Union, a right to security and a right to privacy are both enshrined in the Charter of Fundamental Rights. Thus, unlike other regions, European governments are obligated to address security and privacy simultaneously when considering new policies, technologies or practices.

Europe has also been at the forefront of major privacy and security legislation. For example, the European Parliament passed the Data Protection Directive (95/46/EC) in 1995, obligating all Member States to enact their own data protection legislation based on the principles outlined in the Directive by 1998. Yet, given the age and subsequent inadequacy of the Directive, the European legislature is also currently examining proposals to introduce a Data Protection Regulation which offers greater protections, and which Member States would have to implement directly. Additionally, the EU has enacted laws related to privacy and data protection in specific sectors, such as the telecommunications sector. See, for example, the e-Privacy Directive (2002/58/EC) and the Data Retention Directive (2006/24/EC). European policy has also focused on the security and privacy aspects specific technologies more explicitly than many of the national governments also examined in this document. It outlines principles for the use of RFID, other "smart cards", electronic passports, body scanners and social networking services, to name a few. Like an independent country, it also runs its own security research programme, it has a defence policy and it has an independent data protection supervisor. However, similar to an international organisation, many policy documents outline basic principles and targets rather than legislative obligations.

Researchers identified 371 policy documents from Europe specifically related to security and privacy, utilising the following terms when searching for policy documents: security, privacy, surveillance and data protection. Issues related to defence, security and protection from various threats, including terrorism and cyber-terrorism, featured equally in European policy documents to those focusing on privacy, data protection and other human rights, each making up approximately 50 per cent of the documents collected.

2.3 OTHER EUROPEAN POLICIES

In addition to policies specifically focused on privacy and security, PRISMS also acknowledges that other policy areas are relevant to privacy and security that fall outside of traditional internal and cross-border threats to states and their populations. These could include other policy areas that also cover security and privacy aspects, such as transport policies, financial policies, health policies and immigration policies. Many of these policy documents from the European Parliament, European Commission and various European Agencies focus on topics such as money laundering, eHealth and immigration databases, such as the Visa Information System (VIS) and the Schengen Information System II (SIS-II). In all, partners collected 37 policy documents in these alternate areas, and the majority of these documents focused on the relationship between security and privacy, since these were deemed the most relevant for our purposes in PRISMS.

2.4 UNITED KINGDOM SECURITY AND PRIVACY POLICY DOCUMENTS

Over the last decades the United Kingdom has experienced security threats and attacks from republicans in Northern Ireland and, more recently, Islamists living in mainland UK. These various threats have resulted in the UK leading Europe in introducing surveillance measures intended to enhance security from a government funded programme in the 1990s to introduce CCTV cameras in city and town centres on a large-scale, to the introduction of body scanners in airports immediately after the "underwear" bomb incident in late 2010 and early 2011. However, despite this strong interest in providing security, privacy and data protection, including data security, have remained major issues of focus in the UK, sometimes as a result

of European intervention. The introduction of the Data Protection Act 1998 to ensure that personal data is protected by companies, the public sector, and other organisations has led to better citizen-consumer data protection, but many forms of surveillance are beyond its control. Furthermore, the Regulation of Investigatory Powers Act of 2000 as well as the Protection of Freedoms Act of 2012 have introduced stronger regulation of those using surveillance technologies or practices to provide security, although their provisions and implementation have not necessarily led to less obtrusive, more proportionate, surveillance in many respects. The cessation of indefinite storage of DNA information by the police, and the removal of some types of body scanners in UK airports have both been as a result of a European Court of Human Rights ruling and the removal of European permission respectively. Given the UK's unique positioning within a political context that prioritises security and surveillance as well as pressure from Europe and its own citizens to address privacy and data protection issues, the country makes a unique case for examining policy frameworks within Europe.

Researchers identified 115 policy documents in the UK related to security and privacy, utilising the following terms when searching for policy documents: security, privacy, surveillance, safety and data protection. Issues related to defence, security and protection from various threats including terrorism and cyber-terrorism featured strongly in the UK policy documents, making up approximately 60 per cent of the documents collected. In contrast, privacy, data protection and other human rights considerations were the focus of just under 30 per cent of the documents collected. The remainder of the documents were related to specific issues such as identity cards, DNA or the implementation of European legislation.

2.5 NETHERLANDS SECURITY AND PRIVACY POLICY DOCUMENTS

The Netherlands have been spared from large-scale terrorist attacks similar to those that hit London or Madrid. However, the country has been confronted with a number of high-profile incidents, including the assassination of Dutch politician Pim Fortuyn in 2002, the assassination of filmmaker Theo van Gogh in 2004 and the violent arrest of a radical Islamic group surrounding the person who perpetrated the attack. As a result, security measures were stepped up culminating in the proposals made recently to grant law enforcement significantly additional powers. If adopted, such powers would include access to personal information stored by private entities such as banks and hospitals, tapping the internet traffic of all Dutch citizens, and allowing police to break into local and foreign computers and remotely conduct searches and delete data in the course of a criminal investigation. Although the privacy implications of such current and proposed security measures would be far-reaching, they did not cause the flare up of the public debate as much as topics such as smart metering, the national electronic patient file system, and the introduction of smart cards for public transport.

The stark difference in public response to privacy-invasive initiatives relating to (national) security as compared to measures in other domains (such as public transport or health care) makes the Netherlands an interesting case for this study. We identified 107 policy documents in the Netherlands relating to privacy and/or security, by using the following Dutch keywords for our search: *privacy, persoonlijke levenssfeer (private sphere), openbare orde (public order), veiligheid (security/safety), databescherming (data protection), surveillance* and *persoonsgegevens (personal data)*. Topics discussed in the selected documents cover an array of topics ranging from proposals to increase judicial and police powers and those of the

intelligence services with regards to the collection of personal data, to cyber security, and to the trade-off between privacy and security.

2.6 FRANCE SECURITY AND PRIVACY DOCUMENTS

Unlike many other countries which foreground security concerns, particularly after 2000, French policy has been characterised by a consistent and early focus on privacy via data protection. France was one of the first countries in Europe to enact a Data Protection Act in 1978, thus signifying and establishing an early concern with data privacy. Furthermore, in addition to this early data protection law, France, like the US, has also enacted a number of sector specific data protection laws in relation to video surveillance, consumer protection, and employment as well as others. However, France also does not have any legislation that specifically outlines a right to privacy. Yet, despite this focus on data protection, the French government also demonstrates a clear concern with security, and particularly threats such as terrorism, cyber-crime and other crime. The government introduced widespread powers in the Anti-Terror Act of 2006, intended to enhance government and citizen security via surveillance measures such as the collection of telecom data, the expansion of CCTV surveillance, traffic monitoring, monitoring large events and collecting and sharing passenger name records. This legislation was primarily a response to external events, e.g. the terrorist attacks in New York, Madrid and London, rather than a specific, internal terrorist threat. To date, France has only experienced small-scale attacks, although the country remains a target for Islamist groups as a major western power.

In all, partners collected 33 documents focused on security and privacy policy in France, by searching the following terms: privacy, security, terrorism and surveillance (vie privée, sécurité, terrorisme, surveillance). Where searching the contents of the document was not possible, researchers also utilised keywords such as biometrics, information systems and video surveillance (biométrie, systèmes d'information, vidéo surveillance). One-third of these documents focused on security, counter-terrorism and information security. The remaining documents (66 per cent) were concerned with issues related to human rights, privacy and data protection. This largely conforms to the French policy focus on privacy and data protection.

2.7 ITALY SECURITY AND PRIVACY POLICY DOCUMENTS

Italian policy-makers appear to understand their security context as expanded and broadened in the era of globalisation. For example, they are dealing with a growing interdependence between the national context and the larger European and Mediterranean context, with the increase of external threats and the need to protect Italy by enlarging the scope of national security to include this international contextualisation. In consequence, the Italian Foreign Ministry describes their security policies and legislation in terms of conforming to the principles set by larger, supra-national organisations such as the United Nations, the North Atlantic Treaty Organisation and the European Union.[23] These responses have included, for example, the adoption of laws specifically related to crimes committed with the intention to conduct terrorism (Law No. 438/2001). Therefore, Italian authorities contextualise themselves within these larger organisations and within larger debates around terrorism and security, specifically through making reference to changes after September 2001. Furthermore, in

[23] Farnesia (Ministry of Foreign Affairs), "Fight against Terrorism", 2009. http://www.esteri.it/MAE/EN/Politica_Estera/Temi_Globali/Lotta_Terrorismo/

contrast to other countries, this response to the political context after 2001 is not discussed in direct relation to potential threats to Italy itself, and Italy has not experienced any significant, recent terrorist activity (although there were political terrorist incidents in the 19660s and 70s and extremist incidents in the 80s). In relation to privacy, communication activities as well as activities within the domicile have long been protected by Italian legislation. A relatively new addition has been the Data Protection Code of 2003, which was the result of much political wrangling over appropriate uses of personal data. In some areas, for example consumer protection and preventing "spam", Italian data protections are far stronger than other European or third country counterparts. However, similar to these other counterparts, Italy does have some sectorial privacy and data protections, in relation to video and workplace surveillance in particular.

Partners identified 68 different Italian policy documents relevant to privacy and security policy. These documents were identified by searching the following key words on the web pages of relevant departments and agencies, as well as the Italian *Official Journal*: security, privacy, data protection and surveillance (in Italian: sicurezza, dati personali, protezione dei dati, sorveglianza, videosorveglianza, dati informatici). In relation to the Italian policy documents, laws (leggi) are excluded from this list, but codes, guidelines, decrees and other such documents are included. In total, 22 per cent of Italian policy documents (15 documents) focused on defence, national security, data security and counter-terrorism. In contrast, 69 per cent (47 documents), including 41 documents from Garante, the Italian data protection authority, focused on data protection, privacy and the privacy implications of specific technologies, processes and practices.

2.8 GERMANY SECURITY AND PRIVACY POLICY DOCUMENTS

Germany has been faced with a severe terrorist threat in the 1970s, mostly initiated by far-left terrorist groups. More recently no large attacks have taken place, but far-right groups and foreign terrorist organizations have been suspected of planning attacks. To combat these and other security threats, federal and state policy makers have implemented different regulations limiting the privacy of communications and supporting more video surveillance. However, with regards to privacy and security policy, Germany does not stand out because of its security policies, but rather because of the high privacy consciousness of German citizens and civil rights groups, leading to intense policy debates and one of the strongest legal privacy protection in the European Union. A significant public movement against data retention legislation put this topic on the agenda as a major privacy issue, which eventually resulted in the Constitutional Court ruling that there is no legal basis for data retention. Germany is currently facing a fine from the European Commission for declining to implement the Data Retention Directive. Other cases in which the German focus on privacy protection is clearly visible include legal cases against FaceBook's real-name policy, and Google's StreetView service, both of which faced stiff opposition from both German citizens and lawmakers.

Because public policy in Germany puts a unique emphasis on privacy protection, often by implementing regulations that are stricter than in other EU Member States, Germany is an interesting case for the present study. We identified 53 policy documents in Germany related to security and privacy, by using the following German keywords for our search: *Datenschutz (data protection)*, *Privatsphäre (private sphere)*, *Sicherheit (security)*, *Eingriffen in die Privatsphäre (privacy intrusion)*, *Öffentliche sicherheit (public safety)*, *Informationsfreiheit (freedom of/right to information)*, and *Personenbezogener Daten (personal data)*. The

German Bundesländer (federal states) play a key role in the formulation of their state's own policy, and because of this reason we decided to include two of the Bundesländer in the search: Schleswig-Holstein and Berlin. These two Bundesländer were selected because of their particular contribution to policy in the area of privacy and data protection. Topics featuring prominently in the 53 policy documents are debates on the fight against the terrorist threat which would require more access to personal data, international cooperation in the fight against serious crime, but also deliberations on the impact on individual privacy of security initiatives such as the proposed introduction of body scanners, data retention, and surveillance.

2.9 ROMANIA SECURITY AND PRIVACY POLICY DOCUMENTS

Romania, an ex-communist Eastern European country and one of the new Member States of the European Union, was included in this study in our attempt to capture briefly the European cultural and historical diversity and its effect on perceptions of privacy and security. The prominence of the two topics turned out to be low in the Romanian official documents researched, playing out mainly in the media and in courts of law. To some extent this can be attributed to the multitude of topics vying for the public's attention in a country still in economic, social and political transition. Also, the public discourse on the two topics and over the period covered by this study turned out to be to a large extent reflective, inward-looking and implicit. It focused on past activities of the communist secret police and the ways in which the local population and their officials should deal with them. In that, it covered mainly issues of secrecy, lack of transparency and distrust in public office officials, law enforcement, the secret service and the judiciary. Furthermore, other fundamental rights enjoyed more coverage, in particular the freedom of speech and the freedom of expression. More contemporary topics featuring prominently in the Western European discourse on privacy and security emerged relatively late in the Romanian official documents. Some can be linked to a later adoption of certain technologies, whilst others have to do with recent reform measures required as part of the EU accession package. As such, topics like workplace surveillance and video surveillance have started being addressed in official documents; the implementation of the Data Retention Directive was contested in the Constitutional Court and declared unconstitutional (recently the ruling has been reversed). The Romanian data protection authority is only a recent addition to the institutional landscape and its impact remains as yet limited.

Researchers identified only nine official Romanian documents relevant to the privacy and security discourse. The search used keywords that captured the meaning of the English words privacy, surveillance, safety and data protection and included the following Romanian words or variations thereof: *viata intima* (intimate life), *viata privata* (private life), *securitate* (security; N.B. until 1989 the word had a secondary meaning and was used to refer to the Romanian secret police)*; siguranta* (safety; N.B. like security, the word had a secondary meaning and was used to refer to the secret police organization that preceded the "Securitate"), *supraveghere/monitorizare* (surveillance, monitoring) and *protectia datelor cu caracter personal* (personal data protection).

2.10 USA SECURITY AND PRIVACY POLICY DOCUMENTS

The USA offers an interesting comparative example for the European national contexts for three reasons. First, the USA has been at the fore-front of security discourses, security policy and the introduction of security measures, particularly since September 2001 and has heavily influenced European policy in many areas. Key US policies have also generated significant international attention, for example the US PATRIOT Act and Foreign Intelligence Surveillance Act and may impact upon European citizens. In some contexts, such as the transfer of Passenger Name Records for aviation, Europeans and other non-US citizens and governments are directly impacted by US laws and policies in order to continue to maintain a similar relationship with the US government. Second, the USA is highly influential in many of the supra-national organisations examined in Chapter 2 of this document, including the UN, NATO and the OECD. Finally, unlike the EU and European Member States the US does not recognise an over-arching right to privacy, nor does it have an over-arching data protection law. Instead, it relies upon sectoral regulations, for example in relation to healthcare (Health Insurance Portability and Accountability Act), communications (Electronic Communications Privacy Act of 2000), children's privacy (Children's Online Privacy Protection Act), etc. Furthermore, the USA does not have a data protection authority, and relies upon the Federal Trade Commission and the Federal Communications Commission to enforce sectoral privacy and data protection laws.

In total, this report identified 96 policy documents from the USA using keyword searches across a number of federal agencies. Unlike other national contexts, the committees and organisations within the legislative branch were too numerous to search individually. Therefore, in order to capture the legislative perspective, partners confined their search to the Congressional Research Service, a legislative agency responsible for scrutinising proposed legislation. Partners also searched the websites and repositories of the Office of the President, the Department of Homeland Security, the Federal Trade Commission, the Federal Communications Commission and the Department of Commerce. In each case, keywords such as privacy, data protection, surveillance, terrorism, security and homeland security were used to identify relevant documents. However, in some agencies, this was expanded to also include keywords associated with security and surveillance technologies such as biometrics, body scanners, etc. Some search results returned sets of thousands of documents that were too numerous to be examined using key words. In these cases, researchers used title reviews or other mechanisms to create a manageable data set. Finally, some agencies only listed publicly available documents that were recently released (2010 onwards). Almost 60 per cent of the US policy documents focused on security, cyber-security, anti-terrorism and defence, while 39 per cent focused on privacy; however these figures have double counted documents that relate to both security and privacy.

2.11 SUMMARY

This brief examination of the focus of policy documents internationally, at the European level, within Member States and within the USA suggests that different countries have different relative priorities in terms of security and privacy. While the majority of documents collected from international organisations and countries such as the UK and the USA focused on security, the documents collected in other contexts, including Italy and France appeared to prioritise privacy and data protection. Significantly, European policy documents were evenly spread between being focused on security and privacy. The following section discusses a

horizontal analysis of 56 of these 983 policy documents, in order to examine whether this distinction plays out in the closer reading of these policy documents.

3 HORIZONTAL ANALYSIS

3.1 INTRODUCTION

The long list of policy documents provides some information about the key issues of privacy, security, data protection and surveillance and potential differences and similarities in the way policy makers in different countries have characterised these issues. However, a more in-depth assessment of a relevant "set" of policy documents referring to the security and privacy policies of the Commission and selected Member States enables an understanding of the manner in which concepts such as "security" and "privacy" are framed in a European policy context, what differences exist between countries and over time, and what dominant approaches frame current discourse and policy activities. This horizontal analysis of select policy documents provides such an assessment, and provides the background that will enable the PRISMS consortium to consider how and whether discourses by policy makers influence citizens' priorities and perceptions, as well as how notions of privacy and security might be successfully integrated into a decision support system that protects and provides both privacy and security.

As already noted, "security" and "privacy" have multiple meanings across contexts. What becomes defined as a privacy or security problem (and what is excluded from this) is a political process, conducted at least in part through policy texts and documents. This analysis cannot see "behind the text" to the motives and intentions of the texts' authors, but we should see these texts as particular examples of deliberate attempts to engage in a political process of framing issues of privacy and security in particular ways. These frames may be deliberate and explicit, or they may reflect background assumptions and "common sense". Thus, this analysis places us in a better position to understand one set of influences upon citizen perspectives and attitudes. These texts are all publicly available, and influence mediated second-hand accounts, such as news reporting. Do public attitudes align with, ignore, incorporate or contest the framings found in these documents? Combined with PRISMS' analysis of public attitudes, this horizontal analysis of policy documents allows us to understand better the relationship between policy and public perception as well as broader issues surrounding privacy policy and security policy.

With respect to PRISMS' primary interest in the relationship between security and privacy, the analysis finds that the meaning of both security and privacy varies across different contexts. Security varies as a concept across different countries, and across actors within different countries. It is expanding to include issues such as information security, cyber security and critical infrastructure protection. Privacy, as a concept, is also understood as being under threat from a variety of different sources that appear to diverge across contexts. While some countries may construct the private sector as the primary privacy invader, others focus on policy or the state. Furthermore, there is some evidence that different technologies emerge as privacy threats in different countries. Finally, while many countries utilised the "balance" metaphor to explain the inter-relationship between privacy and security, EU policy documents, in particular, frequently construct privacy and security as complementary rights that must be "respected", which exerts some pressure on Member State governments to adopt similar principles.

3.2 METHOD

As described in section 1.3.3 above, this horizontal analysis is based on a short-list sample of 56 policy documents from Europe, six Member States (Romania, the Netherlands, Germany, France, Italy and the UK) as well as the USA for more in-depth analysis. The short analysis for each of the sampled documents contained six fields. These included the domain addressed by the document; its target audience; its stated purpose; its context, including any other documents referenced; its key points; and an assessment of its importance or significance. The short analyses provide a porthole view of privacy, data protection and security issues in particular countries.

The purpose of this chapter is to conduct a "horizontal", cross-cutting analysis across these documents, viewing the documents not in isolation, but instead by country (or regional context as is the case for Europe), by issue and over time in order to obtain an enhanced view of how policy-makers view privacy and security from a political perspective. As such this chapter is divided into two parts. Part one (Section 12.3) examines the policy documents by context and focuses upon commonalities. It attempts to identify regularities and patterns with the privacy, data protection and surveillance as well as security policy documents of a particular country or region. These contextual findings are then compared and contrasted to one another in the comparative analysis section. The second section (12.4) takes a cross-cutting look at all of the security policies of all of the documents, and all of the privacy, data protection and surveillance policies in order to identify points of divergence between countries or between countries and Europe. The comparative analysis section ends by providing a chronological analysis. This involved placing the documents on a timeline and examining the order in which documents were produced, in order to gain a sense of how the framing of security, surveillance, privacy and data protection may have changed over time.

However, this analysis of 56 documents is based upon a small sample of documents from the long list, and although it may draw some limited generalisations from patterns and trends in these documents, other perspectives might be present in documents not included. As such, any assertions are made upon the basis of the analysed documents, not the policies of particular countries or regions as a whole. Furthermore, the documents are constrained by the limitations of politics itself and may not reflect the priorities and concerns of individual policy-makers, committees or government agencies or departments, but instead must be understood as contextualised within particular political, national and regional constraints.

This information is used in the final section to draft some preliminary hypotheses and questions for the Europe-wide PRISMS survey on privacy and security. The results from the survey will be used to assist in determining the factors that affect public assessment of the security and privacy implications of a given security technology. The project will use these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account the wider social context.

3.3 ISSUE ANALYSIS BY CONTEXT

This section identifies key themes, key issues in privacy, data protection, security and surveillance identified in the documents from the EU and each of the countries examined in the report. Key themes either emerged across multiple documents or are the core subject of a

significant single document. Significantly, many of these key themes emerged as problematic – i.e., the privacy or security issues that are identified as political problems in these documents.

The information for each entity is ordered in approximate chronological order with regard to the documents, with allowances for keeping regularities and key themes together. Where it has been possible to identify changes over time, these have been noted and included in this analysis. Finally, the larger number of policy documents from the EU compared to other countries produced a larger number of key themes, which are analysed at greater length.

3.3.1 United Kingdom

We examined five documents from the UK, including (1) a 2006 report by the Surveillance Studies Network for the Information Commissioner's Office entitled *Report on the Surveillance Society* [Doc #560], (2) a 2008 report from the House of Commons Home Affairs Committee entitled *A Surveillance Society?* [Doc #456], (3) a 2009 report from the House of Lords Constitution Committee entitled *Surveillance, Citizens and the State* [Doc #507], (4) a Joint Committee on Human Rights examination of the proposed Protection of Freedoms Bill from 2011 [Doc #523], and (5) a Ministry of Defence White Paper on National Security from 2012 entitled, *National Security through Technology* [Doc #546]. These documents address a diverse set of themes, such as the surveillance society, the "war on terror", social sorting, terrorism, crime prevention, security, constitutional issues, the state-citizen relationship, the need for reform and the governance of surveillance, the adequacy of existing protections, individual responsibility, data losses, privacy impact assessments, and the global security market.

Privacy, data protection and surveillance

UK documents include several high profile reports on surveillance. The influential 2006 *Report on the Surveillance Society* attempts to inform the public about the social consequences of increased surveillance.[24] It acknowledges the negative potential of surveillance technologies being deployed in areas of medical records, crime and terrorism prevention and border control, especially in relation to the war on terror. This policy document characterises surveillance as engendering "social sorting" and having the potential for significant impacts upon life chances, dehumanisation, implying mistrust, and exerting limitations upon freedom. This report was influential in promoting the concept of the surveillance society in the UK (and elsewhere), even though the term had been coined some years before the report.[25]

The Constitution Committee of the House of Lords scrutinises the constitutional implications of public bills before the House of Lords, and other governmental measures. In 2009, the committee investigated the constitutional implications of developments in surveillance, which they felt had not been sufficiently considered. The report attempts to identify the constitutional principles which governed surveillance in the UK.[26] The Constitution

[24] Surveillance Studies Network, *A Report on the Surveillance Society for the Information Commissioner*, Information Commissioner's Office, September 2006.
[25] David Flaherty used the term in his book *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, Chapel Hill, NC, 1989.
[26] House of Lords Constitution Committee, *Surveillance: Citizens and the State*, Second Report of Session 2008-09, HL Paper 18, The Stationery Office, London, 6 February 2009.

Committee adopts a constitutional perspective on privacy. They regard privacy as part of individual freedom, surveillance as having the potential to erode privacy, and that individual freedom and the rule of law were prerequisites of the constitutional framework of democracy and good governance. The inquiry is primarily focused upon state surveillance, but acknowledges the potential impacts of private sector surveillance. In this document state surveillance is constructed largely, but not exclusively, as a threat to privacy and to broader social relationships, including trust in government.

The House of Commons Home Affairs Committee conducted an inquiry into the growth of public and private databases and forms of surveillance directly relevant to the work of the Home Office, producing a report in June 2008.[27] This inquiry was driven by the perception of the increasing importance of surveillance – the collection, storage and use of personal information – to government policy in crime prevention, border control, and delivering public services. The HAC report mentions the HMRC child benefit data loss of October 2007, and the alleged recording of a Member of Parliament's privileged conversations at HMP Woodhill in 2005/6 as contributory factors in motivating the inquiry.[28] According to the report, the increased potential for surveillance of citizens in public space and public communication has caused increased concern about the danger of becoming a "surveillance society" if trust is not maintained, although it did not consider the UK as a surveillance society at this point in time.

The Protection of Freedoms Bill was introduced in 2011. The scrutiny report by the Joint Committee on Human Rights broadly agrees that the bill enhanced legal protections for human rights and civil liberties; however, the report draws attention to other issues, including measures which may not be compliant with the UK's human rights obligations, or sections which risked infringement of individual rights. In relation to the National DNA Database, these included the retention and processing of biometric materials, the difficulty of adequate anonymisation of DNA samples, and the absence of accurate statistical information on the operation of the database. A key concept throughout this report is proportionality. The recommendations of the report were debated in Parliament and the Protection of Freedoms Act became law on 1st May 2012.[29]

There is no mention of privacy within the Ministry of Defence's report *National Security Through Technology*.[30] There are discussions of the potential trade-offs and balances between best value for money and open, transparent, competitive procurement processes and the requirements of national security (operational advantage and freedom of action).

Regulation and responses

The UK documents also argue that the current use of surveillance technologies and practices required improved regulation and response to better protect privacy and personal data. The Surveillance Studies Network *Surveillance Society* report calls for new privacy regulation for current and emerging surveillance technologies.[31] The authors are not convinced that current regulations on surveillance were capable of restricting the surveillance of individuals. The

[27] House of Commons Home Affairs Select Committee, *A Surveillance Society?*, Fifth Report of Session 2007-08, HC 58-I, The Stationery Office, London, 8 June 2008.
[28] Ibid.
[29] http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
[30] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (Cm 7952) October 2010.
[31] Surveillance Studies Network, op. cit., 2006.

report suggests that drafting improved regulation is under increasing time pressure given the continued development of new surveillance practices, and advocates privacy or surveillance impact assessments as one potential avenue for improved regulation. The Constitution Committee report also examined the suitability of the Data Protection Act 1998 and the need for additional legislation to protect citizens in relation to surveillance and the collection of data.[32] The document argues that Government should not confine itself to questions of legal authorisation and compliance when seeking to improve surveillance, as law alone cannot prevent abuse of surveillance powers, and that surveillance measures may be legal but also unsuitable or damaging to public trust. The report recommends that statutes involving data processing and surveillance should be subject to post-legislative scrutiny. The document highlights the importance of necessity and proportionality, and expresses concern about the overuse of secondary legislation.

One of the foci of the Constitution Committee's report is the changing nature of the relationship between the citizen and the state, and the role of surveillance in this relationship. One anticipated impact of surveillance is the reduction of trust in the state. Undermining trust can cause resistance and lead to creation of an antagonistic relationship between individual and state. The document recommends that before introducing any new surveillance measure the Government should publish its likely effect on public trust and compliance. The *Surveillance Society* report of 2006 is somewhat pessimistic as the persistence and increasing sophistication of surveillance technologies, blurring boundaries between the private and public sectors, as well as government policies promoting information sharing as a solution to social problems, has led to the authors' scenario of privacy-free societies in the future.[33]

The HAC report advocates government data minimisation, proper consideration of risks of excessive surveillance and the provision of ground rules for government and agencies so as to preserve trust. Government should make use of technical means to protect personal information and should conduct risk assessments before developing new information technology projects. The document recommends that the Home Office exercise restraint in collecting personal information and address the question of whether or not surveillance activities are proportionate responses to varying threats. The report contains an explicit discussion about balancing the protection of the public and individual liberty. The inquiry asked contributors to reflect on their processes for balancing these risks. Arguments against benefits included achieving similar goals through less information intensive processes and the opportunity costs of surveillance measures. The document argues that decisions to collect information about people's activities should be taken only after an appropriate balance is struck between the potential harm, including intrusion of privacy, and intended benefit of the project. The use of personal data by the Home Office is particularly significant both in terms of clear benefits, but also potentially more dangerous risks. Risks examined include practical effects of misuse or mistakes; a black market in personal information; data loss and identity fraud; incorrect information and false matches; cumulative effects and disproportionate burdens upon the disadvantaged; impacts on privacy and individual liberty; and as in the Constitution Committee report, shifts in citizen-state relations of trust.

As does the Constitution Committee, the HAC report also examines the strength of existing safeguards, including regulation, data protection principles, public sector responsibilities, technological safeguards (privacy enhancing technologies and digital identity management).[34]

[32] House of Lords Constitution Committee, op. cit., 2009.
[33] Surveillance Studies Network, op. cit., 2006.
[34] House of Commons Home Affairs Select Committee, op. cit., 2008.

The document welcomes technological methods, and advises government to track developments in these, but does not believe they are a panacea, and may introduce "privacy divides". The document makes the argument that where there is no choice to share information, the collecting organisation is particularly responsible for securing that information. The document also examines the case for new safeguards. These parliamentary documents recommend the assessment of the adequacy of the Data Protection Act, and encourage the use of privacy impact assessments (to the extent that they are not bureaucratic exercises, and are carried out as part of preliminary risk assessment), as well as proposing a set of guidelines for future personal information databases.

Security

Against the background of the National Security Strategy[35] and the Strategic Defence Review[36], the 2012 report from the Ministry of Defence explicitly links national security with technology, particularly in relation to industry and defence procurement.[37] The document identifies the UK's security context as a dangerous and uncertain world with continued threats from Al Qaida and groups in Northern Ireland and with constrained government budgets. At the same time, the White Paper describes law enforcement as being better equipped than ever, the UK being the world's second largest defence exporter, and the fifth in security. The UK domestic market for security products is estimated at £1.8 billion p.a. The document notes the significant impact of defence and security procurement upon industry and the economy, and identifies a vital government role in supporting this (including Ministerial support for exports, increased potential for SME involvement, and creating the conditions for greater private sector investment). The concept of national security is defined in terms of operational advantage and freedom of action for the United Kingdom.

Summary

The UK context features increased scrutiny and attention from various parts of the government and parliament to the increased potential for surveillance per se, and its potential social impacts. These documents often included reflection upon appropriate legal and regulatory reform, and support for greater monitoring and assessment of surveillance practices. The texts depicted a UK security context in which technology was an important tool in a dangerous and uncertain world.

3.3.2 Netherlands

From the Netherlands, we examined five key documents, 1) the House of Representatives report on fighting terrorism and security [Doc #598], 2) the Adviescommissie Informatiestromen Veiligheid report on data decisiveness and data safety [Doc #670], 3) the Committee on Security and Privacy's advice to the Ministries of Justice and the Interior on personal data treatment and security [Doc #658], 4) the Council for Public Administration's advice to Parliament on security and trust [Doc #644], and 5) the Senate's evaluation of data protection law [Doc #594]. The documents addressed the themes of mature data protection; counter-terrorism and information exchange as a counter-terrorism tool; pressure upon privacy; trust in government, which is threatened by some security measures; and the privacy v. security debate.

[35] Ibid.
[36] Ibid.
[37] Ministry of Defence, *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security*, The Stationary Office, London, February 2012.

Privacy, data protection and surveillance

All of the documents examined for the Netherlands include detailed debate on data protection. The Dutch documents primarily represent privacy and protection of data as higher on the political agenda than ever before.[38] The texts depict an existing mature and functional data protection regime, in which many issues are already covered by legislation or regulation, and attention therefore needs to be paid to the effectiveness and implementation of these instruments. Policy makers acknowledge that security measures exert pressure upon this data protection and privacy regime, as do developments in technology (particularly databases).[39] A key part of this discourse appears to be maintaining (rather than establishing) a balance between privacy and security.

Data protection and privacy in the Dutch documents are closely related to the EU context, and they reference the Lisbon Treaty as recognising the right to the protection of personal data as well as the right to privacy. The direction of policy influence from Europe to the Netherlands is not only one way. One post-9/11 document suggests that the Dutch government desired EU privacy regulations be adapted in the interest of increased national security.[40] A report from an advisory council to the Dutch government on trust and security suggests that the EU can contribute towards promoting trust in the national government by stressing the importance of protecting basic rights, collaboration with Member States and sound information provision. At the same time, trust can be undermined by the portrayal of the EU by political actors.[41]

According to the documents, current data protection and privacy challenges in the public sector include: digitalisation and the effects upon citizenship; appropriateness of databases for particular uses; insufficient control over authorisation; inadequate division of functions; an exaggerated belief in the power of technology; immaterial rather than material harm; and diffuse damage. These policy documents also specifically relate privacy regulation to counter-terrorism, and the need for more effective counter-terrorism response to terrorist attacks such as 9/11, in addition to broader issues of national security. They stress that the effectiveness of counter-terrorism measures would need to be weighed against privacy law, and that security measures (such as biometric identification and financial monitoring) could have potential privacy impacts. Privacy is constructed as something which could (potentially, in yet unknown ways) limit the tracing and prosecution of terrorist activities, but at the same time, policy-makers identify the granting of additional powers (particularly additional discretionary powers, without sufficient oversight) in the pursuit of counter-terrorism objectives as a potential risk to the balance between security and privacy.[42]

[38] Eerste Kamer, *Evaluatie Wet bescherming persoonsgegevens; Verslag van een expertmeeting inzake de rol van de overheid bij digitale dataverwerking* [Evaluation of the Data Protection Law – notes of the expert meeting organized by the Upper Chamber of Parliament with chair Article 29, EDPS, etc.], The Hague, 22 March 2011.

[39] Adviescommissie Informatiestromen Veiligheid, *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse [*Data decisiveness. Data safety: observations and analysis*]*, Report commissioned by the Ministry of the Interior, Ministry of Defence, Ministry of Justice, The Hague, April 2007.

[40] Tweede Kamer, *Bestrijding internationaal terrorisme; Verslag algemeen overleg op 17 oktober 2001, over terrorismebestrijding en veiligheid* [Fighting international terrorism; report of a general meeting about fighting terrorism and security], Tweede Kamer, The Hague, 1 November 2001.

[41] Raad voor het openbaar bestuur (Rob), *Rob-advies Veiligheid en vertrouwen* [Advice to Parliament re security and trust], The Hague, November 2010.
http://www.rob-rfv.nl/documenten/migratie/boekje_advies_veiligheid_en_vertrouwen.pdf

[42] Adviescommissie Informatiestromen Veiligheid, 2007.

Security

All of the Dutch security documents analysed discuss security as opposed to privacy. From the documentary sources, the 11 September attacks in the USA exerted an influence upon security discussions in the Netherlands, including precipitating meetings of several parliamentary commissions.[43]

A second security theme present in Dutch policy documents is the exchange of information as a counter-terrorism strategy. This includes the exchange of information between intelligence, internal security and law enforcement authorities, and the international exchange of information. The Ministries of the Interior, Defence, and Justice also mention increasing intelligence-led policing. Information exchange is cited in their report as the key way to prevent terrorism, but that in 2001, it was inefficient and often incorrect.[44] However, the Tweede Kamer questions the legitimacy of some information exchange processes, particular when exchanges were treated as exceptional.[45] Increased information exchange, particularly for criminal investigation purposes was not adequately covered by regulatory regimes in practice. The 2007 report for the Ministries of the Interior, Defence and Justice suggests that there was no systematic approach to how investigative agencies should retrieve and use information from the various sources to which they had access.[46] Similarly, policy-makers raises concerns that there was not enough government attention to the significance of data and databases in the security domain, or to the consequences of this use. The report warns that such databases often did not meet existing necessary criteria from a regulatory standpoint, for example, in terms of social controls, effectiveness and appropriateness. This suggests that even a mature data protection regime is not static or comprehensive, and is likely insufficient if criteria set out in that regulatory regime are not met.

Summary

Data protection and privacy are high on the political agenda in the Netherlands, with the perception that law and best practice need to be maintained against pressure from challenges including technological developments and security policy. This context is closely related to the EU. Security documents acknowledge the influence of terrorism and the impact security practices have upon information exchange.

3.3.3 France

The partners examined six documents from France, 1) Guidelines for research and development in information systems security from the Secretariat General for Defence and Security [Doc #716], 2) the French White Paper on Defence and Security [Doc #707], 3) the Senate's proposed legislation to better protect privacy in the digital age [Doc #696], 4) the Secretariat General's General Security Regulatory Framework [Doc #718], 5) guidance on video surveillance [Doc #756]and 6) an opinion on draft legislation authorising the creation of the EDVIGE database, from the Commission nationale de l'informatique et des libertés (CNIL) [Doc #739]. The documents address themes related to individual responsibility, the right to be forgotten, compliance and guidance, increased powers for CNIL, increased individual responsibility supported by increased information and transparency, clarification

[43] Tweede Kamer, op. cit., 2001.
[44] Adviescommissie Informatiestromen Veiligheid, op. cit., 2007.
[45] Tweede Kamer, *Bestrijding internationaal terrorisme; Verslag algemeen overleg op 17 oktober 2001, over terrorismebestrijding en veiligheid* [Fighting international terrorism; report of a general meeting about fighting terrorism and security*]*, Tweede Kamer, The Hague, 1 November 2001.
[46] Adviescommissie Informatiestromen Veiligheid, op. cit., 2007.

and expansion existing of legislation, new databases, "Safeguards" and "guarantees", trust, the new security environment and Europe as a global security actor.

Privacy, data protection and surveillance

Proposed legislation in 2010 aimed to increase the involvement of individuals in the protection of their own privacy, and increase the powers of CNIL, the French data protection authority.[47] This argues that individuals should become key actors in protection their personal data and the documents identified that education in schools could positively influence this goal. The legislation also clarifies the position of personal data processed by the state for security and defence purposes. Some of these proposals actually pre-empted the publication of Directive 2009/136/EC amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, but are presented in the text as aligned with and capable of serving as a working basis for implementing the Directive.

The proposed legislation includes clarification of the "right to be forgotten", i.e., when personal data have been processed, any person establishing their identity has the right, for legitimate reasons, to require their removal, except in a few stated cases.[48] The ANSSI (Network and Information Security Agency) and the Agency for the development of e-administration expresses a desire for citizens and users to be able to trust the electronic services offered by the administration, particularly in regard to protection of their personal data.[49]

Legislation in March 2011, Law No. 2011-267 extended the regulatory responsibility of CNIL to cover all video surveillance on public highways.[50] In their report on a year's activity relating to this responsibility, CNIL suggests an increased number of cameras are being installed, and provided a range of guidance on the best practice use of surveillance cameras. The guidance appears intended to facilitate video surveillance that is respectful of individual privacy. This document also highlights a distinction between "video protection" and "video surveillance". Video protection refers to cameras installed in the streets or in places open to the public. It is subject to the Code of Interior Security. It needs the opinion of a departmental committee chaired by a magistrate and a prefectural authorisation, and it is controlled by the CNIL. Video surveillance refers to cameras installed in places that are not open to the public (a company office, residential buildings). It is subject to the Data Protection Act and must be declared to the CNIL.[51] The CNIL report on video surveillance also mentions the need to increase the amount of information on surveillance and data protection available to lay citizens.[52] This includes the clarification of existing legislation.

Reform of the French intelligence services authorised the creation of two databases processing personal data called « EDVIGE » (Documentary exploitation and valorisation of general information) and « CRISTINA » (Centralising inland intelligence for homeland

[47] Senat, Proposition de loi, visant à mieux garantir le droit à la vie privée à l'heure du numérique, [Proposed legislation to better protect the right to privacy in the digital age], 23 March 2010.
[48] Senat, op. cit., 2010.
[49] Secrétariat générale de la défense et de la sécurité nationale, *Référentiel Général de Sécurité* [The General Security Regulatory Framework], Agence nationale de la sécurité des systèmes d'information Paris, 6 mai 2010.
[50] Commission nationale de l'information et des libertés (CNIL), *Vidéosurveillance / vidéoprotection: les bonnes pratiques pour des systèmes plus respectueux de la vie privée* [Video surveillance / CCTV: best practices for systems more respectful of privacy], Communiqué de presse, June 2012.
[51] Ibid.
[52] Ibid.

security and national interests).[53] The report from CNIL on these databases raised a number of concerns. This document called for more information on the databases to put into the public domain so as to increase transparency and allow an informed public debate. Whilst acknowledging the purposes of the databases, CNIL's report suggested that there were inadequate safeguards in relation to the collection of personal information on ethnic origin, sexual life and health, and the collection of data on public figures. The collection of information on minors should also be surrounded by strengthened guarantees. Due to a massive mobilisation of public protest in France, the government had to withdraw the EDVIGE decree in November 2008. EDVIGE was then replaced by EDVIRSP which was integrated in the Law on the orientation and programming for performance of domestic security on 14 March 2011.

In relation to surveillance, the Defence and Security White Paper advocates improved technological development, and additional programmes in relation to intelligence and preparation for the future, knowledge and anticipation including "knowledge based security", observation, early warning, development of surveillance and armed drones as well as both offensive and defensive cyber war capabilities.[54]

Security

The White Paper on defence and security sets out a traditional concept of security as national security, closely tied to a post-cold war context typified by globalisation.[55] Domestic and foreign security are blurred in this more complex security environment. The document itself also draws together security and defence under the rubric of "national security". The response to this situation identified in the White Paper is to ensure that France harnesses the "information revolution" to manage increased uncertainty. Perceived threats include espionage and influence peddling, serious criminal trafficking, new natural and health risks, heightened technological risk and the exposure of citizens abroad. The new parameters of security include the growing connectivity of threats and risks (such as terrorist links, contagion between unstable regions), thus requiring a wide ranging response, with combined and preventative policies. The document highlights the continuity between internal and external security, with the traditional distinction no longer relevant in the new strategic environment. The document suggests the need to define overarching security strategies and integrate all dimensions of security. There is the possibility of sudden strategic upsets (uncertainty, sudden breaks, new weapons, technological developments in biotech, nanotech and space), and of changes affecting the nature of military operations, for example, increasing urban settings for conflict. The document states that technological superiority has failed to give guarantees of victory and that the human factor remains decisive.

The security White Paper sets out France's ambitions for Europe and being at the forefront of a progressive EU political union, and as a presence on the world stage. The document represents the EU as a relatively new but increasingly important international security actor. It gives strong support for the Common Foreign and Security Policy. France wants Europe to be equipped with civilian and military capability to be a major player in international crisis

[53] Commission nationale de l'information et des libertés (CNIL), Deliberation No. 2008-174 of 16 June 2008 giving an opinion on a draft decree of the Council of State in favour of establishing the Central Directorate of Public Security of automated processing of personal data referred to as "EDVIGE", July 2008.
[54] Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, Le livre blanc sur la défense et la sécurité nationale, [The French white paper on defence and national security – unofficial translation], Paris, 17 juin 2008.
[55] Ibid.

management. The document recommends an intervention force, a capability for two to three simultaneous peacekeeping operations, and increased planning capability and restricting the European defence industry. The strategy constructs the EU and NATO as complementary.[56]

The aim of The General Security Regulatory Framework (RGS) is to regulate electronic exchanges of information between government agencies and citizens.[57] This document equates security with information security, and the protection of information. There is less of a conflict between security and privacy here as the framework represents security as a part of data protection.

The Interdepartmental Committee on Security of information systems, set up by Decree No. 2001-694, produced public policy reports for research and development in terms of information systems security.[58] The 2008 report aims to guide and incentivise strategic choices in research and development in the field of information systems security. The text defines information security as encompassing information control, confidentiality and privacy protection, and as important in establishing public trust in information systems. Information security also includes making sure that information systems are available and usable. In this context, information security is put at risk by rapid technological developments such as data aggregation and the ubiquity of digital identity systems. According to this report, it is essential and necessary to master the integration of these technologies to allow efficiency, security and therefore trust in the information system security.

Security is also related to information security and data protection practices in the CNIL report on EDVIGE, where CNIL asks for more specific information about the security levels surrounding the technical operation of the state database.[59] Similarly, the RGS provides good practices for the security of information for service providers and administrative authorities, with the intent of allowing public authorities to raise their levels of information security.[60] In this document security practices are equated with risk assessment and risk management.

Summary

French data protection politics involves calls for stronger rights and greater control on the part of the data subject, alongside on-going regulation and the clarification of the applicability of data protection legislation and the provision of guidance on best practices. France has also seen reform of the intelligence services, and raised questions about the appropriate extent of state intelligence databases. The security documents depict drives for knowledge-based security, including research and development in surveillance and information security in response to an uncertain global context.

[56] Ibid.

[57] The General Security Regulatory Framework is intended to regulate electronic exchanges of information between government agencies, and with citizens.

[58] Secrétariat générale de la défense et de la sécurité nationale, *Orientation des travaux de recherche et de développement en matière de sécurité des systèmes* d'information [Guidelines for research and development in terms of security of information systems], Agence nationale de la sécurité, des systèmes d'information, Paris, 10 April 2008.

[59] Commission nationale de l'information et des libertés (CNIL), Deliberation No. 2008-174 of 16 June 2008 giving an opinion on a draft decree of the Council of State in favour of establishing the Central Directorate of Public Security of automated processing of personal data referred to as "EDVIGE", July 2008.

[60] Secrétariat générale de la défense et de la sécurité nationale, op. cit., 2010.

3.3.4 Italy

We examined six documents from Italy, 1) the Italian Defence Ministry's White Paper (Libro Bianco) [Doc #774], 2) an annual report of the Garante per la Protezione dei Dati Personali [Doc #788], 3) the Garante's decision on videosurveillance [Doc #819], and 4) decision on data sharing and tracking of transactions in the banking sector [Doc #822], and 5) the Italian Council of Ministers' report on information security policy [Doc #770]. The documents address issues of data protection inspections and decisions, data protection clarification and guidance, the new security environment, the centrality of defence to security.

Privacy, data protection and surveillance

The documents from the Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali*) represent the Italian data protection regime as developed and in place by 2001, but amended through new legislation, supplemented by reviews, inspections and decisions. The commissioner's report on their activities during 2001 summarises a number of legislative developments during that year. Legislative decree no. 467/2001 modified the Data Protection Act (no. 675/1996) and Italian Legislative decree no. 171/1998 (the act responsible for transposing EC Directive 97/66/EC into Italian law). The decree states that this is necessary because the original implementation of Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector was insufficient. The report seeks to explain legislative policy, perhaps to non-policy makers and/or lay persons. It also attempts to reinforce the Garante's commitment to reviewing legislation, conducting inspections and making recommendations around safeguarding personal data.

The Italian DPA's report on information sharing in the banking sector attempts to clarify the application of data protection rules and principles, including appropriate and necessary measures.[61] This was in response to complaints to the DPA about banks accessing information without authorisation. The DPA finds that banks were acting as separate data controllers, and that data sharing between members of that group should be treated as communication with third-party recipients, thus requiring informed consent before being shared. The opinion considers the sharing of customer data between branches or offices of a bank as a flow of data within a single organisation and as it entails no third-party communication does not require the data subject's consent. The document also gives the results of the investigation into internal audit procedures. Nearly all banks have apparently put measures in place to protect consumer assets; however, not all banks have auditing procedures in place to regulate processing or requests for personal data. The document concludes with a set of measures that the DPA considers necessary, and those that it considers appropriate.

Similarly, the DPA also produced guidance in 2010 on the use of video surveillance (CCTV) systems, and the obligations placed upon their users by data protection legislation in the absence of other specific legislation dealing with CCTV, in response to a range of queries over the regulation of CCTV.[62] The document insists that the operation of CCTV should ensure a high level of protection of fundamental rights and freedoms and not interfere with the rights and freedoms of data subjects to an "unjustified extent". This is primarily to be accomplished by a prior-checking exercise.

[61] Garante per la Protezione dei Dati Personali, Data Sharing and Tracking of Transactions in the Banking Sector, *Official Journal*, No. 127, 3 June 2011.
[62] Garante per la Protezione dei Dati Personali, Decision on Video Surveillance, 8 April 2010.

Security

The 2002 review of the Italian armed forces and their activities argues for the centrality of defence, above all the centrality of the Italian armed forces, in promoting Italian security, as well as attempting to provide a strategic vision of the context of military security and defining the conceptual and international reference points that will guide the process of continued transformation of the military.[63] The document identifies a changed international security environment from the cold war, with the rise of ethnic and nationalist tensions in several parts of the world, the events of 11 September 2001 signalling a rise in international terrorism, and a greater public sympathy for overseas military interventions. The text represents threats to security as complex and transnational, and non-reducible to static homeland defence. The report also advocates the integration of Italian military security efforts with the EU, UN and NATO, which should be a priority for defence spending. The text concludes that the appropriate response to the new security environment is reducing the quantity and increasing the quality of Italian military forces, and aligning capabilities with the new security environment.

The subsequent 2010 report to the Italian Parliament on information gathering and intelligence[64] for security also identifies key security risks for Italy. This list is a fairly traditional account of threats to national security, including the vulnerability of the Italian economy; increasing cyber attacks and the potential for terrorist exploitation of cyber attack strategy; international threats such as nuclear proliferation, the exposure of the Italian military overseas and the rise of anti-western sentiment; terrorism; organised crime; illegal immigration and political extremism. Risk multipliers include climate change, resource scarcity and large-scale health risks.

Some Italian texts also integrate information security, data protection and cybercrime into security. Guidance on data protection and CCTV requires that data controllers provide adequate information security, including measures that minimise destruction, loss, unauthorized access, unlawful processing and unlawful retention.[65]

Summary

The Italian policy documents analysed here constructs the Italian data protection and privacy regime as mature, with an active data protection authority that regularly reviews legislation and the use of information systems. In relation to security, the Italian documents selected here appear to foreground the changes in the security context since September 2001, but also to expand traditional conceptualisations of security to include issues such as cyber-security, political extremism and climate change.

3.3.5 Germany

We examined six documents from Germany, 1) a Parliamentary control panel notification about anti-terrorism measures and consequences [Doc #854], 2) a speech by the Federal data protection commissioner on intelligence and police data sharing [Doc #874], 3) Federal government responses to Parliamentary questions on telecommunications and internet data retention [Doc #849], 4) a Bundestag discussion on body scanners [Doc #840], 5) the Federal government report on the framework programme on research for civil security [Doc #852],

[63] Italian Defence Ministry, *Libro Bianco, 2002* [The White Paper, 2002], Centro Studi per la Pace, Rome, 2002.
[64] Italian Council of Ministers, Relazione sulla Political dell'Informazione sulla Sicurezza-2010 [Report on the Information Policy on Security-2010], 2010.
[65] Garante per la Protezione dei Dati Personali, Decision on Video Surveillance, 8 April 2010.

and 6) the report on data protection and personal rights by the committee of inquiry on internet and digital society [Doc #864]. The documents address a diversity of issues including data leaks, body scanners, constitutional protections and compatibility of EU regulation, the effectiveness of surveillance, active promotion of citizens' privacy, linking privacy and cyber security, PETs and privacy by design, intelligence oversight and information sharing, data sharing the with US, Safe Harbour, the Internet, informational self-determination and terrorism.

Privacy, data protection and surveillance

Issued in 2006, the European Data Retention Directive (Directive 2006/24/EC) required Member States to store telecommunication data of their citizens for a period between six and 24 months. The German Federal Constitutional Court ruled that the new German law that would have implemented the Directive was unconstitutional.[66] This document included discussion about the effectiveness of data retention, and concern about the limited evidence base. The German National Parliament adopted a particularly critical perspective on the EU Directive.

The German government regards the ability to protect citizens' offline and online security while at the same time protecting and respecting their privacy and personal data as a key challenge.[67] It regards the integrity, authenticity and confidentiality of data as very important for cyber security, and as a legal and social requirement. The report on the High Tech Strategy 2020 acknowledges a need to encourage privacy-enhancing technologies (PETs) on the basis of privacy by design. German documents mention the right to informational self-determination, and the way that this interacts with online profiling.[68] This High Tech strategy report sees data protection as a social challenge as well as a legal issue, and one that has become more salient for more citizens, as the Internet has increased the amount of personal data being processed.

German documents reveal national parliamentary discussions on the topic of data protection, privacy and surveillance. Data leaks following large-scale leaks at some prominent German companies prompted calls for more legislation to protect the personal data of employees.[69] The Bundestag, the German national parliament, discusses the privacy of citizens in relation to airport body scanners, and broadly concludes that privacy considerations and data protection measures in place are appropriate. Body scanners should only be installed when they do not pose a health risk, have been shown to work properly, and do not infringe upon travellers' privacy.[70] There are discussions about the appropriate terminology as between "body scanner" or "naked scanner".

[66] Bundesregierung, *Vorratsdatenspeicherung und Sicherheitslücken* [Data retention and security vulnerabilities], 22 April 2010.

[67] Bundesregierung, Rahmenprogramm der Bundesregierung "Forschung für die zivile Sicherheit (2012 bis 2017)" [Report of framework programme "Research for civil security"], Berlin, 25 January 2012.

[68] Enquete-Kommission, "Internet und digitale Gesellschaft" Datenschutz, Persönlichkeitsrechte. *Fünfter Zwischenbericht der Enquete-Kommission "Internet und digitale Gesellschaft" Datenschutz, Persönlichkeitsrecht* [Report of the project group 'Data protection and personal rights' of the Committee of inquiry 'Internet and digital society' (fifth report)], Bundestag, Berlin, 15 March 2012.

[69] Bundestag, *Plenarprotokoll der 14. Sitzung vom 19.01.2010* [Report of plenary session of the German National Parliament. Discussion about body scanners (named explicitly 'nacktscanner' or 'naked scanners')], Berlin 19 January 2010.

[70] Ibid.

The report by the Parliamentary Control Panel (PKGr) contains information about how German intelligence services had been dealing with the rules and regulations in the field of telecommunication and data retention.[71] More specifically, it contains the findings of an investigation of this committee about the extent to which intelligence services have violated citizens' privacy and, if they did, whether it was based on legal grounds (criminal investigation, anti-terrorism). The committee conducted an investigation into the extent to which citizens' privacy may have been violated, and the legal grounds for any such violation. This investigation concludes that, in general, the grounds for privacy violations and the way they were balanced against privacy rights are acceptable, but that day to day procedures of the intelligence agencies are time-consuming and bureaucratic with negative consequences for safety and security. The panel suggests the simplification of legislation to make investigation procedures easier. The panel relates balancing and assessment to the German constitution.

A speech by the Federal Data Protection Commissioner in 2009 demonstrates concern about the sharing of data between police and intelligence agencies.[72] This was linked to dangers from historical experience with the Gestapo and Stasi, and is seen as violating the constitution. The document identifies a strict constitutional separation between police and intelligence functions, but increasing pressure for the merging of police and intelligence data following 9/11, along with increased counter-terrorism co-operation initiatives. The key reason for separating (activities of) the intelligence services and the police is to separate intelligence gathering (which is not necessarily started in response to a specific illegal act by an individual) and law enforcement (which would require probable cause before coming into action). The Commissioner is concerned that the merging of the two has significant impacts upon citizens' privacy. The police were granted additional powers to conduct preventative operations post 9/11. The document contends that the joint counter terrorism database, set up in 2007, had been used for unconstitutional purposes when police officers used data gathered by intelligence services in "urgent" operational cases.

Also of concern is the protection of personal data shared outside of the EU, particularly with the United States. The report from the Committee of Inquiry into Internet and Digital Society, Data Protection and Personal Rights Group identifies the German position on data protection in relation to international contexts.[73] It identified a need to ensure a consistent level of data protection, and expresses concerns that the US would not meet the same standards of data protection, despite the Safe Harbour agreement.[74]

[71] Parlamentarische Kontrollgremium (PKGr), *Bericht gemäß § 14 Abs. 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5 und 8 dieses Gesetzes (Berichtszeitraum 1. Juli 2004 bis 31. Dezember 2005)*, [Notification about anti-terrorism measures and consequences], 7 September 2006.

[72] Schaar, Peter, Wie nachrichtendienstliche Erkenntnisse und polizeiliche Daten zukünftig verschmelzen werden – neue Herausforderungen für die Aufsichtsbehörden? Vortrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen der Conference of DPA's of Federal and Plurinational States ["How intelligence data and police data will merge in the future - new challenges for supervision?", Speech by the Federal Data Protection Commissioner at a Conference of DPAs of federal and plurinational states], Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 19 March 2009.

[73] Enquete-Kommission, op. cit., 2012.

[74] European Commission, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), 2000/520/EC. Official Journal L 215, 25 August 2000.

Security

The German government launched a national research programme about civil security in 2007 and the High-tech Strategy 2020 for Germany in 2010. Both of these programmes include cyber security as a particular focus and area of importance.[75] The German government aims to create and maintain an expert position in the field of security technologies; establish international collaborations; further knowledge and capacities within society by establishing a better scientific basis regarding knowledge about cyber security.

German documents also associate security with information security. The 2012 report from the Committee of Inquiry into Internet and Digital Society, Data Protection and Personal Rights Group, discusses the topic of data security is more frequently than data protection in many topic areas.[76]

Summary

The German context features national political discussions of the social, political and technological challenges of protecting citizens' online and offline security and their privacy and data protection rights. These discussions also include the constitutionality of data retention measures originating with the EU, and the adequacy of data protection in the US. There are also concerns about regulation of intelligence agencies and the amount of data sharing between intelligence agencies and the police.

3.3.6 Romania

From Romania, we examined four documents, 1) the minutes of a public debate organised by the Romanian government on individual freedom vs. national security [Doc #881], 2) the Romanian National Security Strategy [Doc #882], 3) the Romanian secret service roundtable on society, democracy and intelligence [Doc #883], and 4) the debate in the Romanian Parliament on the transposition of the data retention directive [Doc #880]. The documents addressed key themes of national security reform; international influences (EU and NATO) and membership; the Data Retention Directive; the country's post-communist context and intelligence services; and the concept of democratic security.

Privacy, data protection and surveillance

The reviewed documents suggest that in Romania debate over individual freedom and national security is explicitly represented as a balance. This is also linked to the balance between transparency and secrecy.[77] The national security strategy stresses the need to find a reasonable and efficient balance between the protection of freedoms and democratic rights and restrictions and punitive measures (e.g., by means of increased transparency and the right to information). This document also mentions the potential for privacy to limit security.

A specific example of EU influence in Romanian security, privacy and data protection in the documents is demonstrated by the debate around the transposition of the EU Data Retention

[75] Bundesregierung, op. cit., 2012.
[76] Enquete-Kommission, op. cit., 2012.
[77] Romanian government, *Stenograma audierii publice din ziua de 27 iunie 2006 «Libertate individuală versus securitate naţională. Echilibrul între transparenţă şi secretizare»* [Minutes of the public debate organized by the Romanian Government on the subject: "Individual freedom vs. national security – balancing transparency and secrecy"], 27 June 2006. Note that here, as well as in other footnotes, translations into English are unofficial.

Directive (2006/24/EC).[78] The first attempted transposition of the Directive was declared unconstitutional by the Romanian Constitutional Court, and the second attempt was criticised by the Senate, the Parliament's Commission for European Affairs, the Commission for Human Rights and Minority Affairs, the Romanian National Association of ISPs, and by the press (where it was described as a "big brother" law). The failure to transpose the Directive by the deadline led the EU to initiate infringement proceedings against Romania in 2011. Critical questions arising from the documents in relation to the transposition include the legal basis for requests for data from law enforcement; the retention period; the specificity of conditions for the destruction of data; penalties for the wilful misuse of data and the categories of authorities entitled to request data.

The role and extent of the powers of the intelligence services (the domestic focused Serviciul Român de Informaţii, SRI, and the foreign intelligence service Serviciul de Informaţii Externe, SIE) were a particular concern in the Romanian documents. The year 2006 saw a public consultation on the proposed legislative package for national security. The legislative package, proposed as part of new measures to counter terrorism, would have extended investigative powers, in particular those of the intelligence services. The document shows some concern that this might bring these powers into conflict with the constitution. The intelligence agencies are also seen by the government as requiring modernisation as part of the membership of NATO and the EU, and in response to the conditions and threats of the 21st century. Human rights advocates and journalists participated in this public consultation process. This concern over the discretionary powers of state intelligence agencies is specifically linked to the historical legacy and experience of Romania's communist past. The documents suggest that intelligence agencies have a negative image in the light of their ancestors in the communist era.

The document from the Director of the Romanian intelligence agency complains that the media do not help this situation by focusing upon "obsolete" topics. From the perspective of this document, the challenges are inter-agency co-operation, oversight, and the contradiction between the secrecy characteristic of intelligence operations, and the democratic need for greater transparency.

Security

The Romanian documents also mention high profile terrorist events outside of the country, such as 11 September attacks, and the London and Madrid bombings, portraying these events as part of a fast moving, internationalised set of security threats.

The Romanian security strategy includes security elements that can be understood as human security – health, food, and elements, and that can be understood as critical infrastructure – infrastructure, energy, financial and information security. The strategy states that security is necessary for the protection and defence of democracy, fundamental rights and freedoms of citizens, and to assert national identity. The strategy includes the concept of "democratic security" and the recognition that fundamental rights and freedoms are important for realising security.

[78] Parlmentul Romaniei, Camera Deputatilor, *Raportul comun suplimentar asupra propunerii legislative privind retinerea datelor generale sau prelucrate de furnizorii de retele publice de comunicatii electronice si de furnizorii de servicii de comunicatii electronice destinate publicului, 22.05. 2012* [*Report and debate about the transposition of the data retention directive*], Bucharest, 22 May 2012. http://www.cdep.ro/comisii/juridica/pdf/2012/rp010.pdf

In terms of institutions and intergovernmental organisations, Romanian policies of security, and, by extension, its political perspectives upon privacy, liberty and freedom, appear to be strongly influenced by the relatively new membership requirements imposed by its participation in NATO and the EU. These determinants are not always congruent, with some conflict identified in the strategy between the EU security strategy and the NATO New Strategic Concept. The national security strategy suggests that the anticipated security risks are international in nature and therefore require international co-operation. The Romanian security strategy of 2006 set out the requirements and changes in policy resulting from NATO and EU membership.[79]

Summary

The Romanian context exhibits the need to balance national security with freedom and democracy. There are discussions of the constitutionality of data retention proposals, and the appropriate roles and powers of the intelligence services, given the communist past. Membership of NATO and the EU are key aspects of both the security and privacy contexts in Romania, which also features a broadening concept of democratic security.

3.3.7 United States of America

We examined three documents from the US, Congressional Research Service reports on 1) the Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act [Doc #889], and 2) the Total Information Awareness Programs [Doc #896], and 3) the 9/11 Commission Report [Doc #943]. The documents addressed themes such as 9/11, new intelligence and security powers, counter-terrorism, immigration and border security, money laundering, surveillance oversight, surveillance funding and information sharing.

Privacy, data protection and surveillance

Following shortly on from the 9/11 attacks, these documents cluster around the impacts of 9/11 and post-9/11 security reforms of law enforcement and intelligence systems. The USA PATRIOT Act modified several laws relating to privacy and data protection, particularly with regard to financial transactions.[80]

Following 9/11, the Defence Advanced Projects Research Agency (DARPA) set up Total Information Awareness (TIA) programmes to develop tools for identifying and detecting terrorists (that would be brought together in a TIA system). The programmes were renamed to Terrorism Information Awareness and then later cancelled in response to public opposition.[81] The Congressional Research Service report of 2003 intends to clarify the funding, composition, and oversight of the TIA programme, given the potentially excessive impact upon individual privacy.[82] The TIA system would have involved significant government databases processing the personal information of individuals. The report's main concern is regarding the transparency of the funding arrangements for TIA. It also expresses concerns about the increasing collaboration between DARPA and other agencies (Department of

[79] Presedintele Romaniei, *Strategia de securitate nationala a Romaniei, Bucuresti 2007,* [Romanian President, Romanian national security strategy], 2007.

[80] Doyle, Charles, *Terrorism Legislation: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Congressional Research Service, Report RS21051, 26 October 2001.

[81] House of Representatives, Conference Report on H.R. 2658, Department of Defense Appropriations Act, (House Report 108-283), 2004. http://www.fas.org/sgp/congress/2003/tia.html

[82] Belasco, Amy, Total Information Awareness Programs: Funding, Composition, and Oversight Issues, Congressional Research Service, 21 March 2003.

Defense, FBI, Department of Homeland Security, and law enforcement), and the lack of monitoring of this collaboration. The report sees this collaboration as reducing accountability, and as raising questions about the specific roles of different agencies.

The 9/11 Commission report refers to surveillance in relation to counter-terrorism efforts but tends not to specify the type of surveillance in question. Privacy is mentioned briefly as a side note, suggesting that privacy should be "respected" when amending national security measures.[83]

Security

Commentary on the USA PATRIOT Act of 2001, passed into law very rapidly after 9/11, indicates linkages in the Act between national security, immigration and money laundering.[84] It also suggests the Act had a number of legal implications, including increased powers for intelligence and security purposes.

The report of the 9/11 Commission is an extensive examination of the past, present and future of America's security in the face of terrorist attacks.[85] Its core purpose is to present the fullest possible account of the events surrounding 9/11. Factors contributing towards the insecurity of the USA in this context included restrictions in communications between security agencies (and with involved actors such as airlines and airports) and the difficulty of sharing information. The report questions the previously dominant paradigm based upon the protection of information, rather than its sharing or dissemination. This paradigm was specifically constructed as protection in terms of protection of intelligence sources and national security, rather than protection of personal information or privacy. Proposed changes to border control, which included tighter security, increased surveillance and trans-organisational information flow, were only beginning to be implemented before 9/11. The report argues that most intelligence agents do not have the necessary clearance to access information on Al Qaeda, and departments do not have the capability to link up information. The document suggests post-9/11 reforms that would enable information sharing and intelligence flow between agencies. The 9/11 report also identifies border security as a national security issue. The report recommends biometric checks, and checks against criminal, immigration, and financial databases.

The main argument of the report's authors is that if the situation were different (if information flowed freely, if the departments knew exactly what their role was), 9/11 perhaps could have been avoided. From the text, one can suggest that the events on 9/11 caused a paradigm shift, from valuing and desiring the protection of information, to advocating the openness and sharing of information across all government departments. The 9/11 Commission report clarified the post-9/11 stance of the US with regard to international intelligence co-operation: all resources would be dedicated to eliminating the threat of terrorism and punishing those responsible for 9/11 (and those who harboured the responsibles). In order to do this, the US intends to work with a coalition to eliminate terrorist groups and networks.[86]

The Congressional report on TIA also expresses concerns about the security of large databases, and notes the difficulty of developing the security measures that DARPA states it

[83] 9/11 Commission, *The 9/11 Commission Report*, 22 July 2004.
[84] Doyle, op. cit., 2001.
[85] 9/11 Commission, op. cit., 2004.
[86] Ibid.

will use to secure the system.[87] This document understands security primarily in terms of national security, the prevention of terrorist attacks and the operation of terrorist groups, adequate funding for counter-terrorism, and the protection of intelligence sources.

Summary

The texts depict a US context dominated by the assessment of causal and contributory factors to the September 11 2001 attacks, including intelligence failures, and the assessment of the various national security responses that followed in its wake. In these texts, the security responses often overshadowed concerns about privacy and accountability.

3.3.8 The European Union

We examined 21 EU documents. These included 1) a European Parliament Recommendation on the future of the area of freedom, security and justice [Doc #79], and Parliamentary resolutions on 2) the prevention and fight against crime [Doc #93], 3) the action plan implementing the Hague programme [Doc #99], 4) the protection of privacy and personal data on the internet [Doc #49], 5) a comprehensive approach to personal data protection [Doc #144], and 6) on proposals for a European policy approach to network and information security [Doc #69]. From the European Commission, the analysis examined 7) the Hague Programme [Doc #188], 8) the communication establishing a framework programme on security and safeguarding liberties [Doc #187], 9) the Action Plan implementing the Stockholm Programme [Doc #204], and 10) proposals on general data protection regulation [Doc #232]. Analysed documents from the Council of Ministers were 11) A Secure Europe in a better world: The European Security Strategy [Doc #146], 12) the declaration on human rights and the rule of law in the information society [Doc #40], and 13) the Stockholm Programme [Doc #164]. We examined three opinions from the European Data Protection Supervisor, 14) on telecommunications data retention proposals [Doc #368], 15) on promoting trust in the information society [Doc #394], and 16) on the data protection reform package [Doc #413]. We also included Article 29 Data Protection Working Party opinions on 17) the need for a balanced approach to the fight against terrorism [Doc #315], 18) on the future of EU privacy [Doc #355], and 19) on facial recognition technology [Doc #363], as well as 20) the data protection reform proposals [Doc #364]. Finally, we examined, 21) joint proposals on internationals standards from the 31st International Conference of Data Protection and Privacy Commissioners [Doc #31], and 22) a report from the European Network and Information Security Agency (ENISA) on cyber security: future challenges and opportunities [Doc #292]. These documents address a diversity of themes, including fundamental rights and freedoms, legitimacy, effectiveness, harmonisation and integration, 9/11 and terrorism, data protection evaluation and reform, information sharing and co-ordination, immigration and border security, information technology development, consent (and withdrawal of consent), awareness, maturing of European security structures, economics of personal data and Europe as global driver.

Privacy, data protection and surveillance

Fundamental rights and freedoms

Support for fundamental rights and freedoms is explicit in many EU texts. Several texts also advocate strict harmonisation and equivalence of fundamental rights, including rights to

[87] Belasco, op. cit., 2003.

privacy and data protection across the EU, and that EU institutions should themselves be compliant with fundamental rights and freedoms.[88] Data protection, privacy and security are all represented by these texts as fundamental rights, and the European Parliament asserts that citizens should not have to choose between being free and being safe.[89] The creation of fully fledged policies for fundamental rights and citizenship was one of the priorities of the Hague programme.[90] The section of the Stockholm programme on protecting citizens' rights in the information society makes reference to the rights to privacy and protection of personal data set out in the Charter of Fundamental Rights. The document argues that the Union must create a comprehensive strategy to protect data within the Union, promote the application of relevant instruments on data protection, regulate the circumstances within which interference with these rights is justified and apply data protection principles in the private sphere.[91]

Threats to privacy

EU documents represent privacy as under threat from a number of sources. One of these sources is developments in information technology. The Council of Ministers argued that new information technologies can bring substantial benefits across areas associated with freedom of expression, information and communication, the respect to private life and correspondence, but also bring new challenges.[92]

For the Article 29 Data Protection Working Party, the dramatic increase in the storage and exchange of personal data in the law enforcement sector, stimulated by the technological developments and in the context of new threats resulting from terrorism and organised crime, poses immense challenges for data protection and should be addressed in any future legal framework.[93] The 2011 Council of Europe Resolution 1843 on the protection of privacy and personal data on the Internet and online media is seen as necessary because the digitalisation of information had caused unprecedented possibilities for the identification of individuals through their data.[94]

A specific technological threat to privacy arises from the rapid increase in the availability and accuracy of facial recognition.[95] The new technology raises specific data protection concerns, but the application of existing data protection requirements may help respond to new forms of

[88] European Parliament, Recommendation to the Council and to the European Council on the future of the area of freedom, security and justice as well as on the measures required to enhance the legitimacy and effectiveness thereof (2004/2175(INI)), 14 October 2004.
[89] European Parliament, Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)), 6 July 2011.
[90] European Commission, The Hague Programme: Ten priorities for the next five years The Partnership for European renewal in the field of Freedom, Security and Justice, Communication to the Council and the European Parliament, COM(2005) 184 final, Brussels, 10 May 2005.
[91] Council of the European Union, The Stockholm Programme – An open and secure Europe serving and protecting citizens, 5731/10, Brussels, 3 March 2010.
[92] Committee of Ministers, Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, CM(2005)56 final, 13 May 2005.
[93] Article 29 Data Protection Working Party, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009.
[94] Parliamentary Assembly, Resolution 1843: The protection of privacy and personal data on the Internet and online media, 2011.
[95] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, WP 192, Brussels, 22 March 2012.

surveillance (for example, the face should be considered personal data, and facial recognition should be considered a form of data processing).

Generally, later EU documents do not see security measures as an inherent threat to privacy. However, shortly after 9/11, the Article 29 Data Protection Working Party Opinion 10/2001 aims to act as a reminder that counter-terrorism legislation and measures of surveillance must be consistent with human rights, freedoms and data protection requirements.[96] The document also warns against amalgamating terrorism and general criminality, and as seeing data protection as a barrier to the fight against terrorism. The Hague Programme uses the language of balancing in the expressed need to strike the right balance between privacy and security in the sharing of information among law enforcement and judicial authorities. This is to be achieved by supporting and encouraging a constructive dialogue between all parties concerned, to identify balanced solutions, while fully respecting fundamental rights of privacy and data protection, as well as the principle of availability of information.[97] The EDPS Opinion on the proposed Data Retention Directive, which would become Directive 2006/24/EC of 15 March 2006, is also cautious. Whilst recognising the importance of fighting terrorism and organised crime, the Opinion sees the proposal as overstepping these needs, and as being disproportionate and not sufficiently respecting fundamental rights. The EDPS also questions the efficacy of data retention in combating terrorism.[98]

Harmonisation and co-ordination

Harmonisation and co-ordination are key issues in relation to privacy and security in EU texts. In 2004, the European Parliament recommends the adoption of joint data protection standards, as well as the formation of a joint data protection authority, as part of a systematic evaluation of fundamental rights policies in relation to the Area of Freedom, Security and Justice.[99] In 2011, it reiterates the necessity of "a comprehensive, coherent, modern, high-level framework able to protect effectively individuals' fundamental rights, in particular privacy, with regard to any processing of personal data of individuals within and beyond the EU in all circumstances".[100] This concept of internationally uniform standards for protection of privacy and the processing of personal data is also present in the Council of Ministers' Declaration on human rights and the rule of law in the information society.[101] Member States are encouraged to promote interoperable communications standards, promote frameworks for self- and co-regulation of private sector actors, promote codes of conduct for media and information providers in relation to judicial processes, provide the legal frameworks necessary for the defence of private intellectual property and the prevention of cybercrime, examine the use of ICT in promoting democracy and guarantee freedom of ICT-assisted assembly, and ensure that monitoring and surveillance of digital assembly does not take place.

[96] Article 29 Data Protection Working Party, Opinion 10/2001 on the need for a balanced approach in the fight against terrorism, WP 53, Brussels, 14 December 2001.
[97] European Commission, The Hague Programme, op. cit., 2005.
[98] European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final), Brussels, 26 September 2005.
[99] European Parliament, Recommendation to the Council and to the European Council on the future of the area of freedom, security and justice as well as on the measures required to enhance the legitimacy and effectiveness thereof (2004/2175(INI)), 14 October 2004.
[100] European Parliament, Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)), 6 July 2011, p. 2.
[101] Committee of Ministers, Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, CM(2005)56 final, 13 May 2005.

In commenting on the implementation of the Hague Programme, the Parliament advocates a single data protection policy that would encompass the former first and third pillars (European Communities and Police and Judicial Co-operation in Criminal Matters).[102] The Joint statement of the 31st International Conference of Data Protection and Privacy Commissioners (the "Madrid Resolution"),[103] advocates uniform standards for facilitating the international flows of personal data brought about by Internet penetration and that the commissioners see as necessary for a globalised world. These uniform standards are based upon limited use, consent, transparency, accuracy, access and security notification, and should include additional protections for sensitive personal data. Tracking without consent is a particular concern in relation to RFID.[104] COE Resolution 1843 also seeks global compliance with obligations in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No.108), due to flows of information having no fundamental boundaries.[105] The COE sees this as the best method for ensuring data protection and privacy, and EU Member States should only agree to transfer personal data to other states that are a party to Convention 108. The Stockholm Programme associates data protection with the idea of European citizenship in a single area of rights and freedoms.[106]

The Council also suggests that the EU should be a driver of international data protection standards, and that these should be included in bilateral and multilateral agreements.[107] Proposals for reform also contains an international dimension in which data protection rights are asserted against third country entities delivering services in the EU, or monitoring the behaviour of Europeans.[108]

Re-evaluation of data protection

Several EU documents call for an evaluation or re-evaluation of existing data protection rules. The Article 29 Working Party's report *The Future of Privacy* assesses the need for possible changes to the Data Protection Directive 95/46/EC in response to new technologies, globalisation, law enforcement and surveillance, and advocates the need for clarification of rules and principles, innovation of new principles, strengthening the effectiveness of the law, and formation of a comprehensive framework post-Lisbon Treaty.[109]

The European Parliament is concerned with ensuring that new legislation still allows 1) a high level of protection, 2) a balance between privacy, freedom of speech and access to

[102] European Parliament, Resolution of 21 June 2007 on an area of freedom, security and justice: Strategy on the external dimension, Action Plan implementing the Hague programme (2006/2111(INI)), 21 June 2007.
[103] 31st International Conference of Data Protection and Privacy Commissioners, Joint Proposal on International Standards for the Protection of Privacy with Regard to the Processing of Personal Data, Madrid, 5 November 2009.
[104] European Data Protection Supervisor (EDPS), Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels, 18 March 2010.
[105] Parliamentary Assembly, Resolution 1843: The protection of privacy and personal data on the Internet and online media, 2011.
[106] Council of the European Union, The Stockholm Programme op. cit., 2010.
[107] Ibid.
[108] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, Brussels, 25 January 2012.
[109] Article 29 Data Protection Working Party, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009.

information and 3) no hindrance to everyday processing of personal data.[110] Privacy is a thematic area of research under the framework programme on Security and Safeguarding Liberties.[111] The Council invites the Commission to evaluate existing data protection instruments and, where necessary, produce further legislation; propose recommendations for data sharing principles with the US; consider data protection agreements with third countries for law enforcement purposes; improve compliance with data protection principles; examine the introduction of a European certification for "privacy aware" technologies; and conduct information campaigns.[112]

Proposals from the Commission for a new legal framework for personal data protection in the EU argues that rapid technological changes have challenged the previous centrepiece of EU data protection legislation (Directive 95/46/EC, complemented by Framework Decision 2008/977/JHA). Whilst its principles are sound, this has not prevented legal uncertainty, fragmented implementation of data protection across the EU, and public perception of risks associated with online activity. The stated objectives of the reform proposals are to ensure consistent enforcement of data protection rules and to rationalise the current governance system to assist with this.[113] A strong logic through this text is the need from economic stakeholders to have consistency increased and uncertainty reduced in relation to personal data protection across the EU. Proposals include: more supervision and enforcement (including protections of the independence of national Data Protection Authorities, stronger enforcement and fining powers, mechanisms for cross-border collaboration of DPAs and a European Data Protection Board built upon the Article 29 Working Party), and measures to enhance individuals' control of their personal data. These include strengthening rights, clarifying the concept of consent, introducing a strong right to object to profiling, greater transparency, rights to data portability, procedures for exercising those rights, and the deletion of unnecessary data (the "right to be forgotten").

The European Data Protection Supervisor's commentary on the data protection reform package re-iterated the drivers for reform in terms of technological change, legal certainty and harmonisation, police and judicial co-operation, and increased global data transfer. For the EDPS, the main weakness of the reform package is that it does not sufficiently remedy the current lack of comprehensiveness of the EU data protection framework. The EDPS is disappointed by the proposed Directive for data protection in the law enforcement area, which it describes as providing protection that is inadequate and inferior to that of the Regulation. [114]

Protective measures for privacy

Measures to protect privacy recommended in the Madrid Resolution include the introduction of codes of conduct, delegated supervisory authorities, privacy impact assessments and co-operation and coordination between data protection authorities.[115] Other measures include

[110] European Parliament, Resolution of 6 July 2011, op. cit., 2011.
[111] European Commission, Establishing a framework programme on "Security and Safeguarding Liberties" for the period 2007-2013, Communication to the Council and the European Parliament, COM(2005) 124 final, Brussels, 4 April 2005.
[112] Council of the European Union, The Stockholm Programme, op. cit., 2010.
[113] European Commission, Proposal for a Regulation…with regard to the processing of personal data, op. cit., 2012.
[114] European Data Protection Supervisor (EDPS), Opinion on the data protection reform package, Brussels, 7 March 2012.
[115] 31st International Conference of Data Protection and Privacy Commissioners, op. cit., 2009.

privacy by design (PbD),[116] along with the incorporation of PbD in existing legal instruments, and legislation to hold service providers accountable for PbD.[117] Privacy by design, default privacy settings and privacy enhancing technologies (PETs) are also advocated by the Article 29 Working Party.[118] Additional protective measures from the Council of Europe include more effective remedies against those breaching data protection, higher protection given to data that forms the core area of individuals' lives including biometric and genetic data, and everyone's being able to control the use by others of their personal data, through meaningful consent (and the withdrawal of consent). The Parliament also encourages awareness raising and media literacy programmes.[119] The Article 29 Working Party calls for a stronger position for the data subject in the data protection framework, suggesting ways of empowering the data subject. This would require improvement of redress mechanisms, including class actions.[120] The Article 29 Working Party also calls for data minimisation, valid explicit consent and the encouragement of PbD and data protection by default as useful supports for privacy. The Commission released its data protection reform proposals in January 2012.[121]

Trust

Standards and the protection of privacy are linked to trust, both trust in institutions and trust in the broader European digital agenda and information society.[122] Trust is noted as important for the emergence and successful development of ICTs, especially for health and government service delivery. The European Parliament has argued that increased transparency and understanding will breed trust for new technologies, and thus increase adoption and use.[123]

Security

Several of the documents selected for detailed examination respond to the post-9/11 and post-Madrid bombings security context. *A Secure Europe in a Better World, European Security Strategy* sets out the key threats facing the EU, the EU's strategic objectives, including an international order based on effective multilateralism, as well as the policy implications for Europe.[124] In general, the security policy documents represent Europe as peaceful and relatively secure, and this partiuclar document states that Europe should be making a more active contribution to global and regional security equal to its potential based upon size, population, economy and available policy instruments. Pressures upon European security include global challenges (such as the increased link between internal and external security, globalisation, armed conflict, underdevelopment, competition for natural resources and energy dependence) and key threats (terrorism, weapons of mass destruction, regional conflicts, state failure, organised crime). The European Parliament states in 2004 that international terrorism is the main problem affecting the security and harmony of the people

[116] European Parliament, Resolution of 6 July 2011, op. cit., 2011.
[117] European Data Protection Supervisor (EDPS), Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels, 18 March 2010.
[118] Article 29 Data Protection Working Party, op. cit., 2009.
[119] European Parliament, Resolution of 6 July 2011, op. cit., 2011.
[120] Article 29 Data Protection Working Party, The Future of Privacy, op. cit., 2009.
[121] European Commission, Proposal for a Regulation…with regard to the processing of personal data, op. cit., 2012.
[122] EDPS, Opinion on Promoting Trust, op. cit., 2010.
[123] European Parliament, Resolution of 6 July 2011, op. cit., 2011.
[124] Council of the European Union, *A Secure Europe in a Better World, European Security Strategy*, Brussels, 12 December 2003.

of Europe.[125] In *Establishing a framework programme on "Security and Safeguarding Liberties" for the period 2007-2013,* the European Commission explicitly refers to 9/11 and the importance of prevention of and preparedness for terrorist activities.[126] The fight against terrorism is also part of the Hague Programme. The programme's priority responses include working toward a global response to terrorism; and focusing on different aspects of prevention, preparedness and response in order to enhance, and where necessary complement, the capabilities of Member States to fight terrorism in relevant areas such as recruitment, financing, risk analysis, protection of critical infrastructures and consequence management.[127] The progress in the implementation of the Hague Programme raised a number of concerns from the European Parliament, which issues recommendations with aims intended to provide European citizens with high level protections against terrorism and organised crime. Strengthening security and human rights are associated together.[128]

With the Stockholm Programme, which replaced and built upon the Hague and Tampere programmes, the EU reaffirms its priority regarding developing an area of freedom, security and justice.[129] Its introduction mentions the removal of internal border controls; more coherent management of external borders; significant steps in the creation of the European asylum system; European agencies reaching operational maturity and enhanced civil co-operation; but acknowledges that there are still challenges to be addressed.

The key justification for European Union involvement in security is that European citizens expect threats to health and safety to be countered at a European level[130] and the EU should respond in creating an area of freedom, security and justice.[131] According to the Commission, the Union can act as a catalyst for reinforcement and extension of legislation in this area, especially when given financial support. Moreover, it states that combining all activities related to law enforcement and crime prevention will lead to increased cost effectiveness and increased transparency. The texts position the security role of the EU as creating a reality for European citizenship above the nation state. The Council believes that the enhancement of actions at the European level, combined with better co-ordination with actions at regional and national levels, are essential to protection from trans-national threats.[132] The Parliament exhibits this position in modifying Commission language that suggested that organised and

[125] European Parliament, Recommendation to the Council and to the European Council on the future of the area of freedom, security and justice as well as on the measures required to enhance the legitimacy and effectiveness thereof (2004/2175(INI)), 14 October 2004.
[126] European Commission, Establishing a framework programme on "Security and Safeguarding Liberties" for the period 2007-2013, Communication to the Council and the European Parliament, COM(2005) 124 final, Brussels, 4 April 2005.
[127] European Commission, The Hague Programme, op. cit., 2005.
[128] European Parliament, Resolution of 21 June 2007 on an area of freedom, security and justice: Strategy on the external dimension, Action Plan implementing the Hague programme (2006/2111(INI)), 21 June 2007.
[129] Council of the European Union, The Stockholm Programme, op. cit., 2010.
[130] European Commission, Establishing a framework programme on "Security and Safeguarding Liberties for the period 2007-2013, Communication to the Council and the European Parliament, COM(2005) 124 final, Brussels, 4 April 2005.
[131] European Commission, Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 171 final, Brussels, 20 April 2010.
[132] Council of the European Union, The Stockholm Programme, op. cit., 2010.

trans-border crime can be best fought at a Union level, with language that suggests it *requires* action at the Union level.[133]

Later EU documents suggest a perceived maturity of EU security infrastructure. The Stockholm Programme claims that policy tools across all areas include: mutual trust, implementation of existing instruments, legislation, increased coherence (between EU institutions and agencies, and greater Council oversight of agencies such as Europol, Eurojust, Frontex), evaluation, training, communication, dialogue with civil society, and financing.[134]

The European Commission says in 2010 that security, justice and fundamental rights should not be treated in isolation, and instead should be considered together in formulating a coherent approach to meet the challenges of a rapidly changing social and technological environment that puts risks on freedoms, justice and security. One of the responses to security threats is to encourage the increased sharing of information between security actors, for security checks, judicial operation and movement of persons.[135] The Commission advocates a more co-ordinated approach towards prevention, preparedness, crisis and consequence management in regard to terrorist threats.[136] It also places more emphasis on promoting and developing partnerships between public and private organisations in the fields of crime prevention, statistics and criminology, protection of victims and witnesses.[137] This is apparently driven by the threat of cross-border criminality, and criminals exploiting differences between jurisdictions.[138] Privacy places some restrictions upon security measures. Although increased information sharing between police, border authorities and criminal justice agencies is advocated in areas such as border security and crime prevention, these information flows must be better understood, and evaluated against their impact upon privacy.[139]

The EDPS comments on the data protection reform package express concerns about the broad concept of "public interest" and variable meanings of "national security" as several sections build upon national law and allow national law to give effect to its provisions, specify or develop rules, and depart from the regulation under certain circumstances.[140]

Immigration

The addition of new states to the European Union raises issues of immigration and border security. As with data protection and privacy, this emphasises themes of coherence and co-ordination, with the Commission recommending a coherent migration and asylum policy

[133] European Parliament, Legislative resolution on the proposal for a Council decision establishing the Specific Programme 'Prevention of and Fight against Crime' for the period 2007-2013, General Programme 'Security and Safeguarding Liberties' (COM(2005)0124 – C6-0242/2005 – 2005/0035(CNS)), 14 December 2006.
[134] Council of the European Union, The Stockholm Programme, op. cit., 2010.
[135] European Parliament, Recommendation to the Council and to the European Council on the future of the area of freedom, security and justice as well as on the measures required to enhance the legitimacy and effectiveness thereof (2004/2175(INI)), 14 October 2004.
[136] European Commission, Establishing a framework programme on "Security and Safeguarding Liberties", op. cit., 2005.
[137] Ibid.
[138] European Commission, Delivering an area of freedom, security and justice for Europe's citizens, op. cit., 2010.
[139] Ibid.
[140] European Data Protection Supervisor (EDPS), Opinion on the data protection reform package, Brussels, 7 March 2012.

across Member States.[141] Several areas of the Hague Programme relate to immigration including a common asylum area, migration management, integration, internal and external borders, and migration. The aim is for a harmonised, balanced and integrated response, one that maximises freedom of movement whilst maintaining security and responding to illegal immigration, smuggling and trafficking in human beings.[142] In response to increased immigration pressure, the Stockholm Programme section on Access to Europe in a globalised world discusses integrated border management and visa policies to allow desirable access (business, tourists, students, scientists, etc.) but also to guarantee security for citizens. This section includes discussion of the role of Frontex, capability building in third nations, the European Border Surveillance System (Eurosur), border checks, the Schengen Information systems (SIS II) and Visa Information System, and shared visa policy.[143]

Cyber security

In 2002, the European Parliament expresses the increasing social and economic importance of electronic communications networks, requiring an adequate legal and policy framework at the EU level to guarantee the protection of network and information security, primarily in order to allow the smooth operation of the internal market.[144] The Parliament sees the level of information security at this point, including critical infrastructure and co-ordinated CERT response, as inadequate, and argues that the context requires a specifically European approach based around the formulation of common definitions and standards, and a European strategy. Network and information security is discussed in the Stockholm Programme as compatible with protecting citizens' rights, and that document talks about establishing a European legal framework for cyberspace.[145] ENISA continues this theme, arguing for a cohesive pan-European approach to cyber security. It states that increased dependency upon ICT makes critical infrastructure protection an issue of economic competitiveness and prosperity as well as security.[146] Cyber threats include cybercrime and cyber espionage. The ENISA report identifies a number of areas where current EU approaches to cyber security could be extended (cross-border collection of data relating to cyber security, improved dialogue between information security communities, a proactive approach to building new cross-border communities, modernisation and further development of ENISA).[147] However, several documents related to data protection reduce information security to technical measures.

Summary

The EU context features frequently expressed and explicit support for fundamental rights and freedoms, alongside drives for harmonised, comprehensive security and privacy policies, and taking on a role as a global actor. Security is increasingly portrayed as linked to fundamental rights. The EU is currently engaged in the re-evaluation of its data protection principles, attempting to maintain a consistent high standard, and allow citizens to exercise their rights

[141] European Commission, Delivering an area of freedom, security and justice for Europe's citizens, op. cit., 2010.
[142] European Commission, The Hague Programme, op. cit., 2005.
[143] Council of the European Union, The Stockholm Programme, op. cit., 2010.
[144] European Parliament, Resolution on the Commission communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European policy approach (COM(2001) 298 – C5-0657/2001 – 2001/2280(COS)), 22 October 2002.
[145] Council of the European Union, The Stockholm Programme, op. cit. 2010.
[146] European Network and Information Security Agency (ENISA), *Cyber security: Future challenges and opportunities*, 2 December 2011.
[147] Ibid.

against challenges to privacy that include technological change. There is discussion of a wide range of privacy protecting measures, often centred on increasing individual control of personal data. There is also on-going discussion about issues of data retention and the appropriate security stance of the supranational organisation. Security policy documents position Europe as politically stable and peaceful, and able to make a contribution to global security, as it continues to develop an area of freedom, security and justice, with increasing security co-ordination at the EU level.

3.4 COMPARATIVE ANALYSIS AND DISCUSSION

The preceding country-by-country analysis of key themes and issues of privacy, data protection, surveillance and security was in a roughly chronological order for each country. This concluding section brings out additional observations from comparing issues across countries and over the time spans covered by the documents analysed.

Drawing upon the stated motivations in the analysed texts, there are six broad and non-discrete categories of identified drivers for the compilation and publication of security and privacy texts. These include: 1) responses to legislative requirements, processes or consultation requests, 2) responses to changed security contexts or the emergence of apparent new security threats, 3) responses to particular events or identified public concern, 4) reminders or re-affirmations of principles and clarification of laws, 5) the results of scrutiny, inquiry or evaluation of existing policies and programmes, and 6) responses to increased surveillance practices and technological developments.

3.4.1 Security

Understanding the framing of security (and insecurity) within security policy documents is important as these documents contribute towards processes of making different phenomena intelligible as insecurities, and therefore as appropriate objects of security policy.[148] These documents therefore give us a better understanding of the extent of the concept of security and the issues that are brought within the aegis of security. Particularly important documents in this process are the several national security strategies that have been included in the document analysis.

Concepts of security are heterogeneous across different countries, and across different actors within countries. There are multiple, divergent framings of the concept of security, across European governments, and between different policy actors within individual countries. However, many of these concepts are more expansive than the most traditional concepts of national security, and there is an indication that the scope of security has expanded across all countries in the analysis as more areas of social life are represented as contributing towards security. All representations include national security, but some countries, such as Romania, make specific mention of fundamental rights and "democratic security" as composing part of security. The Romanian security strategy defines National Security in a broad sense as "a state of normality" "to which the citizens, the communities and the state aspire"[149] It represents security as including economic prosperity and development, full observance of domestic and international law, socio-political "balance and stability" and sees a democratic

[148] Huysmans, Jef., *The Politics of Insecurity: Fear, migration and asylum in the EU*, Routledge, London & New York, 2006.
[149] Presedintele Romaniei, op. cit., 2007.

framework and the exercise of civic rights and freedoms as necessary to achieving national security. The French strategy depicts a new approach of considering defence policy, foreign policy, and economic policy as part of a whole, whilst still considering their distinctive characteristics. The Italian and French security documents also suggest that concepts of homeland defence are insufficient for security, and that there is a blurring of the division between internal and external security issues. Several texts also represent the public, European and national citizens as a collective agent "calling for security" or having "security questions" to be addressed by various actors.

Characterisations of the international security environment are more homogeneous across countries and there are large areas of overlap. This supports the findings of the FORESEC project that observed an increasing overlap of threat assessments in different EU Member States.[150] The security documents present a consistent picture of a *new security environment*, often positioned as the motivating factor behind the development of a new security strategy, or prompting reflection upon existing security practices and traditions. There are some differences in how new this new environment is. The French White Paper and the Romanian security strategy identify the contemporary security context as being post-post-cold war, as opposed to the representation in the Italian White Paper of a post-cold war context. However, the actual descriptions of these contexts are similar. Several texts represent the international security environment as more complex, fast-paced and uncertain, with greater involvement by non-state actors, blurred lines between internal and external security, vulnerable to rapid strategic upset, affected by technological developments, and requiring international co-operation to respond to these new dangers. It is represented as a combination of positive trends with the potential for significant strategic upset. The largest areas of divergence within security documents are when the particular national security priorities of the respective countries move beyond international stability and security, and responding to the shared image of the new security environment, to the concrete security ambitions of particular countries. An example of this type of specific, context-dependent concern is Romania's ambition to bridge the divide it perceives between itself and the rest of the EU. France identifies a shift in power towards Asia, whilst a document from the UK government identifies a continued terrorist risk due to conflict in Northern Ireland. Fundamentally, several security documents from all countries represent this security context as less predictable and more uncertain than previous security contexts.

There is a relatively stable core of what are considered to be security threats, although with some alterations of priority and some interests specific to individual states. The European countries see the likelihood of outright, involuntary war as low. International terrorism, and related "asymmetric threats", sits high on explicit security agendas as well as in what can be interpreted from other texts. Information threats, including espionage, major cyber attacks, technological risks, and strategies of influence are also given a high profile. A third source of shared threat for the European countries is the existence of areas of instability outside of Europe or on the European periphery. 9/11 is the most significant terrorist event in the United States, but is mentioned in subsequent security policy documents across all countries. The apparent frequency and prominence of these mentions reduces over time, and these mentions become part of a cluster of other security events (Madrid train bombings in 2004, London 7/7 2005, etc.). The Madrid and London bombings have greater significance in EU security texts than in US texts. In regard to counter-terrorism, there is no mention in these documents of the

[150] Gregerich, Bastian and Pantucci, Raffaello., *FORESEC Deliverable D2.2 Synthesis Report*, 15 August 2008. http://www.foresec.eu/wp2_docs/Synthesis_Report_150808.pdf

lead role in driving counter-terrorism that has been played by the "Group of Six" (UK, France, Germany, Spain, Italy and Portugal).[151]

All the security strategies in the analysis see collective security as important. Italy and Romania address the increasing likelihood of combined and joint security operations, and the Romanian security strategy explicitly aligns itself with EU and NATO security strategy. France positions its own security concerns as part of Europe, but does however identify fragility and crises of legitimacy within existing systems of collective security (such as the UN). The French security strategy aligns with texts from the EU in suggesting that the answers for many citizens' security concerns are found at the EU level. It could be anticipated that shared assumptions about threats, the contemporary security environment, and particularly the transnational nature of contemporary security issues provide support for collective security arrangements.

Several security documents emphasise the importance of knowledge and pre-emption in security practice. This is related to the complexity of the contemporary security context. The Romanian security strategy states: "In such a tense and complex environment, the security of each individual country as well as that of the international community as a whole depends on the ability to anticipate and to undertake predictive action, rather than reacting to events or adjusting to them".[152] Similarly, the French White Paper argues that France's ambition is "to not submit to this uncertainty, and to harness the knowledge and information revolutions to be able to anticipate, respond to and influence international developments"[153] and that anticipation is a key strategic principle. This identification of the necessity of pre-emption and better awareness for security can provide ready rhetorical support for surveillance practices in the domain of national and international security. In spite of the security context being less predictable, several documents urge the imperative of trying to predict and anticipate security developments.

The texts generally value information exchange between security agencies as an important contributor to security. However, there are some noticeable differences between countries. The 9/11 Commission report sees an absence of information sharing as contributory to 9/11 and argues for a paradigm shift to the sharing of security information. The narrative that a lack of shared intelligence or information contributed to 9/11 appears to have taken hold fairly rapidly and been broadly pervasive. It is also visible in documents from the Netherlands.[154] In contrast to this, German and Romanian documents contain concerns about information sharing between police and intelligence agencies based upon those countries' historical experience, and constitutional frameworks. German documents highlight the constitutional separation between police and intelligence functions. This separation of information collecting agencies from agencies acting upon this information is linked to the concept of proportionality in some German state constitutions. German documents indicate that they do not want police acting upon "soft" intelligence or a blurring of the roles, despite several measures to increase cooperation. This important question raised is if effective counter-terrorism can be conducted without centralisation. In these documents, technical or digital

[151] Rees, Wyn. "Inside Out: The External Face of EU Internal Security Policy" *Journal of European Integration*. 30:1, 97-111, 2008.
[152] Presedintele Romaniei, op. cit., 2007.
[153] Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, *Le livre blanc,* op. cit., 2008.
[154] Tweede Kamer, *Bestrijding internationaal terrorisme; Verslag algemeen overleg op 17 oktober 2001, over terrorismebestrijding en veiligheid [Fighting international terrorism; report of a general meeting about fighting terrorism and security]*, Tweede Kamer, The Hague, 1 November 2001.

separation of information is not seen as sufficient due to the alleged ease with which it can be overcome. These documents do not deny the potential of information sharing to contribute to security, and counter-terrorism, but are sceptical of the extent of its effectiveness, and attempt to refocus attention upon the reason such limitations might be in place.

Economic costs of security are rarely if ever mentioned, even in the context of European economic crisis. The UK government expresses a view of the global security industry as an economic driver[155], and German documents express a desire to maintain Germany's expert position in security technologies. The French national security strategy also includes economic policy within the ambit of national security.

Information security

The concept of national security is expanding in security policy documents across many countries to include information security, often under the rhetoric of cyber security, critical information infrastructure or cybercrime. This raises the profile of information security to that of a national-level security issue. Many practices of information security are similar to practices of data protection, and good data protection measures contribute towards good information security. Reflecting upon this increasing inclusion of data-protection type activities within security politics, the overlap between information security practices and privacy and data protection practices may allow for the reduction of a perception of a fundamental conflict between security and privacy. On the other hand, the frequently made but erroneous equation of data security with data protection in the fuller sense does a disservice to the latter.

Border security

Both the USA and the European Union mention border security and immigration as security issues. They appear less frequently in the policy documents from the national level. Given that some countries have strong and persistent debates on immigration and border control, this relative silence around border security may a result of the limitations surrounding the way these documents were selected for analysis.

3.4.2 Privacy, data protection and surveillance

In a manner similar to the framing of security, these documents provide ways of framing the problematic of privacy, data protection and surveillance and the appropriate policy, legal, social and economic responses to these issues. The texts provide a perspective on how these issues are represented, as issues, within policy documents. The combination of privacy and security documents in this analysis also allows us to reflect upon the way the relationship between the related concepts and practices is presented in public texts.

The current EU position on the conflict between privacy and security appears to be that security and fundamental rights (including privacy) are complementary, not in contradiction. Fundamental rights and freedoms are to be "respected" more than "balanced". The language of "balancing" of privacy and security is however still used at national levels, and can be found in texts from Romania, the Netherlands, Germany and the UK. The House of Commons Home Affairs Committee asked contributors to comment on the processes they use to conduct

[155] Ministry of Defence, op. cit., 2012.

"balancing" between privacy and security.[156] Many scholars have taken issue with the notion of balancing privacy and security, as if they were part of a zero sum game, where the reduction in one is at the expense of the other.[157] Other terms for the interaction of privacy and security include: be respected, be consistent with, be reconciled with, balanced with, balanced against, not interfere with, protect, support, and allow the exercise of.

There are variations across the analysed documents in the representation and use of the concept of surveillance. Surveillance, as a term, appears to be less frequently mentioned than data protection or privacy across all of these texts apart from those from the UK.[158] The most limited use of surveillance is in the documents from the Netherlands, where surveillance is not a core topic in any document. The French and Italian documents directly refer to surveillance only in terms of video surveillance. In this context, the term is used as a description of a particular visual technology. Documents from the respective data protection agencies reiterate that video surveillance is covered by general data protection legislation.[159] German documents also do not make significant use of the concept of surveillance, but identify Internet surveillance and video surveillance as issues within the broader law and politics of data protection. Romanian documents associate surveillance closely with intelligence activities. Surveillance is discussed in the context of counter-terrorism, and the adoption of intelligence service practices by the police. One document identifies increased potential for unwarranted surveillance arising from proposed intelligence reforms.[160] In the US texts, surveillance is externally directed, with the term being mainly used in relation to foreign intelligence gathering[161] and inadequate surveillance of borders prior to 9/11.[162] In contrast to the other countries analysed, many of the UK documents are explicitly and directly about the concept of surveillance, including its social consequences and constitutional implications. Several of these documents were produced in response to concerns that the UK was becoming a "surveillance society" due to increased surveillance infrastructure introduced since 9/11 in pursuit of safety and security, with consequences for public trust and the relationship between citizen and state. Given more sources focused upon surveillance, the picture of the way that surveillance is represented in UK documents is accordingly richer. These texts depict surveillance as increasing, both in surveillance capacity exercised by government and other actors, and in the amount of public concern this creates. Several UK documents also express the need to examine if current limited regulation is sufficient to respond to these increases. In the EU documents there are several direct mentions of surveillance, but it is part of a range of associated privacy and data protection issues. Increased surveillance is one factor (alongside globalisation, new technologies and changes in law enforcement) that prompts reconsideration of EU data protection regulation. EU documents state that surveillance measures should be consistent with (or respect) human rights, freedoms and data protection law. Real-time surveillance, presumably by human agents, is identified as a specific type of intrusive measure, alongside biometrics, telephone tapping, telecommunications data retention and data-sharing. This use of surveillance is much

[156] House of Commons Home Affairs Select Committee, op. cit., 2008.
[157] See, for example, Zedner, Lucia, *Security*, Routledge, London, 2009, pp. 134-137. A critique of the concept of "balance" in the data protection context is in Raab, Charles, "From Balancing to Steering: New Directions for Data Protection", ch. 3 (pp. 68-93) in Colin Bennett and Rebecca Grant (eds.), *Visions of Privacy: Policy Approaches for the Digital Age*, University of Toronto Press, Toronto, 1999..
[158] This may be an effect of the selection of the UK documents for analysis.
[159] Commission nationale de l'information et des libertés (CNIL), Vidéosurveillance, op. cit., 2010.
[160] Romanian government, op. cit., 2006.
[161] Doyle, op. cit., 2001.
[162] 9/11 Commission, op. cit., 2004.

narrower than that used in the UK documents, in essence referring to a practice rather than to a category.

There are somewhat fewer representations of public calls for privacy present across these documents than there are representations of public calls for security. There are also representations of pressures from the public for more surveillance.[163] The UK Home Affairs Committee identified these pressures as arising from raised expectations on security and policing actors due to technological developments. If security practices are legitimised by articulating a supposed public demand for security, then an absence of such readily articulated public calls for privacy, or for data protection, may reduce the weight of privacy in any "balance" against security.

Privacy threats

Different countries have different sets of privacy "threats" – that is, those risks to privacy that are considered to be the most threatening in a particular context. In the UK, this appeared to "the state" most broadly, and the Home Office and law-enforcement agencies in particular. In Germany, this appeared to be the police, intelligence agencies, and the risks of data sharing with the United States. In Italy, the biggest apparent threat to privacy in the analysed documents seemed to come from the private sector.

There is a wide and diverse range of privacy problems identified through the documents. These are often shared between countries, but particular issues appear to have increased salience in some countries in comparison to others. Examples of this include body scanners in Germany, or information sharing between banks in Italy. We should be careful not to overestimate this, as the analysis of a highly specific document (an opinion on CCTV in public settings) as compared with a more general one (privacy issues due to ICT) could present highly different pictures of salience. Several documents are explicitly "triggered" in response to particular privacy breakdowns or failures, including data leaks in Germany, and the transfer of personal data between members of a banking group in Italy These are often taken as emblematic of broader problems requiring some kind of intervention in response or further evaluation to determine the nature of potential responses.

There is a strong thread of technological determinism running through these texts, in which developments in technology are considered to have brought about both increased insecurity, but also risks to privacy and data protection. When threats to data protection or privacy arise, they are often portrayed as coming from information technology (such as "databases") or from information sharing practices, more than from "surveillance" as a phenomenon. Some documents engage with particular new technological developments, as in the parliamentary debate on body scanners in Germany, or the Article 29 Data Protection Working Party's response to increasing use of facial recognition technology.[164] There is little discussion about how these particular forms of technology have emerged (for example for commercial or security reasons), with technological development being presented as a naturalistic *fait accompli*. However, technology use is almost universally positively valued throughout these texts. There are a few texts that suggest that technological developments have precipitated a re-evaluation of privacy regulation, but the fundamental use of technology is positive. We encounter no expressions of security or privacy "luddism". In general, the representation of

[163] House of Commons Home Affairs Select Committee, op. cit., 2008.
[164] Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, WP 192, Brussels, 22 March 2012.

information systems and technology was as "functional" unless attacked by a hostile actor – there was only one discussion about data leaking (in a German text).

Privacy advocates

There is broad agreement across the texts on the broad principles involved in privacy, data protection and surveillance. These principles include proportionality, accountability, transparency, trust, consent, and the rights of the data subject. Texts from each country include those that are actively advocating greater privacy protection or identifying activities that can infringe upon privacy. These texts also provide a representation of the activities of privacy advocates.

As represented in many of these texts Data Protection Authorities (DPAs) appear to play a mediating role in public debate. The issues focused upon by DPAs are important for directing (but not determining) public attention. Data Protection Authorities may use or leverage public attention on issues of surveillance and privacy to push those issues up the policy agenda. Particular interventions or reports can get public attention, and introduce language and concepts in the public debate (e.g., "surveillance society"). The influence of reports, including those analysed in this review, is dependent upon their uptake and use by other influential actors, including the media and advocacy groups..

Across the texts, there are broad ways by which the maturity of a data protection or privacy regime is represented. None of the texts constructs their national data protection and privacy regulatory regimes as non-existent. The Romanian documents present a picture of a somewhat new, tentative or vulnerable regime. Several European countries in this analysis present a picture of a mature and established data protection regime. This takes three sub-forms. The first (found in German and Dutch documents) is of a mature regime that is established and being maintained. The second (also found in some Netherlands, UK and French texts) is of a mature regime that is being tested or put under pressure by external forces (such as technology development or new surveillance practices). The third is of a mature regime being explicitly re-evaluated by political actors (perhaps identifiable at the EU level). Finally, no countries in this analysis considered their data protection and privacy regimes to be either perfect or entirely out of date and irrelevant. Given the absence of any document positioning its own country's data protection regime at either extreme (non-existent or perfect), we can envisage that these serve as rhetorical poles against which existing data protection regimes can be assessed or compared. Countries with mature data protection regimes appear to be primarily engaged in clarification of data protection and privacy regimes. The texts broadly depict privacy protections as adequate or generally acceptable. This clarification includes producing guidance on the interpretation of data protection or privacy legislation, which might be interpreted as actually constructing those regimes. Countries with acknowledged authoritarian histories (Romania, Germany) make reference to this in the documents, particularly in relation to the roles of intelligence agencies, and the separation of law enforcement and intelligence functions.[165]

Privacy protecting measures and policy responses

The analysed documents indicate that there may be differences in the solutions and responses put forward in response to particular problems of privacy, data protection and surveillance.

[165] Romanian government, op. cit., 2006.

This section therefore presents some of the responses to privacy problems and the ways they are represented across the analysed documents. Responses across the texts included the individual control of data; the right to be forgotten, media literacy; transparency; monitoring and evaluation of security practices; privacy and surveillance impact assessments; guidance, and data protection reform (as discussed in the previous section). Particular responses, including informational self-determination and the right to be forgotten were unique to particular countries (in this case, Germany and France).

Some French and EU texts suggested that increased individual responsibility for, and control over personal data, would be an appropriate response to current data protection, privacy and surveillance issues. Such increased control is to be achieved through education and awareness campaigns, greater transparency of data processing, and enforced legal rights. The European Parliament recommended that everyone must be able to control the use by others of their personal data. This required consent for data collection and processing to be given in advance, and there must be the ability to withdraw consent.[166] Commenting on the proposals for reform of Directive 95/46, the Article 29 Data Protection Working Party highlighted the need for the data subject to have a stronger position in the data protection framework, and that this would be based upon consent, notification of data breaches, and greater transparency.[167] The Council appears to also be moving in this direction advocating strengthening rights, clarifying the concept of consent, introducing strong rights to object to profiling, greater transparency, rights to data portability, procedures for exercising rights, and the deletion of unnecessary data.[168]

The strongest form of the idea of individual control over data is found in the German texts. These texts are the only texts that explicitly mention rights to informational self-determination. Arising from opposition to the 1983 census, informational self-determination is the legal anchor for data protection in the German constitution.[169] Distinguished from privacy (as the right to be left alone), the data subject is to maintain control of his or her own personal data as part of a general right of personality. Self-determination protects information from one context proliferating into another, and German documents saw this as necessary for the development of the individual and as a precondition of free and democratic communities. It is used in these texts to reflect upon the constitutionality of profiling.[170] Profiling is particularly problematic for informational self determination because the profile can be more significant than the sum of its component parts, and is not consented to (and perhaps cannot be consented to given the general opacity of profiling systems) in the same way as data provided by an individual. UK parliamentary documents were actively sceptical of increasing individual control over their personal data as an effective response to issues of privacy and surveillance, identifying it as potentially placing too great an obligation upon individuals. There is little mention of the right to be forgotten in texts other than from France[171] and from the European Commission[172]. The Commission sees the right, understood as the deletion of

[166] Parliamentary Assembly, Resolution 1843: The protection of privacy and personal data on the Internet and online media, 2011.
[167] Article 29 Data Protection Working Party, The Future of Privacy, op. cit., 2009.
[168] Council of the European Union, The Stockholm Programme, op. cit., 2010.
[169] Hornung, Gerrit & Schrabel, Christoph "Data Protection in Germany I: the population census decision and the right to informational self determination", *Computer Law & Security Report*, Vol. 25, No.1, 2009, pp. 84-88.
[170] Enquete-Kommission, op. cit., 2012.
[171] Senat, op. cit., 2010
[172] European Commission, Proposal for a Regulation…with regard to the processing of personal data, op. cit., 2012.

unnecessary data, as one measure that contributes towards greater individual control of personal data.

Few documents were highly supportive or reliant upon technological responses to privacy problems, although as discussed in the previous section on information security, information security was seen as highly important, There were occasional mentions of PETs and introducing PbD, but these were presented as solutions much less frequently than legal, regulatory and compliance responses across all countries. The EDPS saw PbD as a guiding principle for technology and process design.[173] Several of these texts should themselves be understood as a form of response to problems raised by privacy and data protection. This is true both for broad strategy guidelines as well as for direct operational guidance produced by DPAs.

Policy documents from the EU, specifically from the Parliament and the Council, suggested various ways in which security and surveillance practices might be themselves subject to monitoring as a way of ensuring that they did not negatively impact upon privacy and data rights. The European Parliament encouraged an independent benchmarking tool for crime prevention, whilst the Council identified evaluation and impact assessments for responsible organisations.[174] Texts from the UK and the EU directly mention privacy impact assessment (PIA). These texts represent PIA as having considerable merit, as part of self-regulation for individuals and organisations. PIA, and the expanded Surveillance Impact Assessment, are shown as a step beyond legal compliance and a way of determining if surveillance activity conforms with ethical principles. PIA should be built into information processes as a form of risk assessment, and the identification of ways that privacy protection can be included whilst contributing towards socially valuable objectives should be part of the PIA process.[175] The Commission also suggests that greater obligations should be placed upon responsible organisations with regard to good data management and security practices, greater accountability, the burden of proof for legality, data protection impact assessments, and the introduction of security breach notification.[176]

International and national interactions

These texts also feature representations of the interactions between countries, and between countries and international organisations. For the EU Member States the EU is a significant actor in privacy and data protection. Several texts provide representations of these relationships.

On the side of security, the EU exerts pressure through the internal and external security policies, through funding research into surveillance and security, and through policies such as the Data Retention Directive. On the side of privacy, the EU exerts pressure through its

[173] European Data Protection Supervisor (EDPS), Opinion on Promoting Trust in the Information Society, op. cit., 2010.
[174] European Parliament, Legislative resolution on the proposal for a Council decision establishing the Specific Programme "Prevention of and Fight against Crime' for the period 2007-2013, General Programme 'Security and Safeguarding Liberties" (COM(2005)0124 – C6-0242/2005 – 2005/0035(CNS)), 14 December 2006; Council of the European Union, The Stockholm Programme, op. cit., 2010.
[175] Surveillance Studies Network, op. cit., 2006; House of Commons Home Affairs Select Committee, op. cit., 2008; 31st International Conference of Data Protection and Privacy Commissioners, op. cit., 2009; House of Lords Select Committee on the Constitution, op. cit., 2009.
[176] European Commission, Proposal for a Regulation…with regard to the processing of personal data, op. cit., 2012.

normative commitment to fundamental rights, post-communist transition, and through data protection regulations. Dutch documents suggest that the EU could contribute to promoting trust in national government. The EU expresses a very strong desire for harmonisation and coherence across both security and privacy/data protection policy areas. This necessity of coherence and harmonisation is less frequently articulated in texts at the national level, which seem to have a tendency to elevate local contexts and local variations upon privacy and security issues above the need for European harmonisation. Harmonisation is rarely present as an actual policy goal, and the assumption that harmonised privacy and data protection law across the EU will be economically beneficial is absent (but not contested) elsewhere. Pressures for both privacy and security are mediated at a national level by (at least) two processes: 1) the representation of the role of the EU in the local context; and 2) the implementation of the EU ruling or measure at the local level. Of the EU members, the UK made the least mention of European influence in both security and data protection.

Joining the EU and/or NATO has implications for the security policies of new members such as Romania, including drives for intelligence and security modernisation. The EU exerts pressure upon both sides of the privacy/security "balance" experienced in national European contexts. This may be due to contradictory policy, the result of having a large supra-national organisation, or of pressures in particular directions arising from particular sections of the EU policy-making process. More politically powerful, confident or influential states appear to express more confidence in questioning EU regulations, and having these questions respected. This is not to say that other countries do not challenge privacy or security policies emerging from the EU, as the Romanian Constitutional Court challenged the Data Retention Directive. The difference in the texts is somewhat rhetorical. This challenge can be seen in resistance to measures perceived as increasing surveillance, as in German opposition to the Data Retention Directive, but also in national level opposition to data protection measures originating at the European level. Germany and Romania have currently not implemented this Directive, whilst the Netherlands and Italy were previously infringing, but proceedings have since been closed. The UK and France have had no infringement proceedings against them in relation to this Directive.

Countries can also interpret EU Directives as they pass into national law, and the documents provide some reflections upon the representation of this process in relation to privacy, security and surveillance. There are several ways the implementation processes might be represented. A text might downplay the agency of the nation-state in comparison to the EU, which might be a sign of either "policy-laundering" or a genuine feeling of disempowerment; it might prevent an account of implementation as business as usual, or highlight the agency of the nation-state. The processes might be represented as consensual or antagonistic, and the particular choices of implementation might be highlighted or covered over. In relation to the Data Retention Directive, Romanian texts identify elements that can be varied in national implementations, including the time of retention (between six and 24 months), the organisations that can request retained data and the penalties for non-compliance.

Across most of the documents the representation of the EU is nuanced. It is both a (necessary) source of security, and a support for privacy and data protection rights, but also brings with it membership costs and its measures can have impacts upon both security and the exercise of rights. Romanian references to the EU include the necessity of transposing the Data Retention Directive despite its being found unconstitutional; that joining the EU has impacts upon security and privacy, but that membership is necessary for security activity (including international action); and that the Romanian national security must be aligned with the EU

and with NATO (even though these may not align with each other). Italian texts also present the EU (alongside NATO) as a reference point for international security. The white paper on security states that transformations in Italian military forces must aligned with the EU for collective defence.[177] An early Dutch document includes calls from the national level for adjustments to EU privacy policies to increase security.[178] The representation of the EU is that the EU can contribute towards public trust by its emphasis on the importance of basic rights, through collaboration and the provision of information. This document actively reflects upon the process of the representation of the EU and is concerned that EU measures may be misrepresented by other political actors.[179] The French documents broadly positively represent the EU in relation to legal alignment. The text on the general security regulatory framework presents EU standards on electronic communication as something to be harmonised with[180], whilst the Senate proposals for a law to protect privacy in the digital age mirror and potentially pre-empt the implementation of Directive 2009/136/EC.[181] German texts comment upon the unconstitutional nature of the Data Retention Directive[182], but also imply that the EU has significantly better data protection law than the US. As might be expected, the US documents in this analysis make no mention of the EU in regard to privacy. Despite being an EU Member State, the UK texts also make no direct link between security, privacy, data protection and surveillance and EU membership. There are mentions of global influences, but not of the regional context, or of any particular measures or reforms at the EU level, either contributing towards or acting as a barrier to increasing surveillance.

In general external influences upon policy process are downplayed. The non-US documents do not describe any post-9/11 security or surveillance measures as being driven by US expectations regarding speedy security cooperation[183], but rather frame these measures as a required response to the revealed security problematic of terrorism or global instability. Recent concerns about industry lobbying around data protection reforms are not reflected in these documents.[184]

3.4.3 Chronology

Given the relatively small samples of documents for each country and given that many of these documents are the result of relatively unique contexts, it is difficult to make well-grounded claims about the changes over time.

It is possible to suggest that 9/11 preceded a range of texts that directly responded to the attacks and to the security measures brought in response. These included initial calls for "balanced" responses that did not infringe important rights in the quest for security or prosecution of terrorism. The few years that followed saw a number of national security

[177] Italian Defence Ministry, Libro Bianco, op. cit., 2002.
[178] Tweede Kamer, Bestrijding internationaal terrorisme, op. cit., 2001.
[179] Raad voor het openbaar bestuur (Rob), Rob-advies Veiligheid en vertrouwen [Advice to Parliament re security & trust], The Hague, November 2010.
[180] Secrétariat générale de la défense et de la sécurité nationale, op. cit., 2010.
[181] Senat, op. cit., 2010.
[182] Bundesregierung, Vorratsdatenspeicherung und Sicherheitslücken [Data Retention and Security Vulnerabilities], 22 April 2010
[183] Nilsson, H., "The EU Action Plan on combating terrorism: assessment and perspectives", in D. Mahncke & J. Monar (eds.) *International Terrorism: A European Response to a Global Threat?,* PIE Peter Lang, Brussels, 2006.
[184] Clark, Liat, "MEPs copied US lobbyists' Data Protection Regulation amendments verbatim", *WIRED*., 14 February 2013.
http://www.wired.co.uk/news/archive/2013-02/14/lobbyplag-eu-plagiarises-us-lobbyists?page=all

reviews and national security strategies. This included security strategies and polices at the EU level, which increased in number over the period analysed. The documents that deal with the review, assessment, clarification or reform of data protection and privacy regimes appear to be clustered in the latter half of the sample. As these reform efforts acquire more substance, there are subsequent commentary documents and texts. Documents that deal with information security, and particularly cybercrime, mainly date in the latter two or three years.

If we look at the long-list documents from the European Commission, Council and Parliament, there are generally more documents focused on security than on privacy, apart from in 2012. There are spikes in number of security-focused documents in 2003 and in 2008, with a relatively high number of documents in between, and a reducing trend afterwards. The number of privacy-focused documents is at its lowest in 2003, and generally increasing over the period 2005 to 2012, with a peak in 2009. This basic quantitative analysis combined with the documents analysed may support a narrative in which security concerns in policy escalated dramatically after 9/11 (following a lag based upon the time it takes political organisations to respond to events) and stayed at high levels for most of the period under review. These initial texts focused upon analysing intelligence failures and other gaps in security, and potential security and counter-terrorism measures that could be taken, or that needed to be taken. This included legal reforms, but also policy attention. These early documents tend to make somewhat token mentions of privacy and fundamental rights. There are several warnings or cautions that privacy, data protection and other fundamental rights should be respected, or should not be infringed by new security measures, and of course that privacy should be balanced against security. However, in these early documents there are few mechanisms for actually conducting such a balancing exercise. Later policy documents tend to introduce more specific measures for the protection of information and privacy rights, and to produce a wider catalogue of social and technological forces impacting upon privacy and data protection. These documents depict privacy as under threat not just from security measures (although this remains a potential) but also from changes associated with the information society and increasing technological capacities for surveillance. The need for security is not repudiated in any of these later policy documents, but it is perhaps more sophisticated. Several later documents, particularly from the EU, attempt discursively to align security and fundamental rights (including privacy) and frame them as not being in contradiction, but instead being mutually supportive.

4 CONCLUSION

This review of policy documents suggests that there will be significant differences between the ways in which members of the public in different Member States understand privacy and security. Different countries appear to focus on different aspects of security. Furthermore, different countries appear to have different relative levels of concern about issues such as privacy, data protection and surveillance. This holds true both across the summaries of the long lists of policy documents for Europe, Member States and the USA as well as the short but slightly more in-depth analyses of policy documents undertaken in the horizontal analysis.

This information will be used to feed into a discourse analysis of policy documents from the European Union, the United Kingdom and the Netherlands that will be presented in the next deliverable. Furthermore, this information will be used to inform the design of the PRISMS Europe-wide survey as well as the elements to be included in the PRISMS decision support system that will assist those who use surveillance and security systems in evaluating the relative impact of these systems on privacy and security.

5 INPUT TO THE PRISMS SURVEY

Part of the purpose of this horizontal analysis of security documents is to produce a number of hypotheses that can be used to generate questions for the survey research in WP9. This documentary analysis has produced a number of lines of questioning.

A general hypothesis would be:

The framing of privacy, data protection, surveillance and security in publicly available policy documents at a national and international level will to some extent correlate with the attitudes and perceptions towards these issues of members of the public in different nations. This will not be a deterministic influence as we can anticipate mediating factors, including individual and group experience, media portrayal, focus or attention on these documents, and the influence of opposing or divergent framing.

The preceding analysis suggests a number of hypotheses, some of which may be testable in the PRISMS Europe-wide survey:

- The core of national security is consistent across countries.
- The particular focus of security and threats varies from one country to another. Individual national security priorities remain despite shared interests.
- Perceptions of "security" are not limited to national defence.
- The international security environment is generally framed as insecure, vulnerable, interconnected, affected by technology, interdependent, with non-state actors. It is seen as a new security environment.
- The rhetoric of 9/11 is waning.
- Local, historical or more recent security events are more salient than 9/11.
- Information exchange for security is often represented as a good thing,
    - Apart from areas with there are constitutional limitations,
    - Or negative historical experience.
- Knowledge and pre-emption are seen as important for security, providing rhetorical support for surveillance.
- The economic costs of security are discounted or not important or not known or not well understood.
- Information security is increasingly part of security.
- An increasing focus on information security reduces the imbalance or opposition between the concepts of privacy and security.
- Cyber security is gaining increasing presence in security discourse.
- Surveillance is less well understood publicly than privacy.
- The UK has the highest level of discussion of surveillance using the terminology of surveillance.
- Technology is less privileged than law and regulation as a protection for privacy.
- What is identified as a privacy problem by political actors in each country will affect what the public sees as a privacy problem.
- Countries have "traditional" sources of threats to privacy, and this will attract (potentially disproportionate) public and policy attention.
- There is broad agreement for increased individual control (or determination) of their own data and strengthened rights for the data subject. This support does vary somewhat between Member States.

- Data protection regimes are represented as being at different levels of maturity.
  - This will affect the next steps or perceived needs.
- Monitoring and evaluation of privacy impact seen as part of a potential solution to privacy and surveillance problems.
- The EU exerts pressure on both security policy and policy regarding privacy, data protection and surveillance in Member States.
  - Different countries experience this pressure differently.
  - Different policy actors represent this pressure differently.
  - These pressures interact with the perceived maturity of the regulatory regime.
  - More established regimes are able to put up more resistance to non-desirable pressure.
  - Regimes that are new or that are re-evaluating data protection regimes may be more open to EU influence than those that are considered mature, stable and "generally acceptable".

Several key hypothesis were extracted from this long list and questions developed for the subsequent PRISMS survey.

1. The core of national security is represented consistently across countries, but the particular focus of security, and threats change between countries

How important are each of these security issues to you?

	Very important	Somewhat important	Unimportant
Corporate crime (e.g., bankers)			
Cybercrime / Cyber espionage / Cyber sabotage / hacking			
Identity fraud			
Street crime			
Terrorism			
Restrictions to fundamental freedoms			

2. Countries have 'traditional' sources of threats to privacy, and this will attract (potentially disproportionate) public and policy attention

Which of the following do you see as the biggest threat to your privacy?

a) My national government
b) Foreign governments
c) Companies
d) Criminals

How concerned are you about privacy threats from each of these organisations?

	Very concerned	Somewhat concerned	Unconcerned
Criminals / hackers			
Companies (banks, insurance companies, advertising companies, etc.)			
Social networks			
Police			
Intelligence services			
National government			
Foreign governments			

3. People from different countries will construct their data protection regime as having different levels of maturity

Are you aware of any efforts to reform privacy or data protection law in your country?
a) yes b) no

Are you aware of any efforts to reform privacy or data protection law in the EU?
a) yes b) no

Are you happy with privacy and data protection laws as they currently stand?
a) yes b) no

Do you feel that your privacy is sufficiently protected by existing laws?
a) yes b) no

Do you feel that your personal information is sufficiently protected by existing laws?
a) yes b) no

Do you feel that privacy and data protection laws need to be updated in response to changes in the way we use technology?
a) yes b) no

4. Information sharing for the purposes of security will be broadly supported by members of the public (Except where there is a history of negative experience)

Is it acceptable for the police and the intelligence agencies to share personal data with each other for the purposes of:

	Acceptable	Unacceptable	Not sure
Crime control			
Cybersecurity			
Preventing terrorism			
Internal management			
National security			
Taxation			
Public safety			

Should the police have access to any information sources that might help them in their investigations?
a) yes b) no

PART TWO

A Discourse Analysis of Selected Privacy and Security Policy Documents in the EU

6 DISCOURSE ANALYSIS – INTRODUCTION AND METHODOLOGY

Part II of this deliverable focuses exclusively on a discourse analysis of policy documents and is the result of research conducted as part of Task 3.2 Discourse analysis.

As mentioned earlier, the general aim of the study for this report was to gain a better understanding of how policy-makers in Europe conceptualise "security" and privacy" in different contexts (national, international, supra-national) and to capture how security and privacy policies are developed in distinct policy contexts, both on the European and Member State levels. The discourse analysis can contributes towards gaining such insights and reveal how specific concepts related to security and privacy (technologies) are used; how they frame perceptions, ambitions and expectations concerning security and privacy; and to some extend how they correlates with citizens' perceptions, needs and behaviour regarding privacy and security.

By complementing the horizontal analysis, the discourse analysis explored in this chapter is meant to shed more light on the intricacies of the privacy and security discourse from a policy perspective. The chapter includes an introduction to the theory of discourse analysis, followed by a brief overview of methodological approaches. It continues with a detailed section on the methodology adopted and adapted for the purpose of our report, and finally it applies that methodology to analyse policy documents of the UK (chapter 2), the Netherlands (chapter 3) and those of EU institutions (chapter 4).

6.1 INTRODUCTION TO AND REVIEW OF DISCOURSE ANALYSIS METHODOLOGIES

Discourse analysis – also referred to as 'critical analysis' – can be understood as a scientific approach (a manner of deconstructive reading) to analysing (written, vocal or sing) language use or any relevant communicative event. The analysis enables access to the ontological and epistemological assumptions behind a (legal) statement, strategy, policy or programme[185]. Moreover, discourse analysis reveals the motivations, ideas and interests behind a text, statement or conversation. Contrary to text linguistics, discourse analysis does not focus on text structures, but on the socio-cultural characteristics of the text[186].

An example of early discourse analysis (literary stylistics) is the study of Leo Spitzer '*Italienische Umgangssprache*' on spoken Italian (1922). In his study he attempts to analyse the forms of Italian conversation (through theatre texts, dialogues in novels and casual remarks of authors) in close connection with the conditions of the discourse and above all with the issue of the addressee[187]. Spitzer was one of the first language critics not only to study the structure of language but also the properties of the discourse and the larger conceptual or situational frame. Spitzer insisted upon using a philologically based approach of textual analysis[188] and perceived language style as an expression of a particular psychological, social or historical sensibility or moment rather than as a general property of a particular language.

[185] e.g. Frohmann, 1992.
[186] Iatsko, 2001.
[187] Voloshinove, 1973.
[188] Catano, 2005.

6.1.1 Michel Foucault and the "archaeological" approach

A key theorist of the discourse analysis, and in particular of the discourse itself, was the philosopher, social scientist and historian Michel Foucault. In one of his most influential works '*L'archéologie du savoir*' (1969), he referred to the institutionalised patterns of knowledge and power that become apparent in discourses. Foucault focusses his analysis on the '*énoncé'* or 'statement' and contends that each statement yields from a network of rules establishing what is meaningful. The whole of regular statements (written and spoken) which produce discourses (discursive formation) can be perceived as a body of anonymous, historical rules, determined in the time and space of a given period, and for a given social, economic, geographical, or linguistic area[189]. The body of rules limits the conditions of discourse's existence in the sense that it provides context and a normative value system (rules on what is 'proper' and 'improper').

"(...) discourse [is] a group of statements in so far as they belong to the same discursive formation; it does not form a rhetorical or formal unity, endlessly repeatable, whose appearance or use in history might be indicated (and, if necessary, explained); it is made up of a limited number of statements for which a group of conditions of existence can be defined."[190].

To reveal the body of rules which limit the conditions of discourse's existence, Foucault uses an 'archaeological' approach. This method seeks to describe discourses in the conditions of their emergence, existence and evolvement rather than in their hidden meaning, propositional or logical content, or their expression of a phycology. The archaeological analysis examines discursive formation only at its level of positive existence, and does not perceive discourses to be traces of something outside themselves. Foucault writes:

"Archaeology tries to define not the thoughts, representations, images, themes, preoccupations that are concealed or revealed in discourse, but those discourses themselves, those discourses as practices obeying certain rules. It does not treat discourse as a document, as a sign of something else, as an element that ought to be transparent, but whose unfortunate opacity must often be pierced if one is to reach at last the depth of the essential in the place in which it is held in reserve; it is concerned with discourse in its own volume, as a monument. It is not an interpretative discipline: it does not seek another, better-hidden discourse. If refuses to be 'allegorical'.

Archaeology (...) [aims] to define discourses in their specificity: to show in what way the set of rules that they put into operation is irreducible to any order; to follow them the whole length of their exterior ridges, in order to underline them the better. It (...) is not a "doxology"; but a differential analysis of the modalities of discourse. (...) It defines types of rules for discursive practices that run through individual oeuvres, sometimes govern them entirely, and dominate them to such an extent that nothing eludes them; (...) it does not try to repeat what has been said by reaching it in its very identity. (...) It is nothing more than a rewriting: that is, in the preserved form of exteriority, a regulated transformation of what has already been written. It is not a return to the innermost secret of the origin; it is the systematic description of a discourse object."[191]

[189] Hynes, 2006.
[190] Foucault, 1972, pp. 116-117.
[191] Foucault 1972, pp. 155-157.

Five elements are of primary importance in Foucault's archaeological method: (a) the analysis of the description of *discursive formations*, (b) the analysis of *positivities*, (c) the discovering of the *archive*, (d) the mapping of *enunciative* field, and (e) the detecting of *discontinuities*. As regards the *description of discursive formations* Foucault contends that this must be understood as the *totality* of statements, relations, regularities and transformations.

"(...) we must understand by this a sort of communal opinion, a- collective representation that is imposed on every individual; we must not understand by it a great anonymous voice that must, of necessity, speak through the discourses of everyone; but we must understand by it the totality of things said, the relations, the regularities, and the transformations that may be observed in them, the domain of which certain figures, certain intersections indicate the unique place of a speaking subject and may be given the name of author. 'Anyone who speaks', but what he says is not said from anywhere. It is necessarily caught up in the play of an exteriority"[192]

Foucault's method analyses only the *positivities;* the verifiably extant aspect of discourse. These positivities constitute discursive formations and relations from a *historical a priori* – a level of historical language which other types of analysis (e.g. structure analysis) depend on but do not address. Discourses function at the level of 'things said or written'; thus any analysis of the formal structure, hidden meaning or psychological traces of discourse take the level of the discourse itself for granted. The historical a priori is a feature of the level of discourse as opposed to other levels of analysis, which does not remain stable, but shifts with the transformation of the positivities themselves. As the discursive practice can change, even the a priori of the positivity can change.

In strong relation to the historical a priori is the '*archive'*, which Foucault defines as 'the general system of the formation and transformation of statements'[193]. Discourse description includes the dimension of a general history of the discourse that can be attributed to the rules of the discursive practice[194]. The analysis of particular discourses yields insight into change and transformation of rules as they have a certain periodic persistence. The transformation of rules is not a homogeneous, chronologically ordered, standard process, but an interplay between different formative systems[195]. The change from one system to the next is not an 'event', not a sudden occurrence of a single statement, but a process that contains several types of transformations and transitions from one condition to the other.

Another central term in the work of Foucault is the *enunciative* field. The level of statement operates by an enunciative function. If a statement is analysed in terms of the enunciative function, one describes the discursive conditions under which it could be said, rather than the grammatical, propositional or strictly material conditions (their appearance at a specific time and place) under which it could be formulated. An enunciation always involves a position from which something is said; this proposition is not defined by a psychology, but by its place within (and its effect on) a field of discourse in all its complexity. The enunciative function designates that aspect of language by which statements relate to other statements.

A last element of Foucault's method is the discovering of *discontinuities* in the history of thought. Foucault found that some of the discourses are regular and continuous over time as knowledge steadily accumulates and society gradually establishes what is (in that period of

[192] Ibid., p. XX.
[193] Foucault, 1972, p. 40.
[194] Jansen, 2005, p. 109 and Foucault 1972, p. 165.
[195] Ibid., p. 110.

time) truth or reason. However, in a transition from the one epoch to the other, there will be overlaps, interruptions and discontinuities as society reconfigures the discourse to match a new context. Thus, by analysing discourses, one is able to discover discontinuities in the conditions of human knowledge and reveal the 'epistemic' space.

"Beneath the great continuities of thought, beneath the suborn development of a science striving to exist and to reach completion at the very outset (...) one is now trying to detect the incidence of interruptions. Interruptions whose status and nature vary considerably. (...) they suspend the continuous accumulation of knowledge, interrupt its slow development, and force it to enter a new time, cut it off from its empirical origin and its original motivations, cleanse it of its imaginary complicities; they direct historical analysis away from the search for silent beginnings, and the never-ending tracing-back to the original precursors, towards the search for a new type of rationality and its various effects. (...) they show that the history of a concept is not wholly and entirely that of its progressive refinement, its continuously increasing rationality, its abstraction gradient, but that of its various fields of constitution and validity, that of its successive rules of use, that of the many theoretical contexts in which it developed and matured."[196]

The analysis of discontinuities is used in the genealogy phase of the discourse analysis. The intention of this phase is to grasp the total complexity of the use of power and the effects it yields. The discourse both reflects and creates power structures. Foucault closely relates power to knowledge, which he understands as the social structuring of what we perceive to be real[197]. Social power/knowledge complexes are produced and disseminated by institutions with which the scientific disciplines can be associated:

"*Each society has its regime of truth, its 'general politics' of truth: that is the type of discourse which it accepts and makes function as true (...) In societies like ours, the 'political economy' of truth is characterized by five important traits: [1] 'Truth' is centered on the form of scientific discourse and the institutions, which produce it; [2] it is subject to constant economic and political incitement (...); [3] it is the object, under diverse forms, of immense diffusion and consumption (circulating through apparatuses of education and information (...)), [4] it is produced and transmitted under the control, dominant if not exclusive of a few great political or economic apparatuses (universities, army, writing, and media); [5] lastly, it is the issue of a whole political debate and social confrontation."*[198]

At any moment in time, certain orders of knowledge determine the social 'truth', which is reflected by a multiplicity of discursive elements which are arranged in various strategies. These strategies can be understood as means to control, select, organize and canalise discourse. In his inaugural lecture at the Collège de France in 1970, Foucault distinguishes in this respect between three types of strategies:

- *Exclusion*. Foucault defines three principles of exclusion. Firstly, the discussion of certain subjects may be *prohibited*: social norms determine what people can speak of (or not) in which circumstances. Foucault writes: "In the taboo on the object of speech, and the ritual of the circumstances of speech, and the privileged or exclusive right of the speaking subject, we have the play of three types of prohibition which intersect, reinforce or compensate for each other, forming a complex grid which

[196] Foucault, 1972, introduction.
[197] e.g. Winkel, 2012, p. 82.
[198] Foucault, 1999, p. 131-135.

changes constantly."[199] A second principle of exclusion concerns *division and rejection*. Foucault refers to the distinction between reason and madness in which the discourse of madness is rejected. The third principle consists of the opposition between *true and false*. Our 'will to know' (*notre volonté de savoir*) is governed by a system of exclusion. The perceived truth constrains the discourse in the sense that it excludes what is (in a certain period of time) perceived as being false. The will of truth can turn towards a critique of the notion truth itself.

- *Internal procedures*. Foucault distinguishes between three types of internal procedures to control the discourse. The first is the division between *canonical text and their commentaries.* Some text are privileged (the canon, in religion, law, literature or science) and others are perceived as commentaries on these major texts. Foucault states: "I suppose (…) that there is scarcely a society without its major narratives, which are recounted, repeated, and varied (….). In short, we may suspect that there is in all societies, with great consistency, a kind of gradation among discourses: those which are said in the ordinary course of days and exchanges, (…) and those which give rise to a certain number of new speech-acts which take them up (…)." The second internal procedure is that of *the author* as a principle for the grouping of the discourses, conceived as the unity and origin of their meanings, as the focus of their coherence. Foucault states: 'The author is what gives the disturbing language of fiction its unities, its nodes of coherence, its insertion of in the real. (…) the individual (…) takes upon himself the function of the author: what he writes and what he does not write (…) this whole play of difference is prescribed by the author-function, as he receives it from his epoch.' The third principle concerns the *disciplinarily*. Disciplines constitute an anonymous system against the principle of commentary and the author as there is a constant need for new formulations within the discipline. Disciplines fix limits to what can be said within the discipline.

- *Limiting access*. Another strategy to influence the discourse is to control the condition of the application of discourse. Foucault distinguishes between four types of discourse control in this respect. The first exists of the *qualification of the speaking subject* which determines whether he/she is accepted as a meaningful contributor to the discourse. This qualification is based on a system of norms and values and rituals. The second manner to control the discourse is to let them take place in certain '*societies of discourse*' – discursive clubs which exclusively practice a select and restricted discourse. Thirdly, discourses can be controlled by *doctrines*, which can be understood as specific elements of a discourse which circulate among societies and exclude other doctrines[200]. The last strategy to control a discourse is the *social appropriation of the discourse*, by which Foucault means the learning about discourse, for instance through education.

By analysing these control mechanisms, Foucault tries to reveal the institutionalised patterns of knowledge and power in a certain period of time. He for instance examined institutionalised knowledge and power in the psychiatry, medicine and human sciences, respectively described in his three historical book 'Madness and Civilization', 'The Birth of the Clinic' and 'The Order of Things'. By reconstructing the discursive elements, the mechanisms of the discourse, effects produced and changes over time, Foucault tries to

[199] Foucault, 1970, II.
[200] Winkel, 2012, p. 83.

unravel rules of thinking, acting and judging. In this sense, one could say that Foucault examines the history of knowledge, reality and truth[201].

6.1.2 Methods of discourse analysis based on Foucault

In his work, Foucault does not provide many concrete instructions on how to empirically apply his concepts to policy analysis. Moreover, critics contend that Foucault focusses too much on theoretical constructs, which are confusing or even contradictory and therefore difficult to operationalize[202]. Some scientists have used the archeological approach of Foucault as a 'way of thinking' when conducting research using traditional methods, such as desk research and interviews[203]. However, other scientists actually tried to operationalize the archaeological method of Foucault. These scientists apply a specific discourse analysis methodology which is labeled as '*Critical Discourse Analysis*' (often referred to as CDA).
Philips and Hardy[204] developed a typology of different discourse analysis methodologies based on a distinction between two aspects a) the degree in which they *combine text and context* en b) the extent to which the approach is *qualitative or discourse analytical*. Whereas the qualitative approaches try to understand or interpret social reality as it exists, discourse analysis aims to uncover the way in which social reality is produced[205]. In addition, the discourse analytical research approach emphasizes that researchers have to make choices about the data they select, as the empirical research is restricted to available resources and time[206]. Dealing with all aspects of discourse theory in the same depth is impossible, and consequently the discourse analysis must be perceived as an interpretation of how social reality is produced.

Phillips and Hardy[207] provide a useful description of four main approaches of discourse analytical research (see figure 1 below). The approaches are categorized along two axes:

(1) *between text and context*, this concerns the degree to which research focuses on individual text or on the surrounding text (context). Phillips and Hardy distinguish between a proximal (or local) and a distal (broader social) context.
(2) *between constructivist and critical approaches*, this concerns the degree to which the research focuses on the social reality itself as opposed to process of social construction.

[201] Landwehr, 2001.
[202] e.g. Keller, 2007 and Winkel, 2012.
[203] Hewitt, 2009.
[204] Philips and Hardy, 2002.
[205] Philips & Hardy, 2002, p. 6.
[206] Ibid., p. 19.
[207] Ibid.

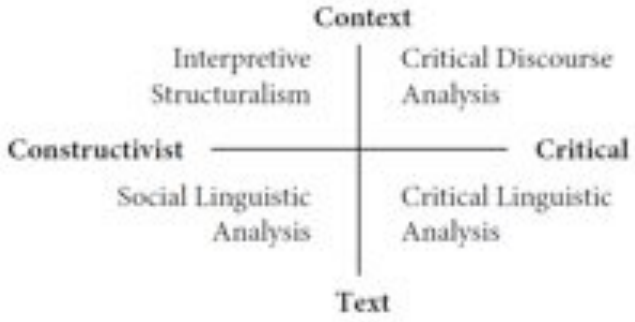

Figure 1: Different approaches to discourse analysis, Source, Philips and Hardy (2002)

As stated before, scientist elaborating on the work of Foucault generally belong to the tradition of critical discourse analysis, which not only concentrates on the main (proximal) text but involves surrounding (distal) texts (context) and include an analysis of power relationships.

6.1.3 Pêcheux's instrument of automatic discourse analysis

One of the first scientist who tried to bring the work of Foucault (and other social scientist such as Derrida) one step further was the French philosopher Michel Pêcheux. Pêcheux emphasized the need of developing an instrument for creating experimental (versus experiential) results[208]. Pêcheux's interest in the need of developing an empirical alternative to linguistic 'speculation', and his emphasis on theoretical and analytical rigor, induced hem to a much more detailed study of linguistics than was common among other philosophers of his time. Pêcheux problematized the traditional forms of content analysis which assumed an analyst to be capable of objectively 'reading' the meaning of a text[209]. Pêcheux wanted to avoid an ideological bias through the reading by the subject and developed the concept of *conditions of production of discourse*, in which the two subject positions – speaker and listener (or writer and reader) – had to be considered. In addition, he tried to develop a method for systematically analyzing a text, without the analyst 'feeding' it with information about the experiential meaning of the words that build up the discourses[210].

"Faire l'imbécile: c'est-à-dire décider de ne rien savoir de ce qu'on lit, de rester étranger à sa propre lecture, d'en rajouter systématiquement sur le morcellement spontané des séquences, pour achever de libérer la matière verbale des restes de sens qui y adhèrent encore."[211]

Key in the approach of Pêcheux, was the concept of the *metaphoric effect*[212]. He stated that meaning is an effect of metaphoric relations (of selection and substitution) which are specific for the conditions of the production of a statement. Metaphoric relations can be understood as the interrelatedness between words. In other words, the meaning of a discourse is created by the relation of words to other words that are not said, words that could not be said (because of value systems – e.g. taboos) and words that are previously said.

[208] Helsloot and Hak, 2007; Henry, 1995.
[209] Helsloot and Hak, 2007, p. 9.
[210] Helsloot and Hak, 2007, p. 11.
[211] Pêcheux, 1981, p. 16.
[212] Ibid., p. 29-33.

The instrument Pêcheux developed was based on an approach developed by Harris[213], who proposed to first conduct a formal analysis of recurring patterns within a text instead of defining pre-given meanings, and subsequently to derive meaning from this formal analysis[214]. Contrary, to the approach of Harris, Pêcheux's method did not focus on one text, but involved a whole body of texts as Pêcheux aimed to construct a field of metaphors. In this way the analyst could not only reveal what was said or written, but also what was not.

The approach developed and labeled by Pêcheux 'Automatic Discourse Analysis' consists of three phases, namely: (1) the phase of the corpus construction, (2) the phase of linguistic analysis, and (3) the phase of the interpretation of the findings. In the first phase of Pêcheux' method, the object of the study is delineated (which discursive formation is to be studied?) and the texts (documents, legislations, statements) and/or vocal expressions are selected. This set of texts and other (e.g. audio, video) material constitutes the 'corpus'. In the second stage of linguistic analysis, all sentences of the corpus are rewritten in metaphoric matrices. Word relations of synonymy and opposition are structured within a format, which exercise yields matrices. In the third phase, these metaphoric matrices (also called *semantic domains*) are interpreted.

While using his approach, Pêcheux found several shortcomings. For instance, as in the metaphoric matrix only relations of synonymy and opposition were included, other relations between elements (e.g. oriented relations) were disregarded. Consequently, word relations which were not an explicit part of the discourse studied (but part of a related discourse) were ignored and certain power relations (e.g. ideological struggles) could not be detected. These omissions, and the criticism of his approach in the linguistic literature[215] resulted in Pêcheux's reconsideration of the theory underpinning his automatic discourse analysis. Pêcheux introduced his theory of interdiscourse, defined as "*tout complexe à dominante des conditions de production du discours*", which assumed that an 'interdiscursive' domain (linguistic 'outside' of single discourses) had to be taken into account.

Pêcheux, however, did not substantially change the method of automatic discourse analysis based on his new theory. In his last years, Pêcheux distanced himself from the automatic discourse analysis instrument and tried to search for a solution for desubjectification – possibilities of a non-subjective position for the analyst to study texts. In addition, he kept emphasizing the importance of tracing the interdiscourse.

"Ainsi, il ne s'agit pas d'une lecture plurielle […] où un sujet jouerait à multiplier des points de vues pour mieux s'y reconnaître. C'est une lecture où un corpus stratifié et hétérogène est articulé en profondeur et où, en fonction de cette lecture, sa structure même se modifie. Il s'agit d'une sorte de lecture où le sujet qui lit sera responsable du sens qui se déchiffre et il en sera en même temps dépossédé. L'interprétation suit alors les traces de l'interdiscours qui, n tant que telles, sont préconstruites et parcourues."[216]

As Pêcheux deceased in 1983, he was not able to finish his work on the analysis of (inter)discourses. Some critics contend that Pêcheux leaves more questions than answers.

[213] Harris, 1952.
[214] Pêchuex stated in 1982 in an interview with Woetzel and Geier: "Harris était fascinant puisqu'on sentait qu'il y avait là quelque chose, que ça permettait de s'en sortir […] à partir d'une position herméneutique et intuitive aussi bien qu'à partir d'une position 'lexicométrique' et positiviste."
[215] For example Provost-Chauveau, 1970 and Trognon, 1972.
[216] Pêcheux, 1983, p. 54.

Helsloot and Hak[217] for instance state that: "The analyst keeps getting stuck in formulations of contradictions one would rather like to avoid: logicism versus sociologism, seriousness versus play, linguistics versus poetry, heterogeneity versus homogeneity, interpolation versus disengagement." Yet, Pêcheux played an important role in the discourse analysis domain as he was one of the founders of a specific approach of critical discourse analysis which can be characterized as 'formal' or 'structured'.

6.1.4 Methodologies based on Pêcheux

Several scientist elaborated upon Pêcheux' 'formal' approach. Maarten Hajer[218] for instance proposed three tools to help arrange research materials. These are 'metaphor' (i.e. generally two or three word phrases which symbolize the key ideas of the discourse such as 'ageing problem'); 'story line' (a sum up of the discourse by means of metaphors); and 'discourse coalitions' (actors sharing the usage of a particular set of story lines over a particular period of time and in the context of an identifiable set of practices) [219] [220].

Dryzek[221] follows a similar approach. First he creates a framework of environmental discourse according to two dimensions of political ideology and practice and then he analyses the research material within each dimension to define four key elements: (1) the basic entities whose existence is recognized or constructed, (2) assumptions about natural relationships between different entities, (3) agents and their motives, and (4) the key metaphors or other rhetorical devices that figure in the discourse[222].
Sharp and Richardson[223] added another element to be examined while analyzing the corpus: signs of transformation of the discourse. This can be perceived to be in line with the archaeological approach of Foucault as he (as stated above) emphasized the importance of the detecting of discontinuities in the discourse. It is in particular here, that power structures can be revealed. According to Sharp and Richardson researchers should in this respect focus on new practices, changes in communication, and linkages between these changes and institutional structures. This can for example be done through collecting descriptions, particularly of opposing views, from people, documents and studying practices. New insights can for instance be gained by discovering differences between policy formation and the way policies actually play out in practice.

Other notable efforts to operationalize content analysis include those of Fairclough and Ruiz.
Fairclough's approach proposes a three-dimensional framework including text analysis (entailing the study of the structure of the text, vocabulary and grammatical cohesion); analysis of the discursive practice (involving the analysis of the processes in which texts are framed, that is, the context in which statements are made and feed into other debates); and analysis of social practice (which requires a study of discourse in relation to wider power structures and ideology). Similarly, Ruiz describes a multi-step process that could be employed and which includes text analysis, context analysis and sociological analysis.

[217] Helsloot and Hak, 2007, p. 20.
[218] Hajer, 2005.
[219] Ibid.
[220] Hajer, 2005, Hewitt, 2009.
[221] Dryzek, 2005.
[222] Dryzek, 2005, p. 19.
[223] Sharp and Richardson, 2001.

6.2 SELECTING A DISCOURSE ANALYSIS METHODOLOGY

From this brief inventory of possible analysis methodologies we selected the approach proposed by Hajer as the most suitable for the purpose of our study.

As mentioned earlier in this section, Maarten Hajer[224] proposes three tools to help systematize research documents. These are: 'metaphor', 'story line' and 'discourse coalitions'[225]. Metaphors are generally two- or three-word phrases which symbolize the key ideas of the discourse such as 'ageing problem' or 'fight against cybercrime'. Story lines summarize the discourse in a short description using the metaphors. As Hajer states, an analyst of texts "quickly realizes that in any field there are a couple of such stories, which fulfill an especially important role"[226]. Discourse coalitions can be understood as "a group of actors that, in the context of an identifiable set of practices, shares the usage of a particular set of practices".

Hajer, in addition to these three analysis tools or devices (i.e. metaphor, story lines and discourse coalitions), suggests the following step-by-step approach to conducting content analysis:

1. Desk research which should provide a first chronology and first reading of events.
2. "Helicopter" interviews meant to gain an overview on the issues from different perspectives.
3. Document analysis aiming to identify storylines and metaphors, and the sites of discursive struggle.
4. Interviews with key players to enable the researcher to construct the interviewee discourses and the shifts in recognition of alternative perspectives.
5. Sites of argumentation consisting of identifying the data which might account for the argumentative exchange.
6. Analysis of positioning effects in order to reveal how individuals, institutions or countries become engaged in some form of interplay.
7. Identification of key incidents in order to understand the discursive dynamics and the outcomes.
8. Analysis of practices in particular cases of argumentation, to be achieved by revisiting the original data in order to assess whether the meaning of the discourse or statements can be related to practices.
9. Interpretation, consisting of an account of the discursive structures, practices and sites of production.
10. A second round of interviews with key actors during which interviewees should recognize some of the hidden structures of language.

6.3 DISCOURSE ANALYSIS METHODOLOGY

As mentioned in the previous chapter, for our research we have adopted and adapted the methodology proposed by Maarten Hajer. For each country we studied and for the EU a similar methodological approach was applied in order to be able to compare the dominance of discourses in the various geographic areas and socio-cultural contexts. The comparison will be part of the final report.

[224] Hajer, 2005.
[225] Hajer, 2005 and Hewitt, 2009.
[226] Hajer, 2005, p. 301.

Subsequently, we tested the methodology: on a limited selection of policy documents (the UK case) so well as on a more extensive selection of policy and other types of documents providing context to the policy documents (the case of the Netherlands and the case of the EU institutions). The three cases are described in the following chapters of this preliminary report D 3.1.
The method we employed and which is described below will be further refined in part two of our research and input from interviews will be added, resulting in the final deliverable 3.2.

The main steps of our methodological approach are as follows:

1. *Systematic document analysis - Identification of key actors, metaphors and storylines*
   - In the first step the key actors, metaphors and storylines in the two policy domains – security and privacy – are identified.
   - *Actors and word combinations*. For each actor, key documents are identified and most frequent word combinations are plotted in 'phrase clouds'.
   - *Metaphors*. Of the most frequent word combinations, the 'metaphors' are selected. Metaphors can be understood as word combinations (cues) which stand for something else (a broader concept, belief or idea). For instance, in the 80s in the Netherlands, the term 'acid rain' was frequently used by Dutch politicians and activists to stress the impact of environmental pollution. A such, 'acid rain' came to be used in reference to a multitude of negative consequences, some of which had nothing to do with environmental pollution[227].
   - *Story lines*. For each metaphor the story line is identified. The story lines consist of statements, often in the form of a narrative (conveying facts in story form). The story line has a certain structure and describes cause and effects (logics). A story line is a condensed statement summarizing complex narratives, used by people as 'short hand' in discussions[228]. For instance, the phrase of the European Commission '*Advancing people's Europe*' could be perceived by some readers as a metaphor for the discussion on the European democratic deficit and the legitimacy of EU institutions. When in fact the story line of the European Commission is that *EU citizens should benefit more from the EU and that the EU should demonstrate citizens its added value to strengthen EU citizens' involvement*.
   - *Scientific perspective.* The metaphor and story lines are reflected upon from a more scientific perspective. For instance, as regards the metaphor 'Advancing people's Europe', the scientific questions concern the legitimacy of the EU.
   - *Deliverable*. To create an overview, the key actors, documents, metaphors, story lines and the problem perceived from a scientific perspective are structure in a table.

2. *Table analysis - Identification of discourse coalitions and their influence*

In step two we proceed to analyze the information in the table described in the previous step. We do so by comparing key metaphors used and story lines produced by institutions and discourse coalitions that can be identified. In addition, by examining the institutionalization of metaphors and story lines, we can infer the extent of their influence.

   - *Discourse coalitions*. A discourse coalition refers to a group of actors that, in the context of an identifiable set of practices, shares the usage of a particular set of story lines over a particular period of time. By comparing the metaphors and story lines as they appear in the table, the discourse coalitions can be identified.

[227] Hajer, 2005, p. 304.
[228] Hajer, 2005, p. 302.

- *Institutionalization*. If a discourse solidifies in particular institutional arrangements then the discourse is institutionalized. A discourse can be institutionalized in several ways, for instance when legislation is drafted, a new public official is appointed, a new agency is established or new forms of cooperation are realized. This step consists of identifying institutional arrangements for each discourse coalition.
- *Dominant discourses*. Metaphors and story lines which are used by most actors (discourse coalitions) and that are also most institutionalized can be identified as dominant discourses .
- *Deliverable*. Coalitions and institutionalization are structured in a second table, which will allow us to analyze the dominant discourses.

3. Interviews with key players

On the basis of preceding steps, interviews will be conducted with central actors in the dominant discourses. The interviews may be used to:

- Validate the identified key actors, metaphors and story lines.
- Generate more information on causal chains (which led to what).
- Achieve a better understanding of the meaning of particular events for the interviewees.[229] The interviewee could for instance be asked how he/she interprets a particular event (e.g. 9/11).
- Sites of the discourse production.
- Reveal shifts in thinking, questions can be asked on the reframing and transformation.

4. Interpretation

In this step we try to find the discursive order that governed the privacy and security domains during a particular period of time or at a specific point in time. An analysis will be made of both statements made *and* the obvious absence of relevant topics or poorly articulated arguments, concepts and ideas. In addition, we describe the type of relationships between security and privacy as well as the factors which might have played an important part in determining the scope and range of a policy described.

5. Cross-country comparison

This part of the analysis will be performed primarily for the final deliverable. Discourses in several EU Member States and the discourse at EU level will be compared and the key differences and similarities will be described. There are broad socio-cultural differences across Europe and they might be revealed in this part of the analysis (for example in terms of differences in the tone, level and substance of the discourse).

6. Hypotheses to be tested in the survey

Finally, the discourse analysis will provide input for constructing hypotheses that will be tested in the survey. The survey will be conducted as part of work package 8. New developments likely to shape the security and privacy discourses will be monitored throughout the duration of the project and if relevant be included in the further analysis in the final deliverable.

The level of interest by members of the public in the topics security and privacy and their interrelation would be extremely relevant for the analysis. For this reason, this has been added as a further step to the methodology. However, the means to gauge such interest in an

[229] Ibid., p. 306.

objective and comprehensive way were absent. As an imperfect proxy we made an analysis of Google searches for “privacy”, “security” and both terms together from 2005 to date.

The following three chapters illustrate the way in which the discourse analysis methodology was used.

7 PRIVACY AND SECURITY DISCOURSES IN SELECTED UK POLICY DOCUMENTS

7.1 INTRODUCTION

This chapter examines how select UK policy documents, and thus some British policy-makers, conceptualise security and privacy. It specifically explores how these terms are contextualised within larger policy discourses within the UK, and provides material that will enable cross-national comparison with Dutch policy documents and European policy documents treated in other chapters. Although the analysis is based on a very small sample of UK policy documents, they reveal that British policy appears to be more concerned than other countries with the relationship between surveillance and privacy, the benefits that surveillance technologies can bring to society and the provision of security using new technologies. However, like other countries, UK discourse primarily relies upon the trope of providing a "balance" between security and privacy, which are often constructed as oppositional.

7.1.1 Methodology

This discourse analysis is based on an examination of five recent UK policy documents. These documents were selected from a long list of UK policy documents, from 2000 onwards that the PRISMS project identified in chapter. As described in that chapter, researchers selected key security and privacy policy documents from each of six European Member States and the USA for further analysis. Chapter 12 produced a horizontal analysis of all of the sample policy documents, while this chapter intends to provide an in-depth analysis of the sample policy documents for specific countries. This analysis follows the methodological guidelines set out in chapter 13, with the caveat that this chapter only examines the sampled policy documents from the UK, not all of the documents contained in the chapter 5 "long list". The sampled UK policy documents include the following:

- A 2006 report by the Surveillance Studies Network for the Information Commissioner's Office (the UK Data Protection Authority), entitled *Report on the Surveillance Society*[230],
- A 2008 report from the House of Commons Home Affairs Select Committee, entitled *A Surveillance Society?*[231],
- A 2009 report from the House of Lords Constitutional Committee, entitled *Surveillance, Citizens and the State*[232],
- A Joint Committee on Human Rights examination of the proposed Protection of Freedoms Bill from 2011[233], and

[230] Surveillance Studies Network, *A Report on the Surveillance Society For the Information Commissioner*, Information Commissioner's Office, September 2006.
[231] House of Commons Home Affairs Select Committee, *A Surveillance Society?*, Fifth Report of Session 2009-10, HC 58-I, The Stationery Office, London, 8 June 2008.
[232] House of Lords Constitution Committee, Surveillance: Citizens and the State, Second Report of Session 2008-09, HL Paper 18, The Stationery Office, London, 6 February 2009.
[233] Joint Committee on Human Rights, Legislative Scrutiny: Protection of Freedoms Bill, Eighteenth Report of Session 2010-12, HL Paper 195/ HC 1490, The Stationery Office Limited, London, 7 October 2011.

- A Ministry of Defence *White Paper* on national security from 2012, entitled *National Security through Technology*[234].

7.2 KEY DISCOURSES

The discourse analysis of these five UK policy documents identified four key discourses: "The surveillance society"; Finding a proportionate balance between security and privacy; Surveillance, security and their associated technologies have social benefits; and, Supporting the security industry. For each discourse this chapter identifies the metaphors associated with that discourse, the storylines that form part of that discourse and the ways in which that discourse has become institutionalised.

7.2.1 The surveillance society

"The surveillance society" was a key discourse running through four of the sampled UK policy documents (the exception being the Ministry of Defence *White Paper*). Although this analysis is limited by the small sample size, the characterisation of the UK as a "surveillance society" has heavily influenced the mass media as well as government discourse. Within this discourse, the following table demonstrates that metaphors such as excessive surveillance and big brother form part of the policy understanding of how surveillance is carried out in the UK. This discourse was very complex and included a number of storylines and associated sub-storylines, many of which outlined the negative effects that surveillance has on privacy, trust and individual rights. They key storylines were as follows:

- Surveillance is part of contemporary life,
- Surveillance reduces trust while privacy enhances trust,
- Surveillance negative impacts on human rights, democracy and ethics, and
- Surveillance poses significant regulatory hurdles.

All of the storylines and sub-storylines are presented in detail in section 1.5.1.

Metaphors	Storylines	Institutionalisation
Surveillance society Modernity Excessive surveillance Big brother Trust Transparency Discrimination Social sorting Risk Data protection Regulation Privacy Impact Assessment	Surveillance is part of contemporary life in Britain • The scale of surveillance has increased • Surveillance and technology are interlinked Surveillance reduces trust while privacy enhances trust • Excessive surveillance erodes trust and implies a lack of trust • Surveillance can disrupt the relationship between citizens and the state • Public trust is linked with good protection of privacy	"Surveillance society" becomes part of government discourse as evidenced by the policy documents analysed here. Production of policy recommendations, possibly influencing the Protection of Freedoms Bill

[234] Ministry of Defence, *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security*, The Stationary Office, London, February 2012.

Metaphors	Storylines	Institutionalisation
	Surveillance has negative impacts on human rights, democracy and ethics • Surveillance is risky • Surveillance can result in discrimination Surveillance poses significant regulatory hurdles • A right to privacy is difficult to define in the UK • There are few regulations surrounding specific types of surveillance in the UK • Existing mechanisms to limit surveillance are too weak • Some legislation has been introduced to better protect human rights • Some measures may risk new infringements of individual rights • The risks to privacy, data protection and other rights should be assessed	

7.2.2 Finding a proportionate balance between security and privacy

The selected British policy documents primarily constructed security and privacy as oppositional elements that needed to be balanced against one another, where protection of one implied undermining another. This discourse was primarily presented in the policy documents produced by the different Parliamentary committees, such as the House of Lords Constitution Committee, the House of Commons Home Affairs Select Committee and the Joint Committee on Human Rights. However, the section below explains that other actors also utilised this discourse to describe the relationship between privacy and security.

Metaphors	Storylines	Institutionalisation
Fair balance Balance Interfere disproportionately with individual rights Less intrusive mechanism	Striking a proportionate balance Some interference with human rights is justified in relation to security Surveillance systems must be "necessary and proportionate"	The Protection of Freedoms Bill was passed in 2012.

7.2.3 Surveillance, security and their associated technologies have social benefits

This discourse was primarily produced in policy documents written by government agencies including the Parliamentary committees identified above as well as the Ministry of Defence National Security Strategy. The proposed benefits include security benefits such as fighting crime, protecting public safety and reducing fear of crime, as well as providing "national security". Significantly, the Ministry of Defence specifically links the provision of benefits to national security as occurring *through* the use of technology. Furthermore, this discourse

raises the prospect of economic benefits in the public and private sectors, where surveillance and information collection technologies offer personalisation and efficiency.

Metaphors	Storylines	Institutionalisation
Better national security through technology Personalisation Choice Efficiency	Technology can contribute to better national security Security is important for freedom Surveillance can help fight crime, protect public safety and reduce fear of crime Surveillance can offer commercial or economic gains including efficiencies	Implementation and proliferation of security and surveillance technologies in the public sector and the commercial sector Public support for security and surveillance technologies

7.2.4 Supporting the security industry

The fourth major discursive thread emerged from the most recent (2012) Ministry of Defence *White Paper* on the national security strategy. In it, the government, via the Ministry of Defence stressed the inter-relationship between the security industry and the economic health of the UK. The Ministry of Defence also foregrounded technology within their understanding of the method through which better national security could be provided, including the use of technology to provide operational advantages. However, the focus on economics also resulted in the policy document including storylines about technologies providing value for money and the government taking better advantage of existing commercial developments rather than developing technologies and systems in isolation.

Metaphors	Storylines	Institutionalisation
Competitive economy Healthy defence and security industry Strong, sustainable, and balanced growth Operational advantage Government as technology customer Value for money	Security technologies are a key economic area for the UK Technologies must provide value for money Government should take better advantage of commercial developments	Implementation of the strategy Establishing elite Technology and Innovation Centres

These four discourses demonstrate that there are a number of competing discursive streams within UK policy documents focused on security and privacy. While some discourses within these policy documents appear to be referencing and supporting a discourse that is highly critical of government policy surrounding surveillance and security technologies and practices, other discourses appear to be supporting current policies and advocating an expansion of the surveillance and security system. Furthermore, while some discourses foreground privacy and other ethical considerations, others appear to omit these considerations all together. In consequence, these discourses highlight the complex and contested nature of security and privacy policy within the UK context.

7.3 KEY ACTORS AND WORD COMBINATIONS

This section outlines primary actors and word combinations that were used in each of the discourses. This section is limited to phrases which are repeated by particular actors within these documents, not sole mentions of particular phrases within the documents. For the British policy context, these word combinations largely aligned with the metaphors presented in the different discourses.

The surveillance society

The word combinations utilised within the "Surveillance society" discourse primarily centred on three themes or metaphors, as outlined in the following figure:

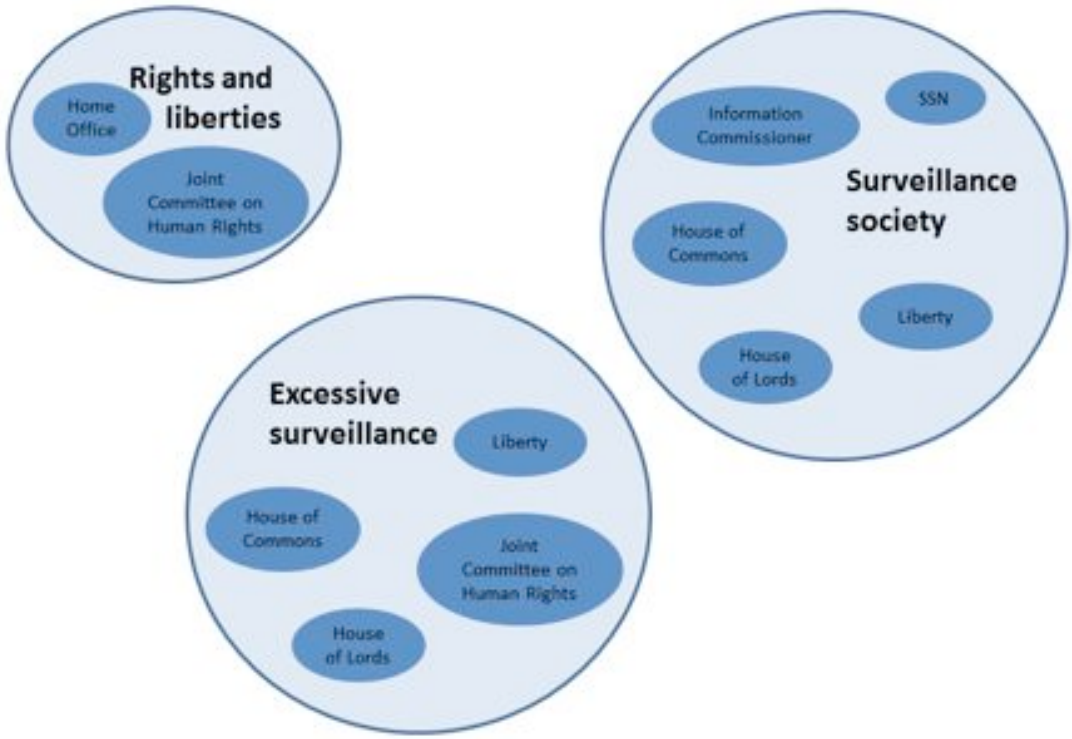

Figure 1: Actors and word combinations within the "Surveillance society" discourse

The "surveillance society" word combination captures the specific actors that utilised the phrase "surveillance society". In addition to report authors, the Information Commissioner, as a government-embedded privacy and data protection advocate, and Liberty, a civil society organisation also utilised this phrase. The second theme, excessive surveillance, also includes references to surveillance that was described as intrusive or over-zealous. Again, while all of the actors were authors of reports, Liberty was also represented as having utilised this phrase. The rights and liberties phrase includes references to human rights, individual rights and individual liberties. Although all of the actors here are government, and CSOs appear to be a surprising omission, this only means that CSOs were not quoted discussing the specific terms "civil liberties", "individual rights" and "human rights" repeatedly within these five documents. The term is attributed to the document authors if they frame the discussion. Clearly, these are all issues that these CSOs regularly discuss.

Finding a proportionate balance between security and privacy

Figure 2: Actors and word combinations within the "Balance" discourse

The figure above demonstrates that it was primarily government and police actors who reproduced the discourse about security and privacy requiring a balance. Actors included government representatives such as the Home Office, House of Commons, etc., as well as policing organisations such as the Association of Chief Police Officers (ACPO). Perhaps surprisingly, the Deputy Information Commissioner is also represented as having utilised this conceptualisation within these documents, despite the fact that the Information Commissioner's Office, as the UK Data Protection Authority, is often aligned with discourses similar to civil society organisations and other privacy advocates.

Surveillance, security and their associated technologies have social benefits

In addition to mentioning the "benefits" that surveillance and security technologies can bring to the UK, actors who utilised key phrases within this discourse also refered to capturing "operational advantage" and providing "choice" and "personalised" services to "customers".

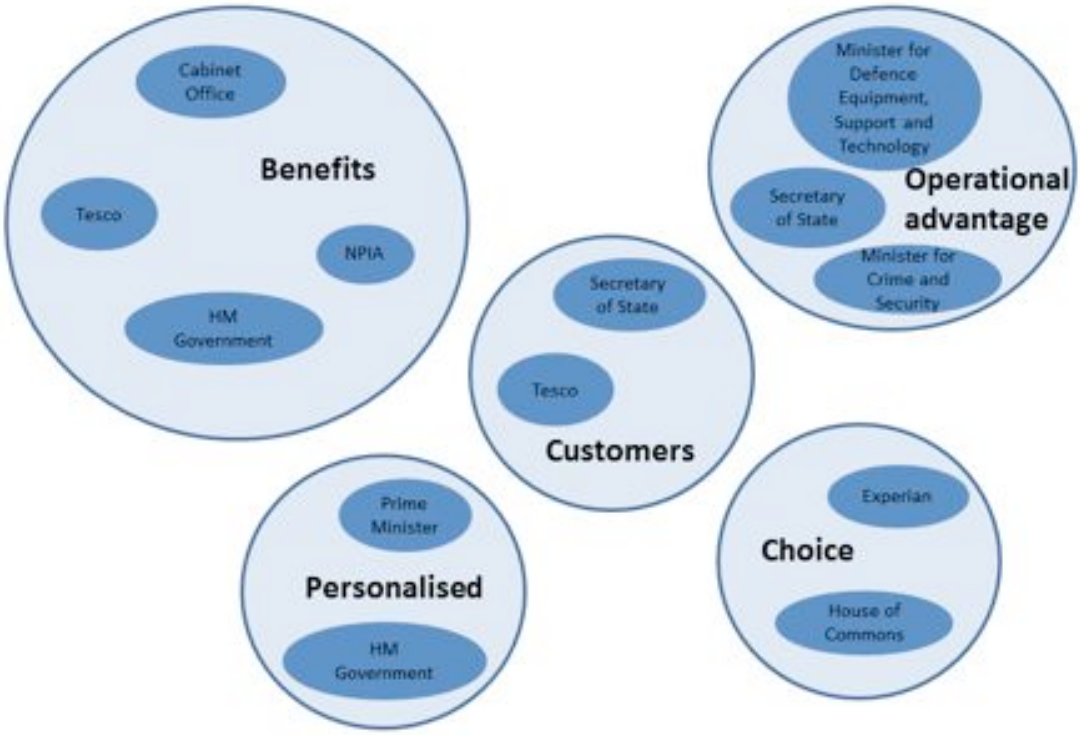

Figure 3: Actors and word combinations within the "Benefits" discourse

Within this discourse, the phrase "operational advantage" also referred to having a technological advantage over adversaries including state and non-state actors within the realm of national security as well as crime fighting. While many of these actors are traditional government agencies, e.g., the House of Commons, Her Majesty's (HM) Government and the Secretary of State, were primarily responsible for using these terms, other quasi-government actors such as the National Policing Improvement Agency (NIPA) also used these phrases.[235] Furthermore, it is not surprising that private companies such as Tesco, a large supermarket chain in the UK, and Experian, a private credit referencing agency, begin to appear within this discourse. Nor is it surprising that academics and civil society organisations are not associated with repeated discussions surrounding the supposed benefits that surveillance and security bring to citizens.

Supporting the UK security industry

Two word combinations were repeated frequently within this discourse – "national security" and "industry". The figure below illustrates that government actors were primarily responsible for repeating these prhases; however the Surveillance Studies Network is included due to a discussion within their report about the interlinkages between the surveillance industry and the government in relation to providing national security.

[235] The police service in the UK falls under the jurisdiction of the Home Office.

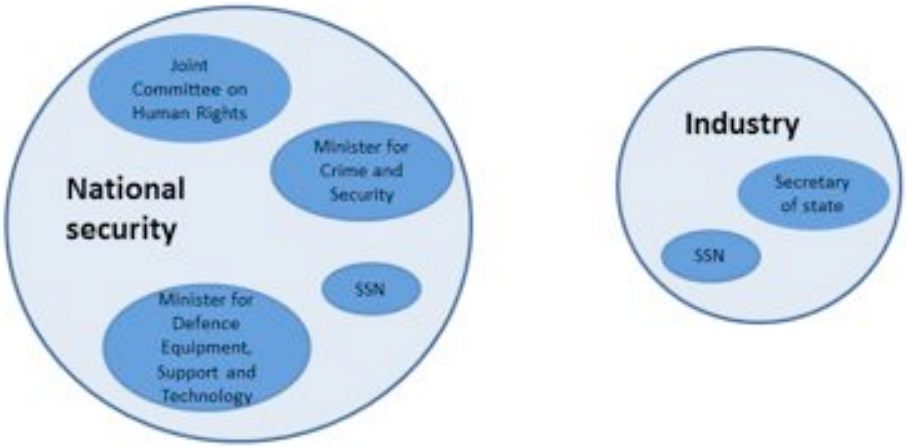

Figure 4: Actors and word combinations within the "Supporting" discourse

These figures outline the different actors and word combinations that are common within the four different security and privacy discourses present in the sample of UK policy documents. These graphics illustrate that different types of actors are primarily associated with different discourses and word combinations. Therefore the security and privacy discourse in the UK is being contested and negotiated by different actors and in different documents.

7.4 PUBLIC INTEREST

In addition to examining actors and word combinations, the level of interest by British members of the public in security and privacy, as well as their inter-relation, is also significant here. An analysis of Google searches for "privacy", "security" and both terms together from 2005 onwards suggests that British public interest in "security", "privacy" and their inter-relationship has decreased slightly over time, although it has generally remained relatively stable. The graphics below reflect trends in search terms, and they are measured as a percentage of peak search activity over time. Thus, the graphs are not comparable to one another, they only reflect changes over time in relation to specific search terms. The table below demonstrates the number of Google searches carried out by British users from 2005 onwards.

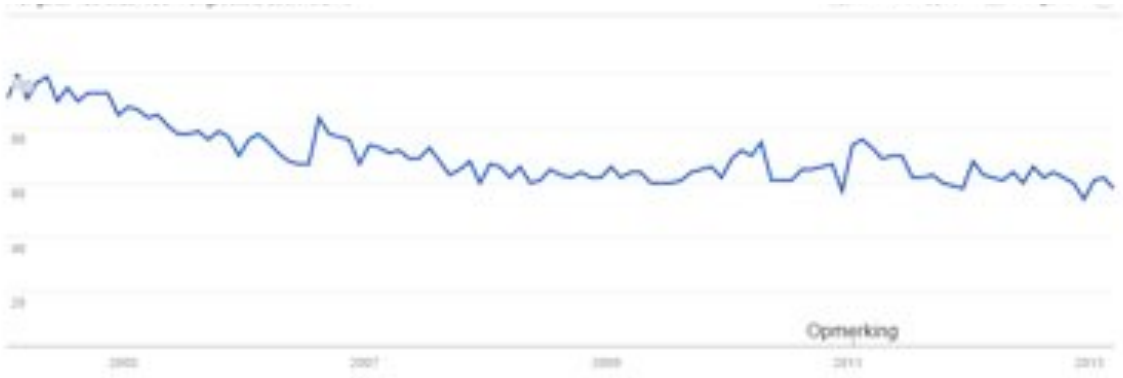

Figure 5: The frequency of the term 'security' entered by UK users into Google search engine (2005-present)

Here, UK users searched issues related to "security" most frequently in 2005, with a steady decline to 2007. From 2007 onward, searches related to security remained somewhat constant with occasional spikes in interest.

Figure 6 below reflects searches related to "privacy" over the same period.

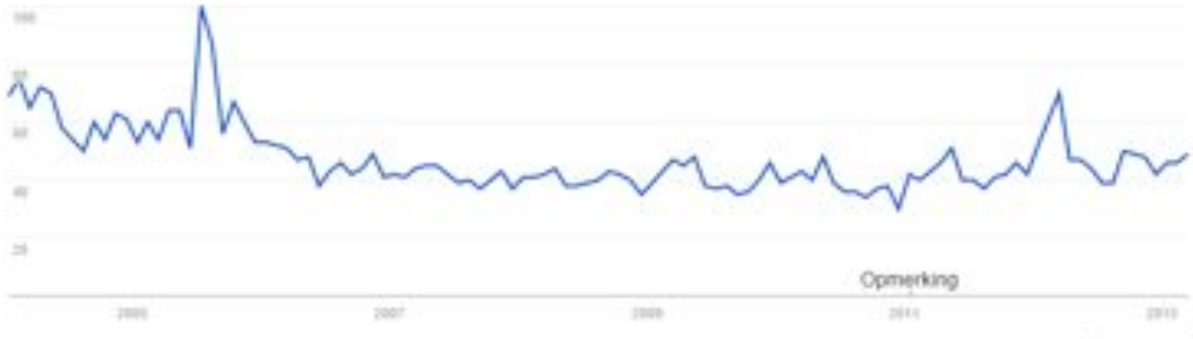

Figure 6: The frequency of the term 'privacy' entered by UK users into Google search engine (2005-present)

The search trends for "privacy" indicate a clear spike in interest in late 2005 and a minor spike in interest in 2012. However, over time, there was less sustained interest in privacy, since the period between the two spikes in interest indicate that overall interest was hovered around 40% of the peak levels, while security remained slightly higher at approximately 60% of peak levels. This suggests that particular events, for example debates around the introduction of identity cards in the UK, might generate peaks in interest in privacy among the general public.

Finally, we examined the frequency with which British users of Google entered both "security" and "privacy" into the search bar at the same time.

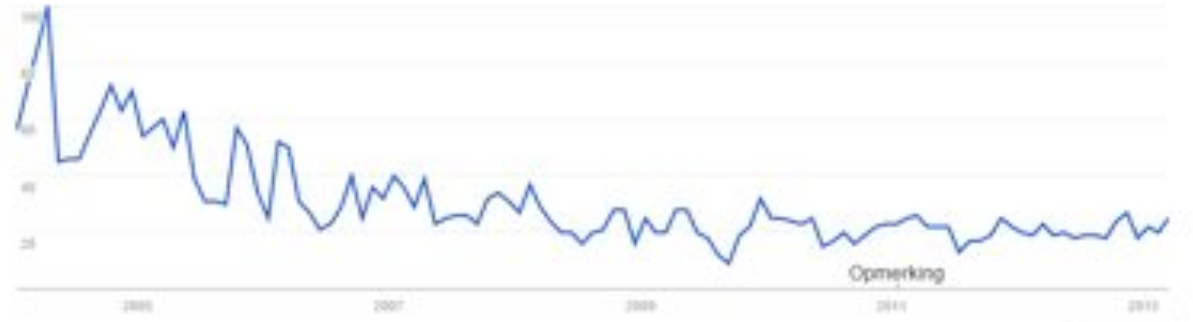

Figure 7: The frequency of the terms 'privacy' and 'security' entered together by UK users into Google search engine (2005-present)

Despite a spike in 2005, which may align with the terrorist incidents in July 2005, relative interest in the inter-relationship between privacy and security appears fairly low. It appears to have steadily declined before levelling off at approximately 20% of peak interest rates in 2009.

In general, the British public appears to have more sustained interested in security in comparison to privacy, and relatively less interest in their specific inter-relationship. However, this is based purely on an analysis of terms entered into one particular search

engine[236] by a specific sub-section of the British population, i.e., computer and internet users. Furthermore, this tool does not enable a comparison between the search rates for different terms. As such, it would be difficult to draw any specific conclusions about how this display of interest links to wider policy discourses in the UK.

7.5 DESCRIPTION OF SECURITY AND PRIVACY DISCOURSES

As outlined above, there were four different discourses emanating from the selected UK policy documents in relation to security and privacy. This section provides more detail about each of the four discourses by describing each of the storylines, and where appropriate sub-story lines, that make up that discourse. As far as possible, this section also includes information about which actors utilised those discourses and any contradictions between different policy documents.

7.5.1 The surveillance society

The "surveillance society" discourse is made up of four distinct storylines. The idea that surveillance is part of life in Britain, that surveillance reduces trust while privacy enhances trust, that surveillance has negative effects on human rights democracy and ethics and that surveillance poses significant regulatory hurdles. Each of these storylines are comprised of a small set of sub-storylines, that are examined in detail under each storyline heading.

Surveillance is part of life in Britain

The "surveillance society" discourse includes a storyline that characterises technological surveillance as "part of life" in Britain. This storyline also constructs the pervasiveness of surveillance as entwined with advances in technology. It is primarily a result of statements by the Parliamentary committees, the Surveillance Studies Network (SSN) and government agencies such as the Minister for Security, Counter-terrorism, Crime and Policing at the Home Office. This storyline includes descriptions of surveillance as "one of the most significant changes in the life of the nation since the end of the Second World War"[237] which has further increased in the last decade[238]. Within these documents surveillance is described as "inescapable", "normal", "widespread" and "routine" [239] as well as "unremarkable" and "just part of the fabric of daily life"[240]. According to the House of Lords Constitution Committee:

> [e]very time we make a telephone call, send an email, browse the internet, or even walk down our local high street, our actions may be monitored and recorded. To respond to crime, combat the threat of terrorism, and improve administrative efficiency, successive UK governments have gradually constructed one of the most extensive and technologically advanced surveillance systems in the world.[241]

Thus, surveillance permeates daily life in the UK and is utilised by the government for a number of different purposes, including public safety, border control, meeting social needs

[236] Furthermore, Google itself has been severely criticised by privacy advocates, therefore, this may further impact the results in that those most interested in privacy may choose a different search engine.
[237] House of Lords Constitution Committee, 2009, p. 5.
[238] House of Commons Home Affairs Select Committee, 2008.
[239] House of Lords Constitution Committee, 2009, pp. 5-16.
[240] Surveillance Studies Network, 2006, p. 1.
[241] House of Lords Constitution Committee, 2009, p. 5.

and maintaining public order. According to the House of Lords Constitution Committee, surveillance is also present "in the majority of commercial environments, such as shopping centres, supermarkets, stores, and banks [and]…has also become an inescapable aspect of life on the internet"[242]. While the SSN also notes that surveillance has "spilled" into "corporations, communications and even entertainment".[243] However, the House of Commons Home Affairs Select Committee notes that it is technological developments which have underpinned this sea change[244], which the House of Lords Constitution Committee has argued has created "formidable regulatory problems"[245].

Surveillance reduces trust while privacy enhances it

Trust has been positively associated with privacy in these documents and negatively associated with surveillance and other information collection processes by both public and private organisations. Furthermore, security is not often mentioned in relation to trust, however this is likely because the sample of UK documents analysed were primarily focused on surveillance rather than security.

According to the House of Commons Home Affairs Select Committee, "trust" refers to "confidence in and reliance on the capabilities and good faith of a person or organisation."[246] According to these documents, surveillance practices by the government, in particular, are associated with an erosion of trust, and that this erosion of trust could alter the relationship between citizens and the state. For example, the Surveillance Studies Network has argued that "all of today's surveillance processes and practices bespeak a world where we know we're not really trusted. Surveillance fosters suspicion" and that this can damage social relationships.[247] The House of Commons Home Affairs Select Committee explicitly links this lack of trust with the relationship between citizens and the state:

> Engaging in more surveillance undermines this assumption and erodes trust between citizen and state. In turn such an erosion of trust—with the citizen living under the assumption that he or she is not trusted by the state to behave within the law—may lead to a change in the reaction of the citizen and in his or her behaviour in interactions with other citizens and the Government.[248]

According to the same document, this could bring about a situation where further surveillance is necessary because citizens have withdrawn or reduced their level of cooperation with authorities.[249]

Instead, trust is linked positively with privacy and good data management practices, both in the private sector and in the public sector. In testimony to the Home Affairs Select Committee, a representative of Tesco, a large supermarket chain in the UK, argued that linking databases of customer information would "massively reduce that trust and, therefore, would not make the scheme effective", since the "scheme relies on customers trusting us".[250] The Committee followed this statement up by noting that:

[242] Ibid., p. 18
[243] Surveillance Studies Network, 2006, p. 6.
[244] House of Commons Home Affairs Select Committee, 2008.
[245] House of Lords Constitution Committee, 2009, p. 15.
[246] House of Commons Home Affairs Select Committee, 2008, p. 38.
[247] Surveillance Studies Network, 2006, p. 4.
[248] House of Commons Home Affairs Select Committee, 2008, p. 9.
[249] Ibid., p. 39.
[250] Ibid., p. 21.

> In the case of the private sector, several of our witnesses saw a direct link between trust and profit, which created a commercial imperative to protect personal information and privacy: losing the trust of customers would result in loss of revenue.[251]

These documents also constructed maintaining or building trust by protecting privacy or managing data appropriately as engendering particular benefits for government as well. According to the House of Lords Constitution Committee, the "Government have shown awareness of the need for privacy protection and the importance of maintaining public trust in other areas of surveillance and data use".[252] This can be built and maintained through better government transparency about data collection and use; however the Constitution Committee warn that simple compliance with the law may not engender and support trust, since many legal information gathering practise are viewed with suspicion by citizens.[253] It is only through privacy that public trust and the "social contract" between the citizen and the state can be supported and maintained:

> Privacy plays an important role in the social contract between citizen and state: to enjoy a private life is to act on the assumption that the state trusts the citizen to behave in a law-abiding and responsible way.[254]

Surveillance has negative impacts on human rights, democracy and ethics

Another key sub-storyline in the "surveillance society" discursive thread is the idea that surveillance technologies and practices can have negative effects on human rights (including privacy, data protection and discrimination) as well as democracy and ethics. These "risks" were primarily discussed by actors such as the Information Commissioner, the Surveillance Studies Network, academics, civil society organisation representatives and the Parliamentary Committees authoring the policy documents. According to the House of Commons Home Affairs Select Committee:

> The risks associated with the collection and use of personal information in databases in particular and the monitoring of individuals' behaviour in general, should not be underestimated. Mistakes or misuse of data can result in serious practical harm to individuals. Those less demonstrable risks which relate to the erosion of one's sense of privacy or individual liberty also have a practical aspect and a broad application in that they affect the way in which citizens interact with the state.[255]

Thus, citizens' privacy, individual liberties and relationship with the state can be undermined by surveillance practices that involve the collection and use of information as well as monitoring behaviour in general. However, according to the Surveillance Studies Network, although privacy and data protection are intended to protect against some of the effects of surveillance, the "surveillance society poses ethical and human rights dilemmas that transcend the realm of privacy".[256] While not intending to minimise the effects of surveillance on privacy, data protection and autonomy, the SSN points out that discrimination against particular groups is often a key outcome of the "social sorting" effects of surveillance.

[251] Ibid., p. 21.
[252] House of Lords Constitution Committee, 2009, p. 67.
[253] Ibid., p. 76.
[254] House of Commons Home Affairs Select Committee, 2008, p. 9.
[255] House of Commons Home Affairs Select Committee, 2008, p. 100.
[256] Surveillance Studies Network, 2006, p. 11

> Surveillance varies in intensity both geographically and in relation to social class, ethnicity and gender. Surveillance, privacy-invasion and privacy-protection differentiate between groups, advantaging some and, by the same token, disadvantaging others.[257]

This can lead to some groups being disadvantaged, for example, black youth in the UK being hugely over-represented in the National DNA Database.[258] Furthermore, some groups may find that surveillance technologies and practices "slow down" their lives and lead to inconvenience and hardship, rather than efficiency and personalisation.[259] Other data protection risks identified by the Information Commissioner include "mistaken identity; where there is false matching and the wrong individual is identified; where there is inaccurate or out-of-date information; where there are breaches of security".[260] Finally, surveillance technologies and practices may also negatively impact other ethical values such as "justice, dignity, self-determination, social inclusion, security, and others".[261]

Surveillance poses significant regulatory hurdles

This sub-storyline was primarily presented in the Surveillance Studies Network report and the House of Lords Constitution Committee report. This sub-storyline argues that surveillance is difficult for individuals and the state to regulate for four different reasons. First, according to the Surveillance Studies Network, it is difficult for individuals and the state to stay ahead of technology developments because ordinary people "do not have the time or the incentive to go in search of" details about "what happens to their personal information, who handles it, when and for what purpose".[262] They also assert that vast majority of individuals do not know their rights, do not know how to exercise them and do not know where to ask for help. Furthermore, regulators themselves are often "running behind technological innovation, unable to understand 'how it works'".[263] Second, although the Charter of Fundamental Rights of the European Union identifies a right to privacy, the UK itself does not have a constitutional privacy right. According to Hugh Tomlinson QC, this represents a "major legal obstacle".[264] Additionally, Article 8 of the CFREU allows limitations to the right to privacy "'in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'", which Professor Bert-Jaap Koops argues leaves a wide margin for interpretation by governments and other actors.[265] Third, different types of surveillance may be subject to different regulations or none at all. For example, the House of Lords Constitution Committee noted that in 2009, there was no "single legislative framework" that governed the National DNA Database and that better oversight was needed.[266] Similarly, civil society organisations such as Liberty and Justice were seriously concerned that "CCTV remains largely unregulated" in the UK.[267] Finally, the existing mechanisms to limit or regulate surveillance are thought to be too weak. For example, the Surveillance Studies Network and the Foundation for Information Policy Research have noted that the power of the Information Commissioner is restricted, and that increasing these

[257] Ibid., p. 6.
[258] House of Lords Constitution Committee, 2009, p. 45.
[259] Surveillance Studies Network, 2006.
[260] House of Commons Home Affairs Select Committee, 2008, p. 32.
[261] Surveillance Studies Network, 2006, p. 77.
[262] Ibid., p. 7.
[263] Ibid., p. 30.
[264] House of Lords Constitution Committee, 2009, p. 33.
[265] Quoted in House of Lords Constitution Committee, 2009, p. 32.
[266] House of Lords Constitution Committee, 2009, p. 49.
[267] Ibid., p. 51.

powers, and funding for the Information Commissioner's Office would help to regulate surveillance and information collection in the UK.[268] The House of Lords Constitution Committee also recommends requiring Parliament to consult with the Information Commissioner on relevant legislative changes or to establish a Joint Committee of both Houses that would specifically consider surveillance and data collection and processing issues.[269]

In order to prevent or address these effects, UK policy documents suggest two possible responses. One is to draft new legislation to provide better protections against surveillance, while another is to mandate that public and private organisations assess the risks to privacy, human rights and ethics before implementing a new surveillance system, possibly through a mechanism such as privacy impact assessment. According to the Joint Committee on Human Rights, the primary purpose of the Protection of Freedoms Bill is to "repeal or reform measures which the Government considers unduly restrictive of individual liberty or which interfere disproportionately with individual rights".[270] Thus, the UK government and the Parliamentary committee recognise that information collection and other monitoring practices do pose a "disproportionate interference" with privacy and other rights. However, the Joint Committee on Human Rights also warns that many of the measures introduced in the bill which are intended to provide additional safeguards, may result in new infringements on individuals rights. Thus, within the document the Committee raises "a number of concerns about specific measures which may not go far enough to ensure compliance with the UK's human rights obligations or may risk new infringements of individual rights".[271] As an alternative to specific legislative measures, many actors, including the Parliamentary committees suggest using a mechanism such as a privacy impact assessment (PIA) to address the specific risks to privacy, ethics and human rights potentially engendered by particular information collection or monitoring practices. The House of Lords Constitution Committee provides an example of such recommendations:

> We recommend that the Government amend the provisions of the Data Protection Act 1998 so as to make it mandatory for government departments to produce an independent, publicly available, full and detailed Privacy Impact Assessment (PIA) prior to the adoption of any new surveillance, data collection or processing scheme, including new arrangements for data sharing.[272]

Finally, the Surveillance Studies Network suggests another option, a Surveillance Impact Assessment, which would consider the social ramifications of surveillance technologies and practices, since one of the main drawbacks of privacy and PIAs is that they are focused on individual rights.[273]

This section has outlined the primary storylines and sub-storylines associated with the "surveillance society" discourse evident in UK policy documents. This storyline appears to be somewhat unique to the British policy context, and has been institutionalised through both the policy recommendations produced by these reports (some of which have been adopted) as well as the endurance of the discourse and the use of the "surveillance society" construction by different actors within the government. However, this discourse analysis is based on a

[268] Ibid.
[269] Ibid., p. 86-7.
[270] Joint Committee on Human Rights, 2011, p. 3.
[271] Ibid., p. 3.
[272] House of Lords Constitution Committee, 2009, p. 73.
[273] Surveillance Studies Network, p. 93.

small sample of UK policy documents and although it provides interesting insights into this discourse, the UK focus on "the surveillance society" may be over-emphasised based on the documents that were examined.

7.5.2 Finding a proportionate balance between security and privacy

All three of the legislative or government reports produced by the three Parliamentary committees discussed here utilised the notion of a balance between security and privacy to describe how these two concepts inter-related. Yet, it was not only these legislative bodies who mentioned finding a "proportionate balance" between privacy and security, other government actors also utilised this conceptualisation, including the Deputy Information Commissioner, the Home Office Minister for Security, Counterterrorism, Crime and Policing, the Department for Business, Enterprise and Regulatory Reform and the Chief Surveillance Commissioner. In these circumstances, human rights, and most especially the right to privacy the right to "respect for private life" remains relatively stable. However, these rights are balanced against multiple conceptualisations of security, ranging from traditional threats from terrorism through to protecting vulnerable groups.

These UK policy documents conceptualised traditional security threats in terms of national security, terrorism and fighting crime. For example, the House of Lords Joint Committee on Human Rights stated that there was a need to "strike a … proportionate balance between the rights of individuals to respect for their private lives and the wider interest in the prevention and detection of crime".[274] Similarly, in quoted testimony, the Home Office Minister for Security, Counterterrorism, Crime and Policing argued that there was a "'need to balance national security with human rights'" in relation to protecting the public from terrorism and "'serious crime'".[275] However, the Home Office Minister also affirmed that protecting privacy was fundamental to the work that their office carries out. Often, these documents mention proportionality or a proportionate balance by stating that the intrusions associated with serious crime would be justified while intrusions associated with minor crimes such as littering would not.[276]

Other actors within these documents described somewhat softer conceptualisations of security that included the need to protect the public, protect vulnerable groups and safeguard the community. While the Joint Committee on Human Rights reminds the government that the protection of human rights is a positive obligation, the document notes that the government has described the Protection of Freedoms Bill as an opportunity to assist in "rebalancing the Article 8 rights of individuals with the 'public' or 'general' interest in protecting vulnerable groups".[277] The House of Commons Home Affairs Select Committee similarly characterises the "potential" that private databases represent as a challenge to governments trying to balance "the right to individual privacy with the need to protect the public".[278] Finally, the Department for Business, Enterprise and Regulatory Reform discusses the issue of mainlining "the delicate balance between individual liberties and the safeguarding of the community in a democratic society".[279]

[274] Joint Committee on Human Rights, 2011, p. 45.
[275] Quoted in House of Lords Constitution Committee, 2009, p. 64
[276] House of Commons Home Affairs Select Committee, 2008.
[277] Joint Committee on Human Rights, 2011, p. 56.
[278] House of Commons Home Affairs Select Committee, 2008, p. 86.
[279] House of Lords Constitution Committee, 2009, p. 66.

Within this discursive stream there is also a storyline that refers to making sure surveillance measures are "necessary and proportionate" in reference to Article 8 of the Charter of Fundamental Rights of the European Union, which states that any interference with privacy must be necessary and proportionate. While this is not quite the same as balance, where taking from one side implies transferring to another, the use of the word proportionate links it to this discourse. However, it diverges from the balancing meta-discourse in that those advocating considering whether measures are "necessary and proportionate" are primarily academics or representatives of civil society organisations. Specifically, the Human Rights Policy Director for JUSTICE argued to the House of Lords Constitutional Committee that "Parliament might restrain the executive's enthusiasm for surveillance by 'refusing to pass disproportionate laws' and by scrutinising laws 'very closely in terms of their proportionality and, going back to the basic point, the necessity'" [280] Professor Graeme Laurie of the University of Edinburgh Law School also pressed law makers to ensure that the state demonstrated that the introduction of surveillance or security measures was "necessary and proportionate in particular circumstances".[281]

Like many other national contexts, these British policy documents primarily constructed the inter-relationship between privacy and security as one which requires "balance". The terms "balance", "fair balance" and "proportionate balance" appear frequently in the documents that are produced by Parliamentary committees and examined here. Furthermore, these phrases are attributable to a number of different types of government actors. However, it is worth noting that actors such as civil society organisations and academics foreground the UK responsibilities towards privacy in relation to the Charter of Fundamental Rights, and although they refer to "proportion" most of these actors appear to avoid using the term "balance".

7.5.3 Surveillance, security and their associated technologies have social benefits

Another thread running through the UK policy discourse on privacy and security is that surveillance, security and their associated technologies have clear social benefits. These benefits include better provision of national security, better protection from crime and economic benefits such as personalised or efficient services. While the Ministry of Defence National Security Strategy was at the forefront of identifying these potential benefits (particularly in relation to national security), the surveillance and human rights-focused policy documents produced by the Parliamentary committees also presented these arguments.

According to the Ministry of Defence *White Paper*, the use of surveillance and security technologies can contribute to better national security and thus, better protection of freedom. This includes providing military and other security actors with "operational advantage" that is gained through technological capability. "We need to provide our Armed Forces and national security agencies with the best capabilities we can afford, to enable them to protect the UK's security and to advance the UK's interests"[282] This can be accomplished through investment in technology. Importantly, the White Paper does not distinguish between traditional national security providers, i.e., the military, and other security agencies, such as law enforcement and the security sector. Instead, these different sectors are described as having a "common

[280] Ibid., p. 73.
[281] Ibid., p. 73.
[282] Ministry of Defence, 2012, p. 8.

interest" and some "common technology sub-systems".[283] This provision of national security also contributes to freedom, in that the "technology and services we need to defend our national security, so that people can go about their lives freely and with confidence".[284] Furthermore, technologies which protect cyberspace contribute to an Internet that "the UK public can use safely and that supports open societies".[285]

Surveillance and associated technologies, such as CCTV or DNA storage and processing, can also contribute to citizen security in terms of fighting crime, protecting public safety and reducing fear of crime. Those arguing that surveillance carries such public benefits were primarily government and policing representatives. According to the House of Lords Constitution Committee, accessing and processing personal information can assist to "fight crime and protect public security".[286] In relation to specific technologies, the Association of Chief Police Officers (ACPO) stated that "the availability of CCTV images greatly assists in the investigation of crime and disorder"[287], while the Prime Minister has argued, and various privacy civil society organisations have also recognised, that the National DNA Database is "'one of the most effective tools in fighting crime'"[288]. According to the Chair of the Local Government Association Safer Communities Board, CCTV is "popular" with members of the public and it enables them to "feel much safer".[289] Furthermore, the 10,000 CCTV cameras used by Transport for London are discussed by the organisation as key for "delivering a safe and secure environment for those who travel".[290] These assertions come despite the fact that the actual effectiveness of CCTV in fighting crime has been heavily criticised in various UK reports.[291]

Finally, surveillance and information collection practices also promise efficiency or other public service benefits for citizens. Public sector representatives who espoused this view focused on public services, while private sector representatives focused on consumer services; however in both respects, personalisation and choice emerged as key concepts. In relation to public services, the House of Lords Constitution Committee discusses information provided by "the Government" which argues that "[t]here is a need to gather and access personal information to support the delivery of personalised and better public services; [and] reduce the burden on business and the citizen".[292] The Prime Minster also argued that new information collection and linking systems will enable the government to share information across the public sector "responsibly, transparently but also swiftly" in order to "deliver personalised services for millions of people".[293] Citizens will particularly benefit through the removal of the need to "provide the same information many times over to separate government departments."[294] The Department for Children, Schools and Families has also argued that information sharing will enable the agency to "safeguarding children and

[283] Ibid., p. 36.
[284] Ibid., p. 6.
[285] Ibid., p. 48.
[286] House of Lords Constitution Committee, 2009, p. 20.
[287] Ibid., p. 21.
[288] Ibid., p. 44.
[289] Ibid., p. 20.
[290] Ibid., p. 21.
[291] See for example, Gill, Martin, and Angela Spriggs, *Assessing the impact of CCTV*, Home Office research study 292, February 2005 and Neville, Mike, Proposal – to extend VIDO units throughout the all 32 BOCU, Metropolitan Police, London, March 2009.
[292] House of Lords Constitution Committee, 2009, p. 20.
[293] Ibid., p. 24.
[294] Ibid., p. 24.

supporting the drive to personalise learning".[295] However, the House of Commons Home Affairs Select Committee cautions that these technological developments should be used to collect information accurately and used properly, including de-personalising data where appropriate.[296] The Home Affairs Select Committee Report, *A Surveillance Society*, also outlines the commercial benefits of information collection and sharing in the private sector to provide personalised services. According to the report, these systems can provide "competitive advantage" for companies seeking to "focus marketing and to design services"[297] and benefit consumers by providing an "impartial decision making process" and "a more appropriate and convenient service"[298]

This discourse outlines some of the drivers which are pushing the UK government and private entities to procure and implement further security and surveillance systems and technologies. The national security, crime fighting and economic benefits that these storylines argue could be captured by new systems may also factor into calculations about how far the UK should "balance" security against privacy. As the following, final, discourse demonstrates, the focus on economic benefits, in particular, is a key area of consideration for the UK government.

7.5.4 Supporting the UK security industry

Although this discourse was primarily present in just one of the policy documents from the UK that we subjected to discourse analysis, the linkages between the security industry and many western governments has been a subject of academic and civil society discussion for some time.[299] Furthermore, the interconnections between the security industry and the civilian market were briefly mentioned in the Surveillance Studies Network Report for the Information Commissioner's Office, which argued that there has been a shift towards military companies exploring the civilian market and creating innovative products that are no longer purely military of civilian".[300] In this "Supporting the UK security industry" discourse, the UK government primarily constructs itself as a platform from which the UK security industry can deliver economic gains for the UK and meet UK security needs. However, the Ministry of Defence notes that the government cannot support the UK security industry for the sake of it; instead the industry must provide good value for money and allow the government to take advantage of commercial developments.

According to a storyline within this discourse, the Ministry of Defence argues that the UK government and society relies upon the UK security industry to provide economic gains and exports, and that this should be supported by government policy. First, the approach to defence and security described in the white paper is characterised as providing "multiple opportunities" for the UK security industry, suggesting that the intention is to assist the industry to grow and compete.[301] In fact, the strategy notes that the UK domestic market for security technologies and products is worth approximately £1.8 billion annually, and that the UK security industry is well placed within the global security market.[302] The strategy specifically intends to support the UK defence and security industry in order to assist the

[295] House of Commons Home Affairs Select Committee, 2008, p. 30.
[296] Ibid., p. 100.
[297] Ibid., p. 16.
[298] Ibid., p. 20.
[299] For example, see Lyon, David, *Surveillance after 9/11*, Polity Press, Sussex, London, 2003 and Privacy International, "Big Brother Inc.", London, 2012. https://www.privacyinternational.org/projects/big-brother-inc
[300] Surveillance Studies Network, 2006, p. 14.
[301] Ministry of Defence, 2012, p. 17.
[302] Ibid., p. 7.

government in achieving "strong, sustainable, and balanced growth for the UK".[303] This is because the defence and security industries make a number of significant contributions. They maintain British defence and security capabilities, they contribute to "export-led growth and a re-balanced economy",[304] they are an "integral part of the UK's advanced manufacturing sector" and support "many highly-skilled jobs and vibrant supply chains".[305] As a result these companies "make a significant contribution to national prosperity" and UK defence policy seeks to complement UK economic policy by providing opportunities to support the British defence and security industry. The document even suggests that the strategy could be used to promote a "UK Security Brand" that leverages the UK's experience in security issues like counter-terrorism and policing and create further economic advantage for the UK.[306]

However, the *White Paper* also argues that technologies must provide good value for money, and that the government would not support UK security industries without achieving economic efficiency. Thus, the Ministry of Defence states that the goal of the security strategy is to obtain "the best products and services at the lowest possible cost to the taxpayer"[307] that does not undermine "our national sovereignty, […] operational advantages and freedom of action that we judge to be essential to our national security"[308]. This can partly be accomplished by taking better advantage of commercial developments. The White Paper argues that while military technology development used to be "the realm of Government research organisations, [it] is now carried out almost exclusively in the civil and commercial sectors".[309] In a reversal of the SSN characterisation of the military sector infiltrating the civil market, the Ministry of Defence sees to ensure that they "make full use of technologies developed for civilian applications and invest in the development of defence and security uses for them".[310] This will reduce costs and promote private investment in research and development of new technologies.

The contextualisation of the UK government as a supporter of the security industry may be somewhat dependent upon the history of the UK in terms of responding to threats such as those from the IRA and Islamic fundamentalists. This may have encouraged the government to invest in defence and security research as well as to foreground the economics of security in providing national security. Significantly, this discourse has recently expanded from providing national security through military capabilities, to include providing internal security by actors such as police, intelligence agencies and other security providers (i.e., private security firms). Furthermore, the availability of advanced technology has also extended from being the sole provenance of military researchers, to the government seeking to take advantage of innovations in the private sector as well. This suggests a blurring between civil and military spheres within the UK that might further influence the discourses utilised by policy-makers in this context.

[303] Ibid., p. 8.
[304] Ibid., p.9.
[305] Ibid., p. 17.
[306] Ibid., p. 55.
[307] Ibid., p. 13.
[308] Ibid., p. 30.
[309] Ibid., p. 38.
[310] Ibid., p. 39.

7.6 GENERAL CONCLUSIONS, REFLECTIONS AND HYPOTHESES

Overall, these security and privacy discourses demonstrate that UK policy surrounding security and privacy is a complex and contested terrain. Some discourses and actors appear highly critical of the current policy regime. For example, the "Surveillance society" discourse clearly argues that current policies fail to adequately consider the privacy, human rights and ethical implications of current surveillance and security technologies and practices. In contrast, the "Benefits" and "Supporting the security industry" discourses argue for an expansion of security and surveillance technologies and practices in order to bring better national security, public protection and economic gains. Finally, the "Balance" discourse appears to argue that some security gains can be captured as long as they do not disproportionately interfere with privacy. Furthermore, different actors appear to be aligned with these discourses, in that government actors, by and large, seek to capture the benefits of security technologies and balance these against privacy, while academic and civil society representatives support foregrounding privacy and human rights considerations, possibly at the expense of new surveillance and security programmes.

In relation to other countries or contexts, the UK seems to share the idea that security and privacy are incompatible concepts that must be balanced against one another. However, it appears that only particular actors within the UK context support such a notion. The idea of balance was primarily espoused by actors from the government, including Ministers, Members of Parliament and police officials. In contrast, although some civil society organisations and academics referred to "proportion", these actors as well as academics from the Surveillance Studies Network were not represented in these documents as supporting the idea that these two concepts must be balanced. This suggests that different policy actors have different conceptualisations of security and privacy that influence how they feel that government policy should respond.

However, the UK appears to diverge from other contexts in relation to three other security and privacy discourses. First, unlike other contexts British policy-makers appear to be heavily influenced by innovations in surveillance technologies and practices and foreground discussions of surveillance activities rather than security activities. Although this may be related to pressures from specific entities within the UK or a temporary spike in interest that is due to fade, it does seem apparent that the UK is more concerned with surveillance than other European countries. Second, the UK government and other policy-makers are highly interested in capturing the economic and other benefits that security, surveillance and information collection technologies and practices can bring in terms of national security, fighting crime, public safety and efficiency. In particular, UK discourse on security highlights the benefits for the UK economy as a whole in supporting the domestic security industry, and highlights the benefits that citizens might enjoy through efficient and personalised services.

8 PRIVACY AND SECURITY DISCOURSES IN SELECTED DUTCH POLICY DOCUMENTS

8.1 INTRODUCTION

The framing of security and privacy by media and politicians in the Netherlands has been highly influenced by various critical events. In the aftermath of 9/11 and the Theo van Gogh assassination for instance, strong statements have been made about (the balance between) security and privacy in political debates and media. In addition, some chains of events – such as several privacy violations by commercial websites – have had a profound impact on the security and privacy debates. In this document these (chains of) events and the subsequent security and privacy debates are described and reflected upon. For each critical period in time, the key metaphors, story lines (i.e. lines of reasoning), discourse coalitions (i.e. actors who share a certain opinion) and institutionalization (i.e. translation of opinions into e.g. rules and practices) are set out (see section 14.4). First however, the tables used for empirical data collection, the key actors involved in the security and privacy debate and the public attention to these notions are presented (respectively section 14.1 to 3). This, in order to provide an overview and sketch the context of the discourses. The document will conclude with a general reflection upon the discourse and hypotheses which provide input for the survey of PRISMS' Work Package 8 (section 14.5) and an overview of the literature and documents studied (section 14.6).

8.1.1 Methodology

For each critical event, leading newspaper articles, parliamentary and policy documents have been studied. Subsequently, (a) frequently used terms, (b) key storylines (lines of reasoning) and (c) all types of actions taken upon the debate (institutionalization) have been collected and structured within tables. In choosing to extract these three aspects from the discourses, we followed the discourse analysis methodology of Hajer[311]. By studying these three aspects the precise framing of the security and privacy concepts, the argumentation used and the extent to which the discourses have had an impact in terms of e.g. new rules, policies and organisations will be revealed. Hajer uses a rather broad definition of the term 'insitutionalisation' as he not only understands the drafting of new rules and establishing of new organisations as 'institutionalisation', but also includes new policies and other actions taken upon specific debates[312]. For a more elaborate description of the methodology, see chapter 13 of this report.

[311] E.g. Hajer, 2005, 2006a, 2006b.
[312] See for example Hajer, 2006b, p. 70.

8.2 KEY DISCOURSES

The key discourses identified are, in chronological order: the 9/11 terrorist attacks; the Theo van Gogh assassination in (2004); Critical reports of key Dutch public institutions (2006-2008); and Security meets privacy (2009 to date). First findings are presented in the four tables below.

9/11[313]

Terms	Key storylines	Institutionalization
• Counterterrorism • Terrorist attack • Attack on 'the Western states' • Attack on democratic constitutional state • Solidarity with US • Fight between terrorism and democracy • New terrorism, new war modes • The start of a whole series of terrorist attacks • Culture clash • Antrax, biological weapons • Radicalization • Liberation 1945 by US	Security • The attack on the US is an attack on all western states • Netherlands should express their solidarity with the US and support them in their fight against terrorism. The US and other allies have liberated the Netherlands in 1945 • The policy should exist of international cooperation, and the key goal is to protect democracy in solidarity with US • The new type of terrorism is characterized by extreme violent behavior, which aims at making as much victims as possible while using modern technologies. • The terrorist attacks in the US are in fact a direct attack on 'Western Democracies' and the democratic rights. • Europe should take all efforts and use all instruments to find the people responsible for these attacks • The term war in Article 5 NATO Treaty should be interpreted in a broad sense and capture war of terror • The New York attack is just the beginning of a series of attacks and the Netherlands could also be target. Privacy	• National Coordinator for Counterterrorism and Security • Ministry of Security and Justice • CT Infobox • Expansion of intelligence services • Quick response team • 'Dreigingsbeeld Terrorisme Nederland' • Harmonization visa policy • Increased protection vital infrastructures of government and industries • Increased border control • Enforced surveillance airports • Expansion intelligence and analysis capacity terrorism • Development of biometric identification technologies • Expansion capacity bodyguards • More capabilities to analyse international telephone conversations

[313] The tables in this section of the report are based on the analysis of several parliamentary documents and news reports. For this table the following documents have been studied: TK, 2001-2002, 27925, nr.5, TK, 2001-2002, 27925, nr.6, TK, 2001-2002, 27925, nr.10, TK, 2001-2002, 27925, nr.11, TK, 2001-2002, 27925, nr.19 and TK, 2001-2002, 27925, nr.26. For a complete list of documents studies see paragraph 6.

Terms	Key storylines	Institutionalization
allies • Sacrificing privacy for safety • Privacy is over-protected • The privacy and security dilemma (trade off concept)	• D66 (social-democrat party) in 9/11 debate: "We find it important that all passengers will be thoroughly examined, as this increases security. The sacrifice we all have to make will be increased queue times and possibly we also have to take privacy infringements for granted." • CDA (Christian-democrat party) in 9/11 debate: "The CDA already stated that the freedom of the individual [red: e.g. privacy] cannot be at the expense of security of the society. This starting point – according to us - also concerns internet, financial investigations, body searches and the telephone taps." • SGP (ultra conservative Christian party) in 9/11 debate: "The question is whether current legislation sufficiently covers new technological possibilities and whether we have not over-protected privacy" • GroenLinks (the greens) in 9/11 debate: "Measures have to be taken. We also realize that this [measures] can have consequences for privacy and the balance between security and privacy. Also my party of course is willing to reorient on this"	• Expansion satellite interception capacity • Increased inspection of legislation concerning identification, financial services and exceptional transactions • Allerteringssysteem Terrorismebestrijding (ATb) (Alert System Anti-Terrorism) • De Wet terroristische misdrijven (terrorist crimes law) • De Wet afgeschermde getuigen (witness protections law) • Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven (law extending police powers) • Wetsvoorstel bestuurlijke maatregelen nationale veiligheid (legislative proposal: administrative measures for national security) • Expansion legislation on telephone taps

Theo van Gogh assassination, 2004

Terms	Key storylines	Institutionalization
• Jihad in the Oosterpark • Terrorist attack • The Netherlands at war • Radicalisation • Fundamentalism • Muslim terrorism • Radical mosques • Breeding grounds for	• VVD (conservative-liberal party): "The fight against terrorism is a fight for the preservation of democracy and human rights. The VVD misses the sense of urgency in the measures taken by the Cabinet in the wake of 9/11. Not only questions the VVD the progress being made but also the effectiveness of the measures to prevent a terrorist attack. The by the cabinet announced measures are inevitable and necessary. [..] The measures of preventative body search are not extensive enough. […] at the airport this should be a permanent measure [and not limited to	• NCTb, Joustra • Enforced control of specific persons • Evaluation of the security organization • Alerting system • Contra terrorisme info box, cooperation between AIVD, Police, OK, IND and MIVD • New anti-terrorism legislation • Etc.

Terms	Key storylines	Institutionalization
terrorism • Better safe than sorry • Mohammed B. • Hirshi Ali • Submission • Fear and confusion • Freedom of Speech • Body guards • Radical Imams • Muslims • Burka	arriving and departing people]. […] The implementation of measures concerning the financing of terrorism is much too slow." • D66 (social-democrat party): "D66 is glad to notice that top politicians finally seem to feel a sense of urgency as regards the threat of a terrorist attack in the Netherlands. […] A clear commando structure is however missing. […] d66 thinks it to be a good idea to intensively track and trace people who are preparing terrorist attacks. D66 awaits the expansion of criminal law, but expects this to be within the constitutional framework. D66 takes remarks of the CBP seriously. Is disappointed that project Vitaal has not been delivered yet. • CDA (Christian-democrat party): "We should act now. Which means that we should not be too occupied with and concerned about legal [Privacy] issues. The right to privacy is subordinate to the security of society. [Measures] concern camera surveillance, a longer retention period of video material, […]" • PvdA (labour party): "The constitutional state nor the protection of freedom of citizens [Privacy] is in conflict with the enforcement of police and the judiciary when this enforcement is needed. The constitutional state is a safe state in which government ensures the protection [security] of the citizen. […] • Groenlinks (the greens): "Measures should be taken to deal with the terrorist threats effectively. However shocked by […] the terminology [Netherlands is at war] and concerned about the expansion of powers [security] and privacy infringements. Afraid this will lead to stigmatizing groups of people" • SGP (ultra-conservative Christian party): citing Scheffer: " the underestimation of terrorism in name of the Islam is a greater threat to an open society than limitations to privacy."	

Critical reports of key Dutch public institutions, 2006-2008

Terms	Key storylines	Institutionalization
• No new security metaphors (same as after 9/11 Van Gogh assassination, e.g. terrorism, fundamentalism) • Internet and privacy • Data protection	• GroenLinks (the greens): '[Minister] do you know the research of Privacy International and Electronic Privacy Information Center, which shows that in the Netherlands privacy is less protected than in other countries? Do you share the opinion of the researchers that in the Netherlands the privacy protection systematically fails?[…]' • Minister Hirsch Ballin, 17 November 2006 "The in the research mentioned (Dutch) competences, such as telephone and internet taps and the exchange of personal data, are compliant with the EVRM, European case law and article 10 of the constitution.[…] These competences are necessary in a democratic society. The competences aim to contribute to the national security, which complies with the in article8, clause 2 of the EVRM mentioned goal criterion. […] In other countries, such as Germany and Belgium, elements of legislation have also been modified because of counter terrorism measures.[…] I do not see any reason to take measures [to strengthen privacy]." • D66 (social-democrat party): About research of Rathenau Institute: "[Minister], do you agree that CBP (the Dutch Data Protection Authority) should have more possibilities to sanction in case of privacy infringements?[…] Do you agree with the statement of Rathenau that the whole of security measures fails to be discussed in a public debate? Do you share the concerns and agree that it is time for a fundamental debate about the emerging technologies and privacy[…]?" • Minister Hirsch Ballin, 31 May, 2007: "There are different views as regards the question whether the CBP has sufficient or insufficient possibilities for sanctioning. […] The first evaluation of the WBP (Dutch data protection law) is currently being conducted.[..] The society is confronted with increased digitalization and internationalization. […]There is […] a reason to the question whether and how the privacy policy needs a new impulse." [turning point in debate] • Proposal D66 (social-democrat party), 11 June 2008 D66 asks the	• Commission Brouwer Korf established

Terms	Key storylines	Institutionalization
	government to develop an integral vision on privacy in the 21st century • Proposal PvdA (labour party), 24 November, 2008: "[…] finding that many commercial websites still collect personal data of children without verifying whether the children have the approval [of their parents]. […]requests the government to conduct research on the bottlenecks of the CBP directives and to examine whether it would be possible to develop Dutch legislation conform the American COPPA (Children's Online Privacy Protection Act)"	

Security meets privacy, 2009-present

Terms	Key storylines	Institutionalization
• Cybersecurity • Wikileaks • Cyber war • Cybercrime • Skimming • Internet fraud • Veilig Internetten • Dorifelvirus • Security and privacy mentioned as matching values instead of rival values • Registrations • Social network sites • Facebook • LinkedIn • Deep packet inspection • Privacy, children and the Internet	• Parliamentary questions SP (socialist party), 27 August 2010 "Are you acquainted with the news report on the exponential growth of cybercrime in the Netherlands? How many incidents of cybercrime are there on a yearly basis? […]" • Answer minister Hirsch Ballin, 7 October 2010 "The news item […] is based on a chapter of the high tech crime report "Overall beeld aandachtsgebieden" of the deparment National Investigations. In addition to the observation in this report that over the past few years an exponential growth of cybercrime and high tech crime can be discerned, remarks have been made that these observations have been based on the statistics available on sub aspects of cybercrime" • Parliamentary questions, PvdA (labour party), 27 October, 2010 "Have you seen the Nieuwsuur TV programme on cybercrime? Do you agree with the interviewees, among which a public prosecutor specialised in cybercrime, that the powers of the police and justice department should be extended as regards cybercrime, more specifically the possibility to "re-hack", irrespective of the location of the computer? " • Parliamentary questions VVD, 7 january 2011 "Have you read the article "Dutch companies target of cyberattacks"? Are you aware of the fact that the Netherlands is among the countries with the most ICT security	• national cyber security strategy • the Cyber Security Board (Cyber Security Raad) • Information Point Cybercrime, • Directive on baseline information security for the national government • the National Cyber Security Centrum (NCS) • Cookie legislation • Revised telecommunication legislation • Proposed revision of the Dutch data protection law •

Terms	Key storylines	Institutionalization
• Privacy and data claims by policy and public prosecutor	incidents within the European Union and that Dutch companies are often victims?" • Parliamentary questions (PVV)"Are you aware of the news report "Browser developers release new version after Diginotar failure"? What are the consequences for the use of DigiD […]?" • Parliamentary questions (PvdA), 11 August 2011 "Are you aware of the fact that Facebook – through the special Facebook application for smartphones – automatically synchronizes the contact persons form telephone lists and friends and that consequently telephone numbers of Facebook friends automatically appear on someone's Facebook page?" • Answer Minister Opstelten: "[…] According to Facebook only the user him/herself has access to the list of imported contacts and this information is used by Facebook to make suggestions for new friends to the users and others. Via www.facebook.com a user can delete the imported contact persons […] The CBP is an independent supervisor and can in case of data protection law violation enforce the law. It is not my duty to decide in an individual case whether the requirements of the WBP (Dutch data protection law) are being met" • Parliamentary questions D66 (social-democrat party), 17 August, 2011"Are you aware of the article "Companies neglect privacy legislation? Do you share the observation being set out in this article, that companies should provide [users] access [to personal data] but that they rarely do so?" • Parliamentary questions, D66 (social-democrat party), 4 October 2011 "Did you read the article "Call for investigation use of cookies by Facebook"? What is your opinion on the collecting of privacy-sensitive information by Facebook by using undeletable cookies?" • Answer Minister Verhagen"[…] the CBP decides in individual cases whether the Wbp (Dutch data protection law) is violated." • Proposal Elissen en Gesthuizen"[…] requests the government in case of the development of all new government ICTs to apply privacy by design and safety by design so that new ICT systems are more secure and	

Terms	Key storylines	Institutionalization
	better equipped against abuse and only then contain privacy sensitive data if this is strictly necessary ” • Proposal Gesthuizen and Verhoven, 27 October 2011 “finding all recent problems concerning privacy, security and the protection of citizens online, makes clear that the Netherlands should take necessary steps as regards ICT security[…] requests the government to inform the Parliament in the first quarter of 2012 about her vision and measures in these areas” [privacy and security mentioned as matching instead of rival values] • Proposal Peters, 20 November 2011 “[…] requests the government to advocate sanctions against Iran and Syria as regards technologies which can be used to violate privacy and freedom of speech.” • Parliamentary questions GroenLinks, 17 November 2011 “Are you acquainted with the news reports concerning the rulling of the court of the American state Virginia that private data of three twitter users can be used in the Wikileaks investigation?[…] To what extend does the cyber security strategy pay attention to the protection of the legal status and privacy of users?”	

8.3 KEY ACTORS AND WORD COMBINATIONS

In the Netherlands, several key actors have been involved in the security and privacy discourse. The debates on these issues were most outspoken in the aftermath of critical events (e.g. 9/11 and Theo van Gogh assassination) in the media (e.g. opinion pages) and in parliamentary debates. It seems that through these platforms (both media and parliament) the tension between security and privacy became most clear and that here the two concepts were attributed meaning. The framing of security and privacy in the media and politics resulted in specific policies of various ministries which applied similar understandings of the notions (i.e. reproduction). In the Netherlands, the data protection authority CBP played a limited role in the discourse. The reason for this may be the relatively limited independence enjoyed by the CBP compared to similar authorities in other EU countries, or just a desire to preserve its independent position by not engaging in public debate. The first supposition could be supported by the fact that the CBP is funded by the Ministry of the Interior and one of the key tasks of the CBP is to support ministries in policymaking and drafting of legislation (for a more elaborate explanation of their tasks, see www.cbpweb.nl). Since the publication of the report of the Commission 'Security and Private Sphere', the limited independence of the CBP has been a subject for discussion. In any case, from the Dutch documents studied the following actor network picture emerges providing an overview of key actors involved in the Dutch privacy-security discourse:

Figure 1:Key actors involved in the Dutch privacy-security discourse

8.4 PUBLIC INTEREST

The extent to which citizens have been occupied with the subjects of security and privacy (i.e. the public attention) can be inferred from the frequency with which citizens have searched for information about the subject on the Internet. When citizens are concerned about a particular issue they – more often than not – will try to find online more information about that issue (e.g. in case of a certain disease, but also a threat or scandal). As the large majority of users

use Google as their primary search engine[314], statistics about the frequency with which users searched for specific information through the Google search engine can provide some indication about the extent to which subjects were important to users. The following tables show the frequency of specific Internet searches over the past seven years.

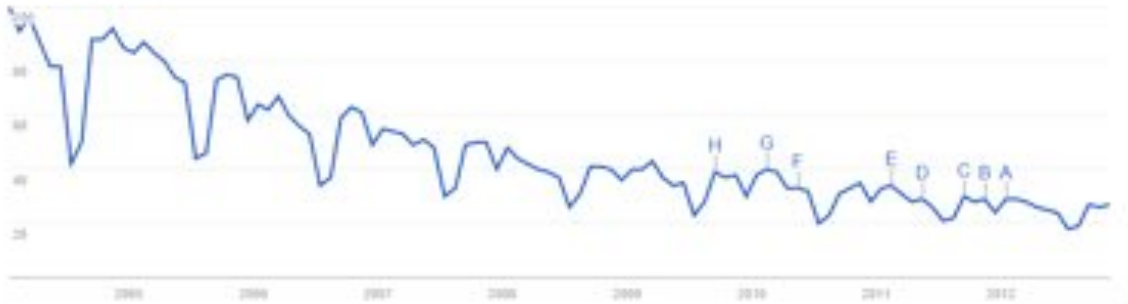

Figure 2, The frequency of the term 'veiligheid' (security) entered by Dutch users into the Google search engine (2005-present).

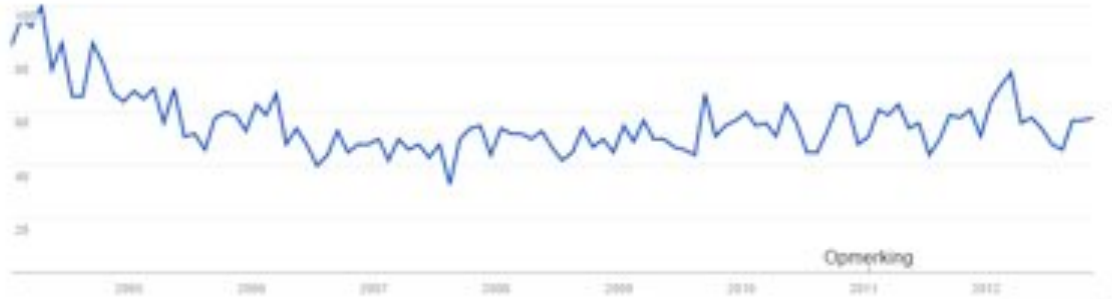

Figure 3: The frequency of the term 'privacy' entered by Dutch users into the Google search engine (2005-present)

As the two tables above indicate, the interest in the 'security' subject among users seem to have declined during the past seven years, whilst the interest in the 'privacy' subject among users seem to have declined from 2005 to 2008 and then slightly increased. This seems to be consistent with the extent to which these subjects have received attention in the Dutch parliament.

When looking at searches on both the terms 'privacy' and 'security' in the table below, it seems that whereas up till 2008 this combination of words was not searched for, since 2008 users increasingly entered the word combination into the Google search engine. This may substantiate our research finding yielding from the parliamentary debates, that over the years these terms have been increasingly understood as matching instead of contradictory notions; another possible explanation is that over the years more security issues have had privacy connotations in which case the two concepts would emerge as contradictory rather than matching.

[314] According to Statowl, in June 2012 Google had 81,1% of the market share http://www.statowl.com/search_engine_market_share.php

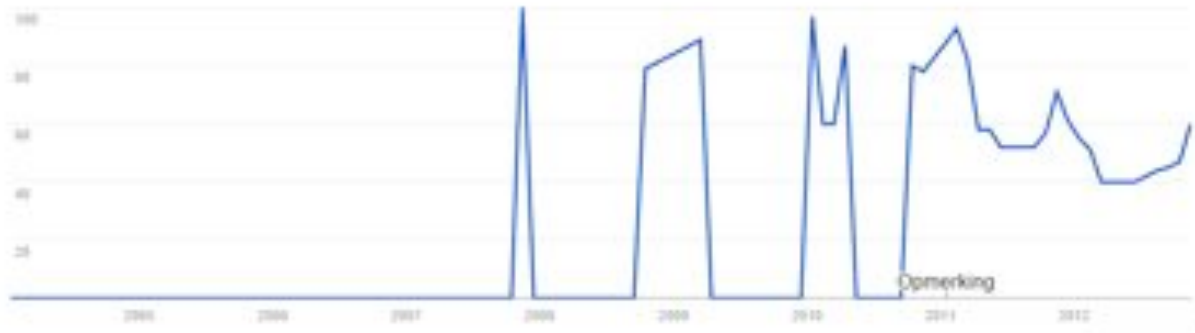

Figure 4: The frequency of the terms 'privacy' and 'veiligheid' (security) entered together by Dutch users into the Google search engine (2005-present)

8.4.1 Description of critical events and the security and privacy discourse

This paragraph provides a narrative description of the Dutch security and privacy discourse over the past decade. As various critical (chains of) events seem to have had a profound impact on the discourse, the discourse will be described within the context of these events. Based upon the terms, storylines and institutionalization as depicted in the tables of paragraph 1 and an additional reading of key news articles, the context of the discourse and the discourse itself are being described for each critical event.

9/11

The first critical event which substantially influenced the Dutch privacy and security discourse over more than a decade were the September 2011 attacks upon the U.S. in New York City and Washington DC. The main Dutch radio and television news stations (e.g. Nederland 1, RTL4 Nieuws, Radio1, BNR) had a full media coverage on the day of the attacks. The next day, headlines of the three important Dutch newspapers read "*Attack on the U.S., Bush wants retaliation*" (NRC), "*Bush promises revenge for attack*" (Volkskrant) and "*U.S. at war*" (Telegraaf), which articles demonstrated strong emotions of shock and provided an overview of the course of events and the reactions of (amongst others) president Bush and the then Dutch prime minister Kok. In the days after the attack, most Dutch newspapers and television stations provided chronological accounts of the event (some minute to minute), made estimations of the number of victims and discussed the possible perpetrator Bin Laden. False incidents of planes allegedly off the radar of European or U.S. control towers (e.g. the so-called "missing" plane of the president of Cyprus) were headlined. Television stations recurrently showed the image of the planes hitting the WTC. All news providers interpreted the event as an attack on the symbol of capitalism and the power of the U.S. In the aftermath of the attack, news coverage focused on personal (tragic or heroic) stories (e.g. of firemen who tried to rescue people from the WTC building), the exact number of victims, the identity and motivations of the perpetrators (mostly stated to be Islamic fundamentalism), evidence against Bin Laden and repercussions of the US (and allies) against the 'terror network of Bin Laden' (used as shorthand for the Taliban, the Islamic fundamentalist movement). In addition, news stories emerged on new types of (nuclear, chemical and biological) weapons (e.g. Antrax) and 'bio-terrorism' such as the deliberate infection of people with all kind of viruses (e.g. Ebola virus) and possible new attacks (e.g. on president Bush, road tunnels outside Amsterdam and Rotterdam). Any accident which might even remotely have been caused by a terrorist act was headlined, extensively elaborated upon and linked to 9/11 (e.g. the Airbus crash near JFK airport New York, November 2001).

In politics, the 9/11 attack evoked intense emotions among Dutch politicians. In their first reactions, Dutch politicians showed strong feelings of abhorrence. In his press conference just after the attacks, the then Dutch prime minister Kok stressed the importance of respecting human rights in the case of a repercussion. In a press conference he stated:[315] *"Powell said […] that if there will be ever a moment when one - who highly values democratic rights - has to know what he stands for, this will be it. And I find this stance of the Minister extremely strong and I think we have to achieve this together. [Reporter: Has it been an attack on the Western democratic system?] It has been a direct hit to the core of the U.S. […] I generally call to use common sense and to find the balance which will be needed the coming period. [Reporter: what will be the greatest threat] The greatest threat lies in the possible continuation of forms of terrorism. Today [eds. 's attacks have] has shown that the […] use of the weapon 'terrorism' can hit many vital targets at the same time. And the fight against terrorism is the foremost task. At the same time, we will have to try, however difficult this message will be - especially today, to – with even more power - maintain democracy and the respect of human rights. And I say this precisely today, now that others with their nasty means – with their inhuman means have violated every notion of respect for human rights. [Reporter: what will be a suitable reaction to this?] To think this thoroughly through. [Reporter: have you ever thought of such a scenario?]. I would rather not speak of a scenario, but what has happened today is beyond words and inconceivable. Anyone who yesterday would have predicted that this would happen, would have been called mentally ill. And still it happened. And this warns us that we should be prepared for the worse and that we should demonstrate determination, to show power just now with each other. Also mental power.*"

In the Dutch parliamentary debate about the 9/11 attacks[316], the majority of parties started with strong condemnation of the attacks and showing their compassion for the American people. There was a broad agreement among parties that the attack on the US should be understood as an attack on 'Western democracies' in general and that the Netherlands should express solidarity with the US in their fight against terrorism. Parties stated that the attack on the US was an attack on democratic rights, such as freedom of speech. Some parties stated that also the Dutch were hit by the attack. Both the parties in office (the Labour party PvdA, the conservative-liberal party VVD and the social-democrats D66) and opposition parties contended that the 9/11 attacks could be perceived as a new form of terrorism in terms of impact (hitting central targets) and strategy (e.g. new type of 'weapons') and that defence strategies and policies should be changed in response to this new form of terrorism. The large majority of parties expressed their feeling that the Netherlands could also be a potential target and/or that this form of terrorism also could be a serious threat for the Netherlands. Several politicians stated that the attacks "have shown the vulnerability of modern societies". Parties disagreed about and questioned the way in which the Netherlands should demonstrate their solidarity with the US and how they should translate this into tangible support. This contradiction and unanswered questions became apparent in the discussion on the content and the scope of article 5 of the Washington Treaty[317] on collaborative military action. Whereas several (predominantly right wing, but also PvdA) parties stated that article 5 could provide a basis for a possible military support of the US, other parties (e.g. the Socialist Party SP) found the application of article 5 unwise as the Netherlands consequently would be involved in (possible disproportional) repercussions conducted by the US. Both SP and Groenlinks (the

[315] Underlined words were strongly emphasized by the Dutch prime minister.
[316] TK, 2001-2002, 27925, No 6.
[317] http://www.nato.int/cps/en/natolive/57772.htm

Greens) expressed their fear of an international 'spiral of violence' and stressed the importance of respecting human rights in the response to the attacks.

Following this debate and meetings between ministers, the cabinet proposed extensive national security measures to be implemented, which were then discussed in parliament. Examples were the increased cooperation with relevant European intelligence agencies, enhancement of the Dutch intelligence services, the development of biometrical identification techniques, establishing a harmonized European visa policy, increased control of mobile telephone communications and legal basis for telephone taps. Although privacy was not frequently mentioned during parliamentary debates on these measures, in some instances politicians referred to the balance between privacy and security. D66 for instance stated in a meeting on countermeasures against terrorism [318] "*My party has great worries about the security of Schiphol. […]. We find it important that all passengers be thoroughly checked, as this enhances security. The sacrifice we all have to make will be longer queue times and possibly also having to take privacy infringements for granted*." In the same debate D66 stated: "[…] *Sometimes one reads about Amsterdam, weapon depots, IRA, etc. On the Internet I found the measures taken by the German government. I mention the Rasterfahndung [drag nets], the linking of data which ignores all privacy aspects in order to detect the financial activities of criminals. In Germany, religious unions have been deprived of legal protection. In addition I read that all kinds of fundraising activities are forbidden or will be forbidden there [in Germany]. I do not mention this to ask the government to do the same, but I would like to know if all measures which we have taken following the Van Traa inquiry […] are applicable to these kind of terrorist organisations*."[319]

Other statements made by parties during this debate[320] which were related to privacy were for instance (the Christian Democrats, CDA): "*The CDA already stated that the freedom of the individual [eds. e.g. privacy] cannot be at the expense of security of the society. This starting point – according to us – also concerns internet, financial investigations, body searches and telephone taps*". And the SGP: "*The question is whether current legislation sufficiently covers new technological possibilities and whether we have not over-protected privacy*". GroenLinks: "*Measures have to be taken. We [GroenLinks] also realize that these [measures] can have consequences for privacy and the balance between security and privacy. Also my party is willing to reconsider their position on this*". Deputy minister de Vries (VVD) stated in a newspaper interview in Trouw, 16 October 2001: "*The balance between privacy of citizens and the tracing by police and intelligence agencies has tipped over to privacy. Currently citizens are victims of privacy legislation more than they are protected by these regulations*". And minister Korthals of VVD[321] in reaction to parliamentary questions about the statement of deputy minister de Vries: "*This [her statement on the balance between privacy and security] concerned in particular the retention period of data and so forth. We found that this [the retention period] should be extended. This is also what the [telecom] industry wants. For that matter, interests could – in the advantage of criminal investigations – match*".

When considering various Dutch security and privacy debates in the aftermath of 9/11 it appears that some key metaphors have been used by politicians and newspapers. The most

[318] TK, 2001-2002, 27925, No 19.
[319] In 1996, Van Traa (Dutch politician of the labour party PvdA) led the parliamentary inquiry into criminal investigation methods.
[320] TK, 2001-2002, 27925, No 19.
[321] Ibid.

important ones might be '*Bin Laden*' and '*the war on terror'*, of which the first personifies the general fear among politicians, journalists and the Dutch citizens of attacks by fundamental Islamic groups and the second shows the determination of the US and (in its slipstream) other countries to take all measures possible to combat terrorism. The omnipresence and intensity of the fear of terror in the aftermath of 9/11 is demonstrated by several articles reporting on incidents which the media immediately linked to the attacks (e.g. missing plane of president Cyprus, accident with Airbus near JFK) and extensively elaborated upon, but which eventually turned out to be unrelated events. Also the broad attention to all kind of other possible (nuclear, chemical, biological) weapons, potential targets and perpetrators express the general fear of attacks. The decisiveness of the Dutch government to fight terror becomes apparent seeing the numerous measures taken by the Dutch government to fight terrorism and the substantial increase of security budgets. Some of the measures were for example: the establishing of a National Coordinator for Counterterrorism and Security, the installation of a quick response team, the expansion of capacities of intelligence and security services, expansion of the possibilities to intercept and analyse international telephone conversations, increased border control, enforced surveillance at Dutch airports and the counterterrorism alert system.

When specifically looking at privacy, the limited number of political debates in which the notion privacy is mentioned is significant (e.g. when comparing it with the number of debates in which privacy was mentioned in 2011). When privacy is mentioned in 2001, the great majority of politicians explicitly state security to be of more importance than privacy. Most parties contended that they were willing to accept privacy limitations for the sake of security. The statements made by politicians reveal that they perceived the privacy and security balance to be a trade-off concept; more security necessarily implies less privacy and vice versa. Although prime minister Kok mentioned human rights to be of crucial importance in dealing with 9/11 (during a press conference on 9/11), the human right 'privacy' seems not to have received much consideration during the discussion on the security measures to be taken.

Theo van Gogh assassination

The second event which had a decisive impact on the security and privacy discourse in media and politics was the assassination of Dutch film director Theo van Gogh in 2004. The number of articles in the media and the intensity of Parliamentary debates reveal that the killing of Theo van Gogh had more impact on the security and privacy debate in the Netherlands than the bombings in Madrid (11 March 2004) and London (7 July 2005). The Dutch film director, author and television personality Theo van Gogh, was murdered by Mohammed B. on 2 November 2004. News stations had a full media coverage on the day of the murder. Several newsreels (e.g. Netwerk) invited prominent intellectuals to discuss the event, some of whom made strong statements on Muslims and the Islam. Bart Jan Spruyt – Dutch historian, journalist and right-wing conservative thinker - for instance stated in Netwerk "*This is not the work of one disturbed person. It yields from a certain culture*" and Paul Scheffer – author and eminent PvdA politician: "*Something like collective guilt does not exist, but there is an extra responsibility. Muslims have been too silent, they have frown away*". The host of Netwerk (Tijs van den Brink) stated: "*Dialogue? Shouldn't we be much tougher and say what is wrong with the Islam?*". On 2 and 3 November the headlines of three key Dutch newspapers read: "Slaughtering" (Telegraaf), "Filmmaker Theo van Gogh murdered" (NRC) and "AIVD [Dutch intelligence services] knew suspect". The Dutch newspaper Telegraaf published a large photo of the Theo van Gogh's corpse on its front page with the knife that dealt the deadly blow still in the chest of the film director. All news providers expressed heavy

indignation about the assassination. In their first analyses, most news providers related the murder to the provocative attitude of the film maker (often called the 'bête noir' of Amsterdam's intellectual elite) and his film 'Submission', which criticized the Quran. Several newspapers and the main news station NOS quoted ministers Donner (Justice) and Remkes (Internal Affairs) who stated that the perpetrator might have acted on to possibly have a radical Islamic basis. News providers interpreted the murder to be an 'attack' on the freedom of speech, many of them stating that it had been a *terrorist attack*.

To a far greater extent than after the attacks in New York, Madrid and London, the murder of Theo van Gogh evoked strong reactions among Dutch citizens. At the evening of the attack, a public "manifestation of noise" was held at the Dam square[322], which was attended by around 20.000 people who brought all kind of instruments (e.g. whistles, pans, rattles) to collectively make noise. The idea to make noise came from a group intellectuals who called themselves "Friends of Theo" and who wanted to demonstrate that the killing of Van Gogh did not lead to silence and that they were not intimidated by the murder. On all kind of websites[323] fierce debates emerged and the website of Theo van Gogh ("The healthy smoker") had to be closed down, due to the overwhelmingly number of posts on the website (www.theovangogh.nl). The condolences website www.condoleancepagina.nl, which was opened one hour after the murder received 8,000 posts in the first two hours and subsequently was aborted as the website administrator found that there were too many racist reactions. Two other condolences websites also had to be closed down. The one register which could stay open[324] received around 47.000 contributions. Not only among Dutch citizens, but also among Dutch intellectuals and artists heated debates emerged. In talk shows (e.g. Barend and Van Dorp) and newspapers (opinion pages), these debates particularly focused on the right to freedom of speech and the curtailment and the boundaries of this right. Several artists stated that they were no longer able to make provocative statements as they feared repercussions by Islamic fundamentalists and that the killing of Theo van Gogh had led to self-censorship among artists.

At the time of the assassination of Theo van Gogh, the political climate in the Netherlands was characterized by an increased polarization – particularly on the subject of integration of ethnic groups - between left wing (e.g. SP, PvdA and GroenLinks) and right wing parties (mainly Groep Wilders and VVD). Several right wing politicians considered the murder of Theo van Gogh to be a confirmation of their opinion that the Islam was a serious threat, that the Dutch immigration policy should be much more restrictive and that police and intelligence services should have more power to combat Islamic fundamentalism (e.g. TK, 22-1278, 11 November 2004). According to these politicians, the Dutch government's attitude towards migrants had been too soft and naïve (see also Hajer, 2007:5). Shortly after the killing, several public figures - among whom some politicians – positioned themselves as friends or acquaintances of the filmmaker and made use of the opportunity to stress their ideas about immigration, integration and/or freedom of speech. The VVD Minister Verdonk of Immigration and Integration for instance invited herself to the 'manifestation of noise' and held a speech in which she stated she had known 'Theo' and implied that she and the filmmaker were 'on the same side' (see also Hajer, 2007:10)[325]. Much more than was the case

[322] Hajer, 2007, p. 9.
[323] e.g, www.fok.nl, www.maroc.nl
[324] www.condeleance.nl
[325] VVD Minister Verdonk during the manifestation of noise: "I knew Theo. And I learned to know him better and better. Theo was the one who on the one hand said: 'Rita, keep that back straight!' But Theo was also the one that said: 'But also think about yourself, and think about the people'".

after 9/11 and the Madrid and London attacks, politicians participated in the 'public' debate, for instance through discussions with mixed audiences (e.g. artists, journalists, scientists) in talk shows (e.g. Barend en van Dorp).

During the parliamentary debate held after the murder of Theo van Gogh[326] politicians showed strong emotions. Wilders (Groep Wilders), who opened the debate, stated: "*Chairman. I am devastated and furious. I am furious, as Theo van Gogh is killed in a barbaric fashion by a Muslim terrorist, who also has fascist ideas. I am devastated, as my dear friend Ayaan Hirsi Ali has been threatened in an utmost disgusting manner for two years now, because of her statements and ideas and that – up to today - she cannot live a normal life. I am furious, as in many neighbourhoods in our country […], people are terrorized by – not rarely – Moroccan youths. […] But I am also furious as for years now Imams do things in Dutch mosques which do not stand the light of day […]. Chairman. I am furious, as we know that there are 200 people in the Netherlands which are being observed by the AIVD, as they are willing to use violence for the Islamic Jihad and that these people are roaming free.[…] In the Netherlands we have been too tolerant for people who would like to kill democracy, like people who adhere to radical Islam and want to die for that.*" Van Aartsen (VVD party leader): "*Mr. Chairman. Since last week the country is anxious and confused. Something smoulders and slumbers. The attack on Theo van Gogh hits the core of our national identity, the freedom of speech. The self-image of the polder has – more or less – fallen into pieces. This [the polder] was more or less our national proud, our World Trade Center, which has been destroyed by a terrorist. Which may be the cause of the confusion*". GroenLinks: "*Chairman. All strong words to describe the horrible murder on Theo van Gogh have been used. But a week after this terrorist attack we are still trembling. The pain in your stomach, the storm in your head, the elusive fear when you turn the corner of a street; whomever you speak to, the sadness is great, just like the confusion*." SP: "*Mr. Chairman. The country is bewildered. The country is confused. People fear for escalation and ask themselves: what next? It has been only 9 days after the coward murder on Theo van Gogh. […] The killing of Theo van Gogh was a terrorist attack*."

In the Theo van Gogh debate, all parties agreed that increased security measures were needed. PvdA (opposition party) for instance stated: "*We get the feeling that this Cabinet reduces the threat of an international organized and financed political movement to an integration problem of 'polder' size. Then you completely miss the point. The real solutions, […], should be sought elsewhere. Precisely because of the ruthless and international divided character of the political Islam, we have come to the conclusion that – at short notice – as regards the dealing with terrorists and potential terrorists emphasis should be placed on intensifying the approach of the police, Ministry of Justice and intelligence services. […] And if more capacity is needed, then more capacity there should be. Our society has seen a threat which we did not know before. Against this [threat] measures may be taken which we also have not known before. […In case of] an intensified use of powers, […], we will always advocate a higher level of control of the actions of – particularly - intelligence services*." And GroenLinks: "*Members of my party consider strong and effective measures against terrorism as inevitable and necessary. We do not disagree about the goal of a strong and effective fight against terrorism. We will never leave the Cabinet a total free hand in their measures, but we are willing to go beyond our political interests if the Cabinet demonstrates the necessity and the efficiency of the measures*." CDA and VVD (both parties in office – together with D66) stated that they supported the measures proposed by the Cabinet[327] among which: the

[326] TK, 29854, 11 November 2004.
[327] TK, 29854 no. 3.

elimination of resentful websites, increased observation by AIVD (Dutch intelligence agency) of persons who are – in some way – related to terrorism or radicalization, intensified searches on unknown radical or extremist persons, investment in data mining techniques, real-time access of AIVD to relevant datasets, expansion of AIVD capacity to gain intelligence abroad.

During the Theo van Gogh debate, privacy was mentioned in one instance by party leader of the CDA Verhagen. He stated: "*We should act now against potential terrorists. Security really is of more importance than privacy. We came to that conclusion before. We see that there is public support for this [statement]. Namely, someone who does not have anything to hide, does not have to fear.*[…] *For that matter I notice that some time ago the College Bescherming Persoonsgegevens [Dutch privacy watchdog] had strong criticism [on the extension of the powers of intelligence services]. That College stated that the necessity of the extension of powers was not proven. I however think that the murder of Van Gogh demonstrates that there actually is a necessity*." In a meeting of the parliamentary commissions on internal affairs and justice on the subject 'counterterrorism'[328], which assembled shortly after the Theo van Gogh assassination, privacy or privacy related subjects were mentioned a few times by other parties. PvdA stated: "*According to professor of Administrative Law Brenninkmeijer, the constitutional state nor the protection of the freedom of citizens [e.g. privacy] is in conflict with enforcement of the powers of police and the judiciary when needed. The constitutional state is a safe state in which the government ensures the protection of [the security of] citizens*." And CDA: "*The CDA perceives life more important than an inviolable legal position. Law is produced by humans, based on agreements and convictions. The CDA finds the constitutional right to security the most important right. Public security is the oldest classical task of the government. One has to act united and decisive in the war against terrorism*." SGP: "*The underestimation of terrorism in the name of the Islam is a greater threat to an open society than limitations to privacy*". Groenlinks stated during this debate that "*measures should be taken to effectively deal with the terrorism threat*." However, Groenlinks politician Vos stated that she was shocked by the way in which the Cabinet developed its new policy. She was concerned about the terminology used by the Cabinet and the extension of powers [of e.g. intelligence services] and stated: "*According to the Cabinet the Netherlands is at war. Does the Cabinet imply it has the permission to take measures with which it can extensively affect the rights and privacy of people*?"

Furthermore, it seems that top officials interpreted the role of the CBP restrictively and that they perceived the role of the CBP to be supportive to government policy making. Minister Donner (CDA) of Justice for instance stated in a debate on counterterrorism[329] shortly after the killing of Theo van Gogh that he would exchange thoughts with the CPB on the subject of privacy, but that the CPB should not be charged with the monitoring of operational actions. He agreed with the parliament that there should not be the impression that law enforcement agencies (e.g. intelligence agencies) do not comply with legislation (e.g. in case of information exchange). He however did not want to *"[generally] commit himself to the submitting of protocols for approval to CBP or asking the CPB for formal advice*". He stated that: "*Generally the CBP is quite cooperative, when it is aware of the facts*."

When taking stock of the security and privacy debates after the Theo van Gogh murder it seems that the murder has been firmly framed by politicians as a *terrorist attack*. Whereas

[328] TK, 27925 and 29754.
[329] TK, 27925 and 29754, 2004-2005, no. 149.

before 9/11 political or ideological murders often were referred to as *assault or assassination* (the murder of a prominent person or political figure by a surprise attack usually for payment of political reasons) politicians and media agreed this to be a an *attack* (as in military terms) of a *terrorist* – someone who uses or threatens to use violence against people with the intention of intimidating of coercing societies or governments for ideological or political reasons. In other words, the Van Gogh assassination was interpreted as an act of intimidation with the aim to disorder society and government. Some politicians spoke of the Netherlands being at war against terrorists. The word combination 'Terrorist attack' was not only used to describe the murder of Theo van Gogh, but also to describe the killing of Pim Fortuyn (a Dutch controversial politician) by a native animal rights activist two years earlier. In addition, the word 'terror' was used to describe all kind of violations and crimes such as 'street terror' – youths loitering around neighbourhoods while annoying and harnessing passers-by. Terrorist attacks were understood to be the great threat which could occur anytime and anyplace and by any extremists. Media and politicians clearly felt that with the killing of Van Gogh the Netherlands had been targeted by terrorism. Both media and politicians expressed their fears and (strong) emotions. All political parties asked for more security measures and most of them stated security to be of more importance than privacy. Only rarely potential privacy infringements were mentioned. Privacy was generally perceived as an impediment for security measures and the CBP in some instances as hindrance-causing institute. In some discourses it seemed that people who brought up privacy implications were perceived to be obstructers to (security) measures or nags.

Several publications on privacy in the Netherlands

From 2006 onwards, the security and privacy discourse seemed to slowly alter in the sense that privacy as a notion seemed to become more "salon-fähig" and that privacy concerns were more openly discussed. Publications of leading institutes, such as the Dutch Rathenau Institute (a research organization, founded by the Ministry of Education, Culture and Science) and Privacy International (an international advocacy organization which campaigns on privacy issues), may have substantially contributed to the renewed discussions on privacy subjects. In 2006, GroenLinks (the Greens) for instance asked questions about a yearly publication of Privacy International in which it ranks countries on the extent to which they respect human rights. In the 2006 report, the Netherlands was ranked 23th of countries which protect their citizens' privacy (below countries such as Hungary, Slovakia and Lithuania)[330]. Of the maximum of 5.0 points for countries which 'consistently uphold human right standards' (top three: Germany, Belgium and Austria), the Netherlands had 2.3 points and was labeled by Privacy International as a country which has 'some safeguards but weakened protections'. GroenLinks submitted the following question on 14 November 2006[331]: *"[Minister], do you know the research of Privacy International and Electronic Privacy Information Center, which shows that in the Netherlands privacy protection systematically fails? […]"*. Minister Hirsch Ballin (CDA) replied in a formal answer on 22 December 2006[332] "[…] *The in the research mentioned (Dutch) competences, such as telephone and internet taps and the exchange of personal data, are compliant with the EVRM, European case law and article 10 of the constitution. […] These competences are necessary in a democratic society. The competences aim to contribute to the national security, which complies with the in article 8, clause 2, of the EVRM mentioned goal criterion. […] In other*

[330] Privacy International, (2006), Surveillance Monitor 2006, International country rankings, based on EPIC Privacy and Human Rights Report, London.
[331] TK, 2006-2007, 2060702930.
[332] TK, 2006-2007, supplementary document no. 538.

countries, such as Germany and Belgium, elements of legislation have also been modified because of counter terrorism measures. I do not see any reason to take measures [to strengthen privacy]."

In 2007, the (aforementioned) Rathenau Institute published the report "From privacy paradise to surveillance state?"[333] in which it stated that since 9/11 the Dutch government (and governments of other countries) had taken many security measures (e.g. extension of retention dates of telecom data) which till 9/11 were unconceivable because of privacy infringements. The institute noticed that the security measures taken up till then, did not raise much public debate. In addition, it stated that the technological developments (e.g. advanced telephone taps, surveillance cameras, DNA profiles, data-mining) together with the far-reaching extension of powers of law enforcement agencies, provided these agencies with an almost unlimited access to personal data of citizens (Rathenau, 2007:6). The institute called for a societal and political reconsideration of the question to which extent 'we as a society' want to give up privacy for security. On 31 May 2007, D66 submitted questions about the Rathenau report and a publication "Protection privacy requires more sanctions" in the Dutch newspaper NRC (12 May 2007) to the Ministers of Justice and Internal Affairs[334]: *"[Minister], do you agree that the CBP should have more possibilities to sanction in case of privacy infringements? […] Do you agree with the Rathenau's statement that the whole of security measures fails to be discussed in a public debate? Do you share the concerns and agree that it is time for a fundamental debate about the emerging technologies and privacy […]?*". The Minister Hirsch Ballin (CDA) stated in reaction on 11 July 2007 to this[335] "*There are different views as regards the question whether the CBP has sufficient or insufficient possibilities for sanctioning. […] The first evaluation of the WBP [Dutch data protection act] is currently being conducted. […] The society is confronted with increased digitalization and internationalization. […] There is […] a cause to consider if and in what way the privacy policy should have a new impulse*."

Whereas up to mid-2007, the several Dutch cabinets (existing of both left wing and right wing parties) had consistently pursued a policy in which security measures were perceived to outweigh privacy, in July 2007 one of the ministers explicitly stated that the Dutch privacy policy might need a new impulse. It seems that at this moment the security and privacy discourse took a turn and that – in the political debate – privacy started to received more attention. However, the political attention to privacy concerned very specific – technology related - aspects of privacy.

Media-driven discourse on the implications of new technologies

From 2008 onwards, media increasingly reported on the possible privacy violations by (mostly social network) websites (e.g. NRC and Volkskrant 2008). Alarmed by the news reports, political parties started to expressed their concerns about the online collecting and use of personal data by commercial businesses. On 5 November 2008, members of parliament Heerts and Bouchibti (both PvdA) submitted questions to the Minister of Justice on the online privacy protection of children (TK, 2008-2009, 2080904630, nr. 912): "*Is it true that the administrators of Internet sites do not check whether children under 16 have the permission of their parents to publish personal data on the network sites, which, based on article 5 of the*

[333] Rathenau Instituut, *Van privayparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw,* Den Haag, 2007.
[334] TK, 2006-2007, 206071600.
[335] TK, 2006-2007, supplementary document no. 2146.

WBP [Dutch data protection act], is obligatory? Are you willing to conduct research on this and – when needed – to alert to administrators that they have the legal obligation to ask parents for permission? […]". And on 24 November 2008, member of parliament Atsma (PvdA) submitted a proposal to conduct a study on the online privacy protection of children. Atsma stated (TK, 2008-2009, 31700 VIII, nr. 49): *"[...] finding that many commercial websites still collect personal data of children without verifying whether the children have the approval [of their parents]. [...]requests the government to conduct research on the bottlenecks of the CBP [Dutch data protection supervisor] directives and to examine whether it would be possible to develop Dutch legislation conform the American COPPA (Children's Online Privacy Protection Act)*". On 10 December 2008[336], minister Hirsch Ballin provided the parliament with an extensive response in which he stated that in case of the data collection of children under 16, according to the WBP (Dutch data protection law) administrators of websites should verify whether the children have the permission of their parents to publish personal data. However, the minister stated not to be able to give an indication of the extent to which websites comply with this regulation. The cabinet stated that "*this subject [online privacy protection of children] has the full attention of the government, in particular of the Ministers of Justice and Youth and Family*"[337].

On March 2008, the Ministry of Justice and the Ministry of the Interior decided to establish a temporary commission 'Security and private spheres', also referred to as the Commission 'Brouwer-Korf'. Key task of this commission was to consult the government about the drafting of legislation and providing of information to citizens about security and privacy issues. The main conclusions of the Commission were that on the operational level (professionals involved in law enforcement) more attention should be paid to privacy protection of citizens and that the Dutch privacy watchdog CBP should work more independently. The Commission found that, as the CBP is founded by the Ministry of the Interior and predominantly perceived by government officials as an advising and facilitating body, the CBP would not be able to forcefully supervise government actions. The commission advised a fundamentally different role for the CBP, namely focused on critically monitoring government policy instead of supporting government. Both the cabinet and the large majority of political parties endorsed the conclusions of the Commission[338].

Meanwhile, the discussion on security had taken a turn as well, as ever more emphasis was placed on the subject 'cybersecurity' (protection against criminal or unauthorized use of electronic data). Due to several incidents (so-called 'phishing attacks', data leaks, examples of identity theft and hack of the Dutch public transport chip card) and reports on 'emerging cybercrime', members of parliament increasingly submitted questions and proposals on cybersecurity. In July 2010, the Dutch national police published a report which identified important 'crime areas' and stated 'high tech crime' to be one of these areas[339]. In the report it was said that: "*The growth of the phenomenon cybercrime and high tech crime undiminished continues. As far as measurable, the numbers show an exponential growth over the years - in some sub areas of 100% each year. This growth is enabled by the fast digitalization of societies which yields new 'attack vectors'. In addition, the cyber security awareness within society is low. [...]*". Both left wing and right wing parties posed questions on the subject and submitted proposals in order to enforce cyber security. On 27 August 2010, member of

[336] TK, 2008-2009, 2080904630, no. 912.
[337] TK, 2008-2009, 31700 VIII, no.144.
[338] TK, 2009-2010, 31051, no. 5.
[339] KLPD – Dienst National Recherche, (2007), Overall-beeld Aandachtsgebieden, Driebergen

parliament Gesthuizen (SP) asked the minister of Justice and Economic Affairs[340]: "*Do you know the news report on the exponential growth of cybercrime in the Netherlands [Dutch news provider webwereld.nl]? How many incidents of cybercrime are there on a yearly basis?*". And the member of Parliament Recourt (PvdA) submitted the following question (TK, 2010-2011, 2010Z15331): "*Have you seen the Nieuwsuur program [Dutch newsreel] on cybercrime? Do you agree with the interviewees, among which a public prosecutor specialized in cybercrime, that the power of police and justice should be extended as regards cybercrime, more specifically the possibility to 're-hack', irrespective of the location of the computer?*". On 7 January 2011, the member of Parliament Schaart (VVD) asked the minister of Economic Affairs[341]: "*Have you read the article "Dutch companies target of cyber-attacks" [Dutch online news provider Nu.nl]? Are you aware of the fact that the Netherlands is among the countries with the most ICT security incidents within the European Union and that Dutch companies are often victim?*"

Between 2007 and 2010, both the privacy and the security debate took a significant turn. The influence of emerging technologies played a dominant role in both discourses. In the security debate new terminology appeared (e.g. 'cybercrime', 'cyber war', 'cyber attacks', 'cyber defense') and the privacy debate was highly focused on online privacy of citizens and data protection. At the onset of the online privacy and cybersecurity discourses, the debates were held separately and in some instances statements of parties in the debates were even contradictory. The PvdA for instance asked the minister of Security and Justice in the cybersecurity debate to extend the power of law enforcement authorities to fight cybercrime (e.g. by providing them with the power to 're-hack' computers) and – in a parallel debate on online privacy – demanded from the same minister measures to enhance the online privacy of internet users. An integral discussion on technological developments and the implications for security and privacy seemed to be missing. In addition, as stated before the security – the privacy discourse was heavily focused on technological implications while leaving out other aspects of privacy (e.g. seclusion, bodily integrity, private possessions and property).

Security meets privacy

In the summer of 2011, the debate on social media and privacy seemed to peak as a flood of parliamentary questions were posed on this subject by both left wing and right wing parties. Most of these questions yielded from news reports. On 11 August 2011, members of parliament Recourt and Van Dam (PvdA) for instance submitted the following question to the Minister of Security and Justice: "*Do you know the article 'How LinkedIn links users and advertising?' [Volkskrant, 4 August 2011]? […] Is it true that the network site LinkedIn has changed user settings in such a way that photos and names of users can be used unasked for advertising? […] Does the CBP act upon this?*" On the same day Recourt and Van Dam submitted the question[342]: "*Are you aware of the fact that Facebook – through the special Facebook application for smartphones – automatically synchronizes the contact persons from telephone lists with [Facebook] friends and that consequently telephone numbers of Facebook friends automatically appear on someone's Facebook page?*". On 17 August 2001, members of parliament Verhoeven and Schouw (both D66) asked the minister (2010-2011, 2011Z16149): "*Are you aware of the article "Companies neglect privacy legislation" [Telegraaf, 13 Augustus 2011]? Do you share the observation being set out in this article that companies should provide [users] access [to personal data] but that the rarely do so?*". And

[340] TK, 2009-2010, supplementary document no. 3367.
[341] TK, 2010-2011, 2011Z00123.
[342] TK, 2010-2011, 2011Z16066.

on 4 October 2011, member of Parliament Verhoeven (D66) submitted the following question to the minister of Economic Affairs, Agriculture and Innovation (TK, 2011-2012, Aanhangsel 556): "*Did you read the article "Call for investigation use of cookies by Facebook?" [Dutch news website nu.nl]? What is your opinion on the collecting of privacy sensitive information by Facebook through the use of undeletable cookies?*". In most of the instances the responsible minister or deputy minister referred to the CBP (Dutch privacy watchdog) stating that the CBP is responsible for the supervision of compliance to the WBP (Dutch data protection law) in specific cases.

In addition, discourses emerged in which privacy and security were mentioned as matching instead of competing values. Whereas in the aftermath of 9/11 and the Theo van Gogh assassination security and privacy were understood by politicians as rival notions, since 2011 there was a general call for security measures to protect citizens' privacy. The Dutch government stated in its report 'Cybersecuritybeeld NL' (2011) that: "*The government and businesses store many personal data and citizens - in a voluntary manner - share much personal information through amongst others social networks. Ever more privacy sensitive information is in detail stored in [so-called] profiles, but is also linked to other data. The detailed storage makes that people are vulnerable for malicious or undesirable use or publication of the information*." Also in political debates, privacy and security were increasingly mentioned in the same sentence, as part of the same perceived problem. On 13 October 2011, the members of parliament Gesthuizen and El Fassed (respectively SP and GroenLinks) stated in a proposal that[343]: *"[…] considering that the insufficient direction in ICT security policy and privacy protection has led to several instances of deficiencies and the danger of citizens' privacy and security. […] [We have] the opinion that a parliamentary inquiry on the causes, effects and possible improvements of the […] government ICT security […] is needed*." And Gesthuizen (SP) and Verhoeven (D66) proposed on 27 October 2011[344] *"[…] recent problems as regards privacy, security and the protection of citizens on the internet reveal that the Netherlands has to take necessary steps in the area of ICT-security. […The party] asks the cabinet to inform the parliament in the first quarter of 2012 about its vision [on ICT security]*."

In more recent years, both the security and privacy debates have been highly technology driven. In the privacy debate a strong focus can be found on data protection (the creation of safeguards for individuals relating to personal data stored on a computer) and in the security debate on cyber security. "Facebook" or "Linkedin" may have been the most important metaphors in the privacy discourse, which terms can be perceived as emblems of the debates about privacy infringements by commercial websites. "Cybersecurity" seemed to be a dominant metaphor in the security debate, which term was used for all kind of technological security measures. In addition, both debates seemed to have converged as the notion (cyber) 'security' is increasingly defined as a precondition for (online) 'privacy'. Cyber security and online privacy have been institutionalized in all kind of new rules, policies and organisations. As regards cyber security, the Ministry of Security and Justice for instance implemented a National Cyber Security Strategy, drafted a directive on baseline information security, established the Cyber Security Board, Information Point Cybercrime and the National Cyber Security Centre. Measures taken to strengthen online privacy were (amongst others) the drafting of Cookie legislation.

[343] TK, 2011-2012, 26643, no. 194.
[344] TK 2011-2012, 24095, no. 294.

8.5 GENERAL CONCLUSIONS AND REFLECTIONS

When taking stock of the security and privacy debate in the Netherlands, a number of interesting patterns emerge. First, it seems that the framing of security and privacy in the Netherlands has taken place particularly in the media and parliament. Here, (new) meaning has been attributed to the notions security and privacy, which were reproduced in all manner of policy documents and eventually translated into concrete measures. Contrary to other countries, in the Netherlands the data protection supervisor CBP has played a very limited (almost negligible) role in the discourse. Moreover, the role of the CBP was perceived until the report of the security and privacy Commission Brouwer-Korf in 2009 as supportive and compliant to the Ministry of the Interior. The analysis of documents shows that after critical events, such as 9/11 and the Theo van Gogh assassination, strong ideas on the balance between security and privacy were predominantly conveyed through media and politics. These ideas had a certain regularity in the sense that security and privacy were perceived as a trade-off concept and security was generally given more importance than privacy.

A second pattern that emerges from the discourse analysis is the break with the discursive tradition in which privacy had been perceived as less important than security and the increased convergence of security and privacy debates. Whereas between 2001 and 2007 security and privacy were generally understood as rival values, from 2008 onwards security and privacy were increasingly mentioned as matching values. After 9/11 and the Theo van Gogh assassination there was a general call for more security – if needed at the expense of privacy. The debates on security and privacy mostly took place separately, within different parliamentary commissions or – in the media – in different television programs or news articles. Although today this separation between debates still can be noticed (e.g. in 2011 the PvdA party submitted a proposal to extend the online power of intelligence agencies in the one debate and submitted proposals to strengthen online privacy of users in another debate) the debates seem to converge more and more. Over the past couple of years, security started being mentioned more often than privacy, often as a precondition for privacy protection (i.e. technological security measures that should be taken in order to protect citizens' online and offline privacy). Over the years, a conceptual shift can be distinguished in the way in which privacy and security are defined and understood (i.e. from rival values to matching values) as well as an increased integration of the hitherto separate debates on privacy and security.

Third, important metaphors used in the discourses were "*terrorism*" and "*Facebook*" or "*Linkedin*". The term terrorist attack was for instance not only used in cases of an attack (in military terms) of a group of people whose intention was to intimidate society and government, but in all kind of other cases, such as the assassination of Pim Fortuyn by an animal rights activist. Various incidents were viewed through a "terrorism" lens: for example youths loitering in urban areas and disturbing the public order were referred to as street terror. Terrorism functioned as an emblematic issue; it was an emblem for the general fear of disruption of the Dutch society by extremist actions. While "terrorism" was an important metaphor in the security discourse, "Facebook" or "Linkedin" may have been the most important metaphors in the privacy discourse. Facebook and Linkedin can be perceived as emblems of the debates about privacy infringements by commercial websites. Media and politics seemed to share a mutual understanding of intentional violation of users' privacy by commercial websites for the organizations' gain and frequently used Facebook or Linkedin as emblem for this behaviour.

Fourth, in both the media and the political debate the way in which the concept privacy is defined is relatively narrow. The past few years there was a strong focus in the discourse on online data protection (generally defined as safeguards for individuals relating to their personal data stored on a computer). The right to privacy however can be interpreted much broader. In literature, privacy has been defined as both a negative and positive right. Whereas the negative perspective focusses on forms of privacy infringements, the positive perspective tries to define find ways to strengthen individuals' privacy (e.g. Solove, 2008). When comparing the definitions and taxonomies in literature with the definitions used in the political and public discourse it seems that the latter do not do justice to the complexity of the notion privacy. Forms of "off-line" privacy invasion seem to be under-exposed in the discourse, such as invasive acts that disturb one's tranquillity or solitude, incursion into a subject's decisions regarding private affairs or the revealing of someone's nudity, grief or bodily functions. In addition, the right to privacy is rarely addressed within the broader context of the full spectrum of fundamental rights.

Sixth, institutionalization. Overall, privacy protection in the Netherlands seems to remains limited, as revealed by the on-going institutionalization of the fight against terrorism and a limited role for the Dutch data protection authority.

8.6 HYPOTHESES FOR THE PRISMS SURVEY

Based upon the observations made in the previous paragraphs the following hypotheses can be formulated. These hypotheses shall be verified through the WP8 survey of the PRISMS project.

- The understanding of the notions 'security' and 'privacy' is predominantly shaped by media and politics, with only a limited role for watchdogs and citizens.
- The framing of the notions 'security' and 'privacy' by media and politicians is highly influenced by incidents and lacks a more profound vision on these concepts.
- In today's discourse, the complex notion privacy is interpreted narrowly with a strong focus on the relation with technology, while under-exposing other (mostly off line) aspects of privacy.
- In today's discourse, very specific aspects of online privacy (e.g. data protection) receive much attention, while a broader and more fundamental discussion on human rights is lacking.
- The notions 'security' and 'privacy' have been predominantly approached by media and politics as a trade-off concept – more security by default implies less privacy and vice versa.
- In political debates, general statements about the balance between security and privacy were made which did not do justice to the complexity of the notions and the complicated relationship between the notions.
- In the past decade, the problem definitions and concepts underlying the notions 'security' and 'privacy' have substantially changed from mainly 'terrorism' to 'technology' driven.
- Around 2008, in the Netherlands there was a break with the discursive tradition (from 2001-2007) in which security was perceived to be more important than privacy (until then the term security had more rhetorical power).
- Around 2008, in the Netherlands there was a break with the discursive tradition (from 2001-2007) in the sense that the 'complaining' connotation of the word privacy

diminished (privacy as a notion became more popular, salon-fähig, 'sounded more right').

- In the past decade, the discourse coalition among Dutch political parties shifted form the shared use of a story line focused on terrorism to the shared use of a story line focused on emerging technologies.
- After 9/11 and the Theo van Gogh assassination, the shared story line of Dutch political parties that 'far-reaching security measures were needed to combat terrorism' has been highly institutionalized (reproduced in policies, organizations and translated into various of practices).
- The security discourse has been much more institutionalized (translated into policies, rules, organisations) than the privacy discourse.

9 PRIVACY AND SECURITY DISCOURSES IN SELECT POLICY DOCUMENTS OF THE INSTITUTIONS OF THE EUROPEAN UNION

9.1 INTRODUCTION

The framing of the two topics, security and privacy, by the European Council, Commission and Parliament has been highly influenced by various critical events. Of these incidents, 9/11 may have been most influential as it gave rise to new definitions and metaphors such as "terrorist offences" and "combating terror". Moreover, as the discourse analysis will demonstrate, the content of the privacy and security discourse and the specific measures taken by the Commission have been substantially influenced by one of the key actors of the discourse, the United-States of America (US). The terminology used by the US, as well as specific actions taken can be traced back in debates and policy documents of European institutions. This document describes the security and privacy debate in the aftermath of 9/11, specific debates in which there was much controversy on the security and privacy subjects (the PNR debate) and debates in which there was less dispute on these subjects (the Stockholm Programme). For each debate, the key metaphors, story lines (i.e. lines of reasoning), discourse coalitions (i.e. actors which share a certain opinion) and institutionalization (i.e. translation of opinions into e.g. rules and practices) are set out (in section 16.4). First however, the tables used for empirical data collection, the key actors involved in the security and privacy discourse and the public attention to these notions are presented (sections 16.2 to 16.4 respectively). This, in order to provide an overview and sketch the context of the discourses. The document will conclude with a general reflection upon the European institution's discourse on privacy and security and hypotheses which provide input for the survey in PRISMS' WP8 (section 16.6) and an overview of literature and documents studied (section 16.7).

9.2 METHODOLOGY

For each specific debate, leading parliamentary and policy documents have been studied. Subsequently, (a) frequently used terms, (b) key storylines (lines of reasoning) and (c) key actions taken upon the debate (i.e. institutionalisation) have been collected and structured within tables. We have chosen to extract these three aspects from the discourses based upon the discourse analysis methodology of Hajer[345]. By studying these three aspects the precise framing of the security and privacy notions, the argumentation used and the extent to which the discourses have had an impact in terms of e.g. new rules, policies and organisations will be revealed. Hajer uses a rather broad definition of the term 'insitutionalisation' as he includes not only the drafting of new rules and establishing of new organisations, but also new policies and other actions taken upon specific debates[346]. For a more elaborate description of the methodology see chapter 13 of this report.

[345] E.g. Hajer, 2005, 2006a, 2006b.
[346] E.g. Hajer 2006b, p. 70.

9.3 KEY DISCOURSES

The three key discourses identified are: combatting terror; Passenger Name Records; and the Stockholm Programme.

The first table below outlines the key metaphors, story lines, discourse coalitions and institutionalisation of the broader European debate on the topic of the fight against terror (combatting terror) in the aftermath of 9/11.

Combating terror

Terms	Key storylines	Institutionalization
• Barbaric act • Attack on open, democratic societies • Terrorist offences • Combating terror • Solidarity with US • One European judicial space • Weapons of mass destruction • Biometric data • Democratic deficit • Fundamental freedoms • Democratic freedoms	Council of Europe • "Terrorism is a real challenge to the world and to Europe, terrorism is a priority objective of the European Union." • "The Council is totally supportive of the American people. The attacks are an assault on our open, democratic, tolerant and multicultural societies." • "The EU will cooperate with the US in bringing to justice and punishing the perpetrators, sponsors and accomplices of such [9/11 attacks] barbaric acts." • "On the basis of Security Council Resolution 1368, a riposte by the US is legitimate." • "The Member States of the Union are prepared to undertake such actions, each according to its means. The actions must be targeted and may also be directed against States abetting, supporting or harbouring terrorists." • "The EU will step up its action against terrorism through a coordinated and inter-disciplinary approach embracing all Union policies. It will ensure that that approach is reconciled with respect for the fundamental freedoms which form the basis of our civilization." • "EU has to act rapidly, visibly and decisively in the fight against terrorism." European Parliament • PPD-DE "There is no greater risk to the freedom of thought, of expression and to the right to life itself, than violence expressed through terrorism." • PSE "I have no respect for those who seek to take the lives of others in order to achieve their aims. None at all. In my view, no effort to put an end to this is too	• Plan of action of the Extraordinary European Council meeting on 21 September 2001 • Framework directive on combating terrorism • European arrest warrant • Common definition of terrorism • Framework decision on freezing assets of suspects • Measures taken by the Transport Council which covered amongst others: the classification of weapons, technical training for crew, checking and monitoring of hold luggage, protection of cockpit access and quality control of security measures applied by Member States.

Terms	Key storylines	Institutionalization
	great. On the other hand, however, I have the greatest respect for our democratic system and rights, and also believe that the Parliament has an obligation to defend them with the same enthusiasm. ” • Verts/ALE “The issue of the European arrest warrant is quite bizarre, not only because important issues remain vague, but also because Parliament lacks the courage to exact what it agrees to in substance. […] This [the definition of serious crimes] remains unclear, and a lack of clarity in criminal law leads to the sense of justice being eroded. […] If the Council is just as dynamic and decisive in guaranteeing citizens' rights as it is in taking repressive measures, the European arrest warrant will not run unto any delays.” • GUE/NGL “Mr President, for a second time, we are rejecting a text which forms part of a campaign conducted by the Bush Administration and which, in the name of the fight against terrorism, merely seeks to place the most basic democratic freedoms in jeopardy throughout the world, with total disregard for international conventions. […] And, several dozen prisoners are now being detained in appalling conditions, at the Guantanamo Bay military base, who have no guarantees and no status.” • EDD ”[…] the date of 11 September has made it even clearer that a tough battle against terrorism and organized crime is what is needed in order to guarantee the free area of peace and security in the Member States. Via the present proposals, the Council is making a commendable effort to contribute to this by making rapid extradition possible.” • UEN “[…] since the terrorist attacks […], we in the European Parliament have debated the threats to our freedom, democracy and values in a more realistic light than before. Most of us have realized that an attack on the US is an attack on ourselves. Just a few moths further on, however, there are circles that are busy relativizing the threats by distancing Europe from the US. None of us like the restriction and controls that hit all of us and limit everyone's right to freedom, but we have to accept them because we do not know where, and precisely who, the enemy is. […However] legal certainty is not, in all Member States, at a level that can justify such far-reaching [European arrest warrant] surrender procedures as are at issue here.”	

The table below outlines the key metaphors, story lines, discourse coalitions and institutionalisation related to the controversial, much-debated and long-drawn-out topic of the Passenger Name Records (PNR).

Passenger Name Records

Terms	Key storylines	Institutionalization
• United States • US Aviation and Transportation Security Act • Fight against terrorism • Passenger Name Records • 'light' agreement • Data Protection Directive 95/46/EC Rules of Procedure • Legal basis for exchange • Retention dates • Adequacy finding • Right to privacy and data protection • Proportionality • "push" or "pull" system • Exceeding powers • Democratic deficit • Appeal to Court	European Commission • "The US is a democratic country, governed by the rule of law and with a strong civil liberties tradition. The legitimacy of its law-making process and strength and independence of its judiciary are not in question." • "Press freedom is a further strong guarantee against the abuse of civil liberties. […] The Community is fully committed to supporting the US in the fight against terrorism. The Community should not interpret and apply its own rules in a way incompatible with this commitment or raise obstacles to US measures to protect its own borders unless these are clearly dictated by the law of the Community or the European Union**."** • "The Commission discussed privacy guarantees for European citizens as regards PNR with the United States on several occasions since the publication of the implementing rules, which, after one postponement, entered into force on 5 February 2003." • "As a result of the démarches by the Commission, the United States' Customs agreed to waive the imposition of penalties on non-complying airlines until 5 March 2003. These penalties included severe fines and even the withdrawal of landing rights." • "In order to reconcile United States' requirements with the requirements of data protection law in the Union, a meeting took place on 17 and 18 February 2003 between senior officials of the Commission and the United States' Customs Service." • "As a result of those discussions, the two sides issued a Joint Statement which sets out the steps that need to be taken to reach a mutually satisfactory solution that can provide legal certainty to all concerned." • "Both sides agreed to work together towards a bilateral arrangement under	• Joint declaration of 19 February 2003, US and the European Commission • Undertakings of the US Department of Homeland Security Bureau of Customs and Border Protection • European Commission's Decision on Adequacy Finding • European Council Directive 2004/82/EC, of 29 April 2004, on the obligation of carriers to communicate passengers data, Official Journal of the European Union, L 261/24, 6.8.2004 • PNR agreement 2004, Official Journal of the European Union, L 183/83, 20.5.2004 • PNR agreement 2007 (applied on provisional basis), Official Journal of the European Unions, L 204/18, 4.8.2007 • PNR agreement 2012, Official Journal of the European Union, L 215/5, 11.8.2012

Terms	Key storylines	Institutionalization
	which the Commission, in response to information and undertakings provided by the United States side about the way transferred data would be handled and protected in the United States, may take a decision under Article 25.6 of the Data Protection Directive, on the adequacy of the level of protection ensured by the United States." • "The US-EU PNR agreement complies with Community law." <u>Article 29 Data Protection Working Party</u> • "PNR data may only be transferred when adequate safeguards are afforded, among which: transitional nature of an adequacy finding by the Commission, proportionality (e.g. type of data, retention dates), adequate method of transfer (e.g. push of pull data), limited purposes (limited to terrorism, no other serious criminal offences), effective enforcement of data subjects' rights and independent third-party supervision." • "More guarantees are needed, for instance: (a) specifying the data which could be legitimately transferred without risk (the Working Party suggested 19 items on 13 June 2003 referred to in Article 29 of Directive 95/46/EC1), (b) replacing the 'pull' system (which has no filters for sensitive data or for non-transatlantic flights) with the 'push system' (which enables airlines to transfer only legitimate data and only in respect of flights to US destinations), (c) negotiating an international agreement with the US which will offer genuine guarantees for passengers or, at the very least, the same protection as is afforded to US citizens." <u>European Parliament</u> • PPE-DE "If the Americans do not get by this route the information they require, they will obtain it by other means, whether this involves questioning at the border, mandatory visas or interviews in Consulates-General. […] if we do not get this agreement, our citizens will be in no better a legal position as regards data protection; indeed they will be in a worse one, because we will have no influence whatever on what the Americans do with the data they obtain." • PPE-DE "the […] opinion of the Court […] will only postpone the signing of the	

Terms	Key storylines	Institutionalization
	agreement and leave a legal vacuum in place in relation to the treatment of personal data by the US authorities […] We also believe, naturally, that this agreement can be improved but also that the fight against terrorism and cooperation with third countries in the field, with the US in this case, is a priority for the European Union. […], we need the agreement now […]" • PSE "[…] for more than a year, a majority in this Parliament – although the Group of the European People's Party and European Democrats are of the opposite opinion – has claimed that it is a serious violation of the fundamental right of European citizens to data protection to demand that all European airlines are obliged to process European citizens' data contained in their computerized reservation systems as requested by the United States Department of Homeland Security, Bureau of Customs and Border Protection and in line with US legislation. On top of that, there is not even any US legislation since no US law existis to protect private data." • GUE/NGL "On many occasions, the Commission has said that this is the best agreement that it could extract from the United States Government, but it must be said that, the more debates we have, the worse the situation gets for European citizens. Indeed, today we know that this agreement not only implies a violation of the Treaties, but even the possibility that these data will be transferred to a third country and will be processed by them, which thus made it more difficult to get the debate on the first part of the agreement under way." • ELDR "There is a huge democratic deficit when the Commission comes forward with a proposal like this and does not give either the EP or national parliaments the chance to say yes or no". And: "[…] I am not very happy about the Commissioner's remark that there is no violation of Regulation 95/46. Paragraph 4 of the agreement itself states that all data of European passengers will be processed according to US constitutional requirements. One of the laws in the United States that should apply is the Privacy Act, but this Act does not apply to people from third countries, to name but one example. Article 6 of the agreement states that there will be reciprocity insofar as feasible and that it shall be strictly applied. […] I can easily give you another ten examples of things	

Terms	Key storylines	Institutionalization
	that are not right and are, in my view, a violation of our privacy legislation." • Verts/ALE "it is indisputable, Commissioner Bolkestein, that by not entering into a real international agreement with the US, the Commission, has chosen to bypass Parliament's opinion. The fact that you have opted for a soft law instead of a real agreement already speaks volumes about the Commission's intentions to exclude democratic control of this agreement, and I find this particularly worrying".	

The last table (below) outlines the key metaphors, story lines, discourse coalitions and institutionalisation of the European debate on a comparatively less disputed topic of the Stockholm Programme.

The Stockholm Programme

Terms	Key storylines	Institutionalization
• Area of Freedom, security and justice • Citizen's Europe • Single area • Charter of Fundamental Rights • Freedoms and privacy beyond national borders • Data exchange and data processing • Protection of personal data • Restriction of privacy rules in the exercise of lawful duties (trade-off)	European Commission • "The main thrust of the new programme will be 'building a citizen's Europe'. And that 'All action taken in the future should be centred on the citizen[..]." • "The area of freedom, security and justice must above all be a single area in which fundamental rights are protected, and in which respect for the human person and human dignity, and for the other rights enshrined in the Charter of Fundamental Rights, is a core value. For example, the exercise of these freedoms and the citizen's privacy must be preserved beyond national borders, especially by protecting personal data; […] and citizens must be able to exercise their specific rights to the full, even outside the Union." • "The Union must secure a new comprehensive strategy to protect citizens' data within the EU and in its relations with other countries." • "It must also foresee and regulate the circumstances in which public authorities might need to restrict the application of these rules [regarding data protection] in the exercise of their lawful duties." European Parliament • The Stockholm programme has only sparsely been a subject of debate within	• Communication on a new legal framework for the protection of personal data after the entry into force of the Lisbon Treaty • New comprehensive legal framework for data protection • Communication on Privacy and trust in Digital Europe: ensuring citizen's confidence in new services • Personal data protection agreement for law enforcement purposes with the US • Communication on core elements for personal data protection in agreements

Terms	Key storylines	Institutionalization
	the European Parliament. • In November 2009 the Stockholm Programme was debated in the European Parliament, one month before the programme was adopted. The general attitude towards the programme as expressed in this debate was positive and the need to continuously balance measures aimed at creating security and measures aimed at protecting the rights of individuals was often stressed. • "[…]the basic point here is the balance between security and freedom. It is obvious that we have to protect our citizens against terrorism and organized crime, but maybe, after 9/11, we have put too much focus on security and protection. I think that the Stockholm Programme […] has to rebalance that towards respect for fundamental rights and also more openness in society.[…] it is more ambitious than the Tampere Programme and the Hague Programme, but with a more important focus on the fundamental rights of the people."	between the European Union and third countries for law enforcement purposes

9.4 KEY ACTORS AND WORD COMBINATIONS

In the European political arena, several key actors have been involved in the security and privacy discourse. The debates on these issues were most outspoken in the aftermath of 9/11 in several Euro-parliamentary gatherings. It seems that precisely within the parliamentary debates (and in the interaction of the European Parliament with the European Commission) the tension between security and privacy became particularly apparent and that here the two notions were attributed meaning. The framing of security and privacy in European politics resulted in specific policies of Directorate-Generals (e.g. Justice) of the European Commission which applied similar understandings of the two notions (i.e. reproduction). As stated before, the minutes of debates and policy documents studied reveal the dominant role of the US in the security and privacy dialogue. The terminology applied by the US and the measures proposed can be traced back in debates and policy documents of the European Union. In addition, the European Data Protection Supervisor played an important role in the discourse. Metaphors and storylines provided by the European Data Protection Supervisor were adopted by Members of the European Parliament (MEPs) and reproduced in their discussion with the European Commission. However, when examining the several PNR agreements between the US and the EU, it seems that the opinion of the European Data Protection Supervisor has been institutionalised only to some extent. The following actor network picture provides an overview of key actors involved.

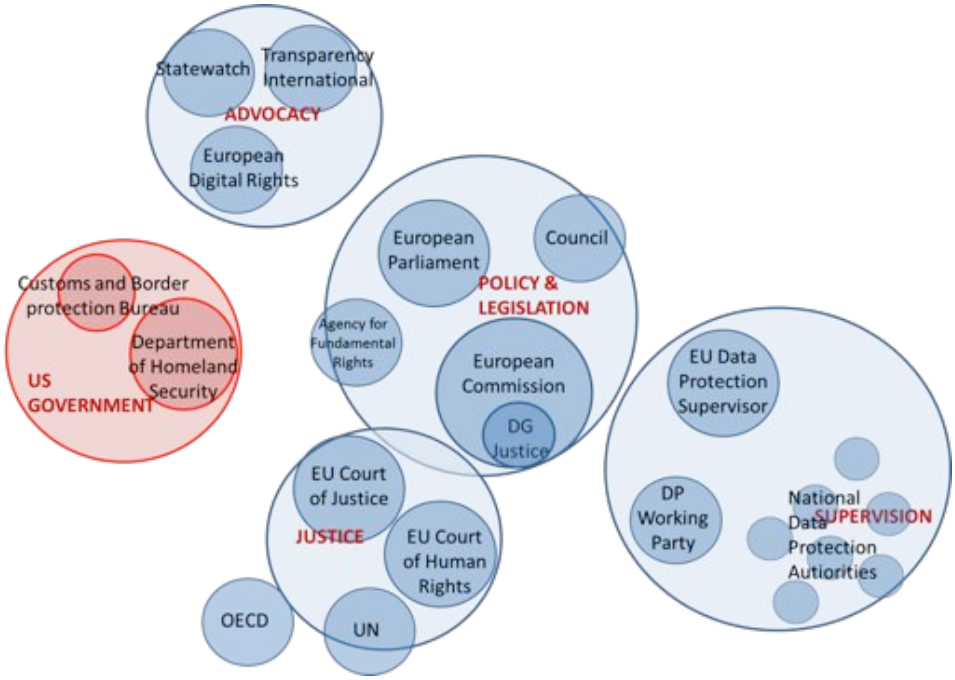

Figure 1, overview key actors involved in the European privacy and security discourse

9.5 PUBLIC INTEREST

The extent to which citizens have been occupied with the subjects 'security' and 'privacy' can to some extent be deduced from the frequency with which citizens have searched for information about the subject on the Internet. When citizens are concerned about something, they often will try to find online information about the subject. As the large majority of users use Google as their primary search engine (according to Statowl, in June 2012 Google had

81,1% of the market share[347]), statistics about the frequency with which users searched for specific information through the Google search engine can provide indications about the extent to which subjects were important to users. As for the present European discourse analysis it was not feasible within the scope of this work package to examine the search behaviour of the citizens of all European Member States. Therefore, we decided to depict the searches of citizens of four European Members States within the four geographic areas: Northern, Southern, Eastern and Western Europe. The four countries of which the searches have been mapped in graphs are Sweden, Italy, Romania and France. Although no general conclusions can be drawn on the interest of European citizens in security and privacy topics based on the findings in the four countries, a comparison of the graphs can contribute to the formulation of hypotheses (in section 16.6 of this document) which will feed into work package 9 (survey) of this research project. The following graphs show the frequency of specific Internet searches over the past seven years in these four countries. The y-axis reflects the percentage of searches of the total search volume.

Sweden

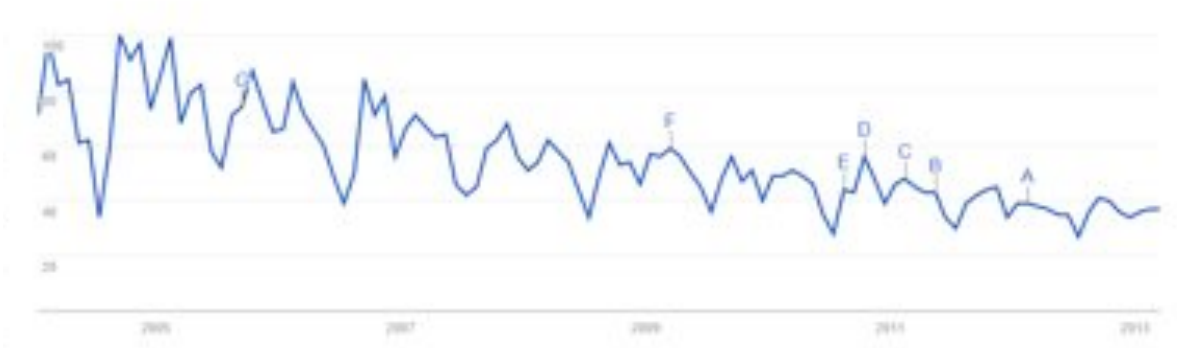

Figure 2: The frequency with which the term 'säkerhet' was entered by Swedisch users into the Google search engine (2005-present).

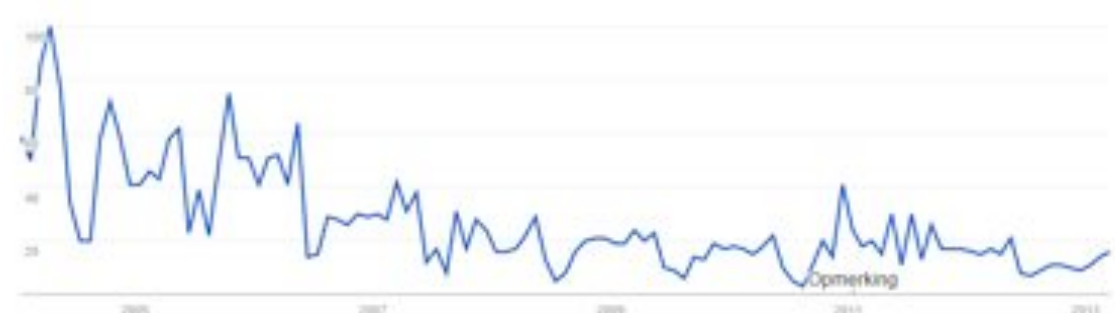

Figure 3: The frequency with which the term 'terrorism' was entered by Swedish users into the Google search engine (2005-present).

[347] http://www.statowl.com/search_engine_market_share.php

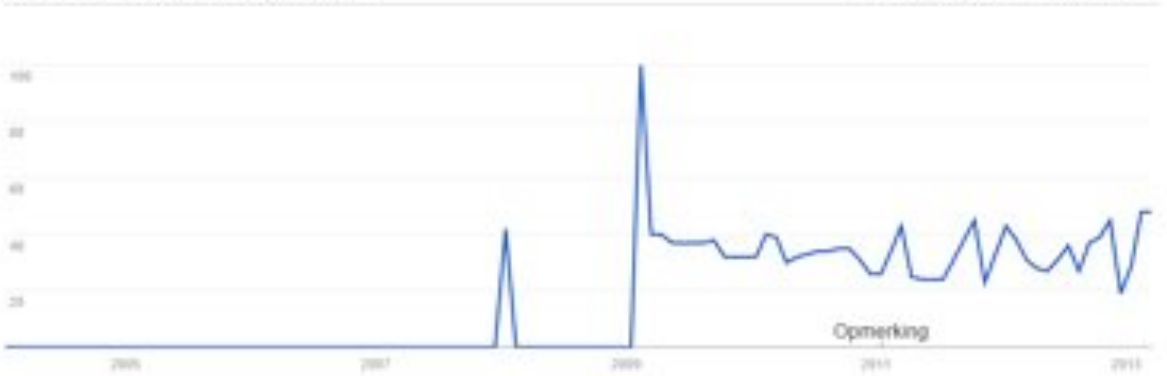

Figure 4: The frequency with which the term 'privatliv' was entered by Swedish users into the Google search engine (2005-present).

Romania

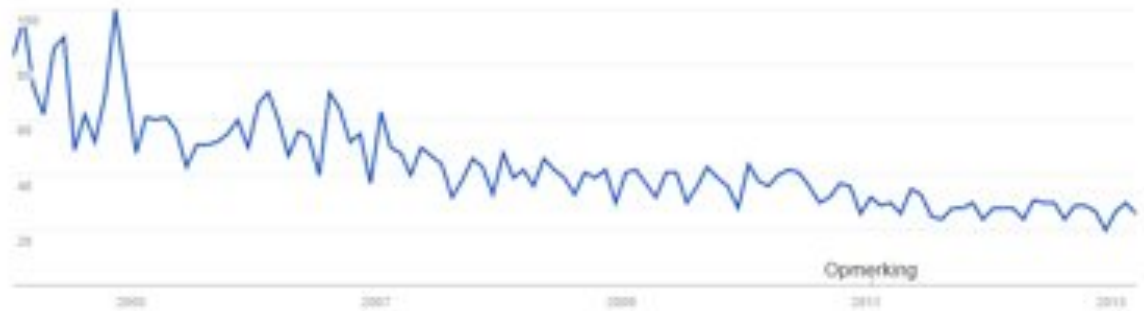

Figure 5: The frequency with which the term 'securitate" was entered by Romanian users into the Google search engine (2005-present).

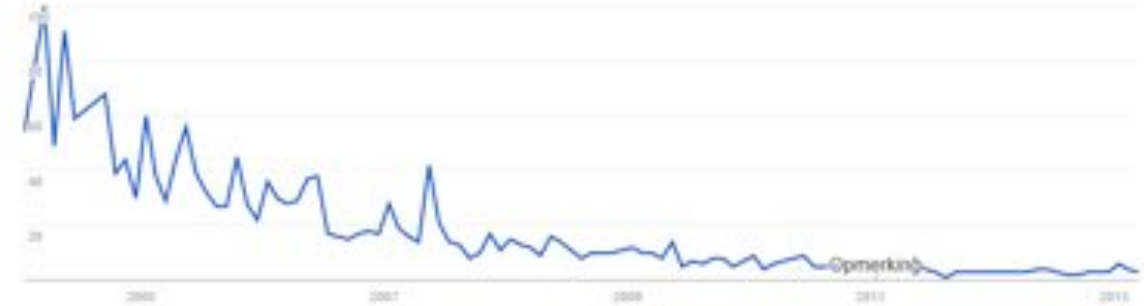

Figure 6 (above): The frequency with which the term 'terorism' was entered by Romanian users into the Google search engine (2005-present).

Figure 7 (above): The frequency with which the term 'viata privata'was entered by Romanian users into the Google search engine (2005-present).

Italy

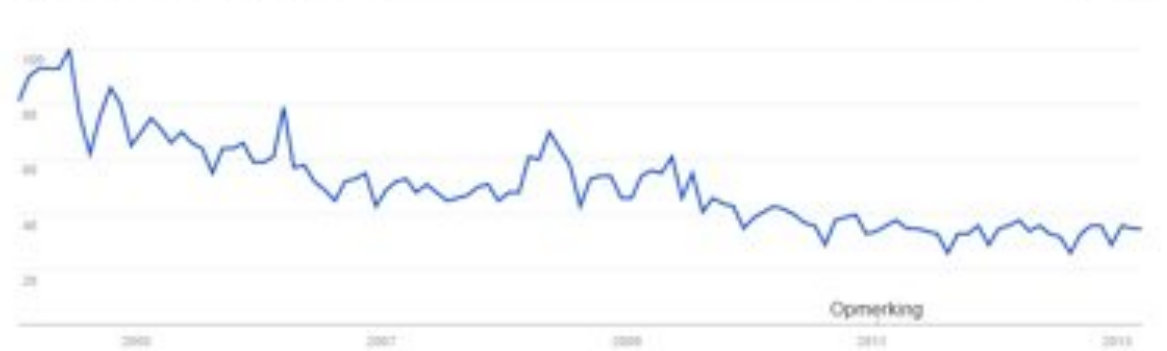

Figure 8 (above): The frequency with which the term 'sicurezza' was entered by Italian users into the Google search engine (2005-present).

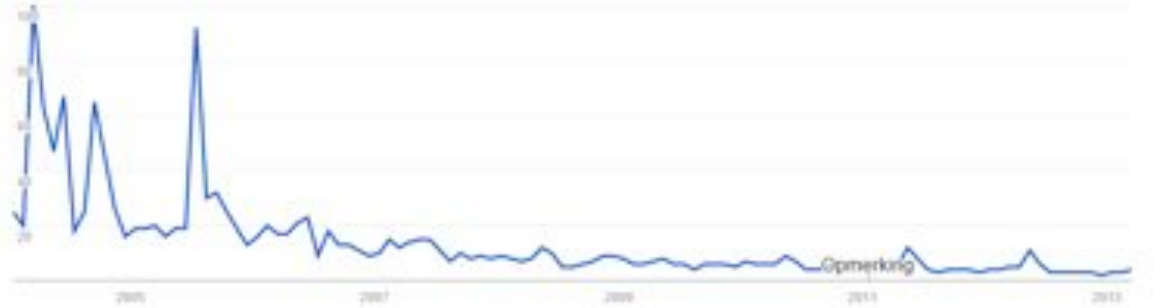

Figure 9 (above): The frequency with which the term 'terrorismo' was entered by Italian users into the Google search engine (2005-present).

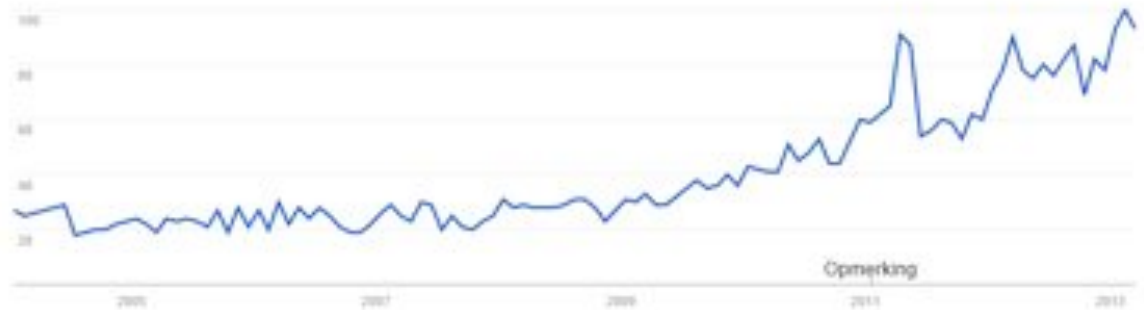

Figure 10 (above): The frequency with which the term 'vita privata' was entered by Italian users into the Google search engine (2005-present).

France

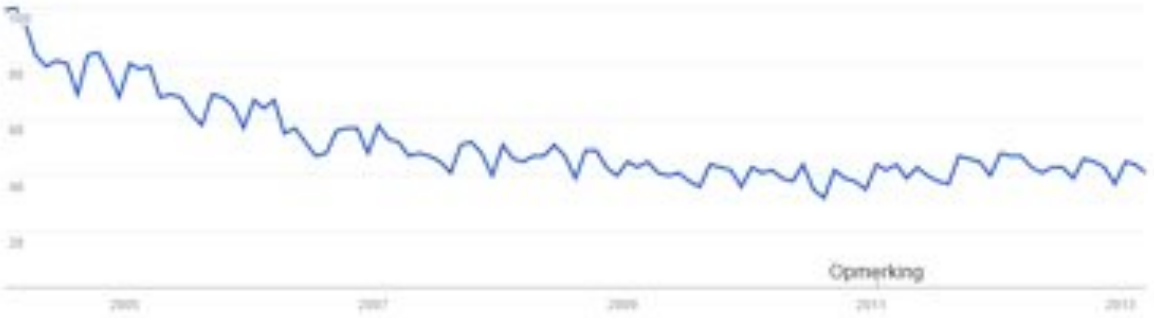

Figure 11 (above): The frequency with which the term 'sécurité' was entered by French users into the Google search engine (2005-present).

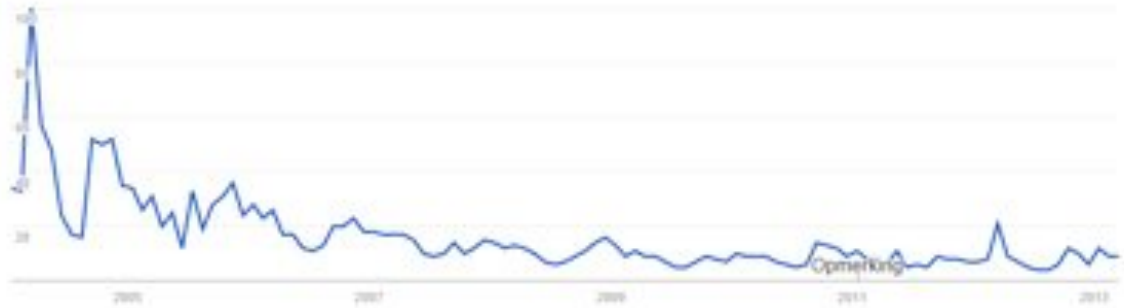

Figure 12 (above): The frequency with which the term 'terrorisme' was entered by French users into the Google search engine (2005-present).

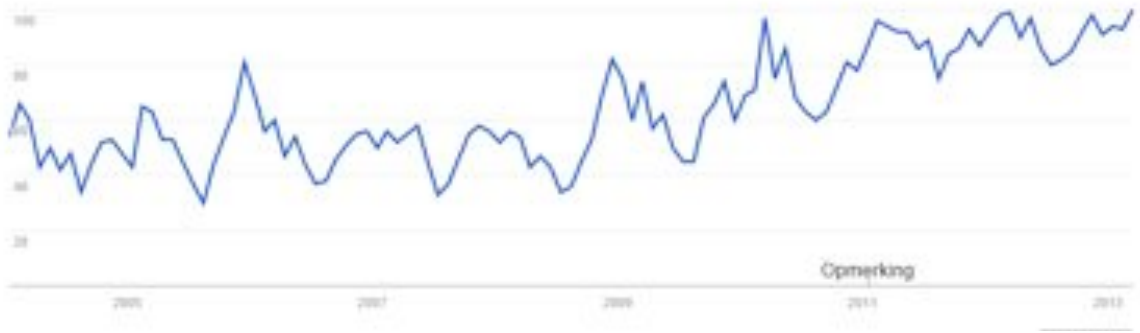

Figure 13 (above): The frequency with which the term 'vie privée' was entered by French users into the Google search engine (2005-present).

In all four countries the interest in the term 'security' seems to have decreased between 2005 and 2009 and stabilized between 2009 and 2013 (in one countries, France, it slightly increased over the past few years). In addition, in all four countries the interest in the term 'terrorism' appears to have significantly decreased between 2005 and 2009 and stabilized between 2009 and 2013. Compared to the interest in the term 'security', the interest in the term 'terrorism' in the four countries seems to be more irregular (the 'terrorism' graphs of the four countries demonstrate more peaks and troughs than the 'security' graphs). The fact that the 'terrorism' search trends are less stable may be explained by the broader (and thus more regular) use of the term 'security'. The search graphs on the term 'privacy' are difficult to interpret, with at least of two countries; Sweden and Romania showing extreme irregularities (wide variations between 0 percent to 100 percent of the search volume). This may be explained by a low absolute number of searches on a topic, which makes that a slight absolute increase of searches is presented in the graph as a huge relative increase. The public interest in security and privacy in Romania is particularly difficult to grasp and to interpret by these menas given the multiple meanings of words such as "securitate" (security) and "siguranta" (safety).
As for France and Italy, the 'privacy' graphs show from 2009 onwards a gradual and steady increase in the interest of citizens in the subject.

9.6 NARRATIVE DESCRIPTION OF THE SECURITY AND PRIVACY DISCOURSE

Combating terror
The security and privacy discourse at European Union level has been highly influenced by critical incidents such as 9/11 and the London and Madrid attacks. Of these incidents, 9/11 may have been the most influential as it gave rise to new definitions and metaphors such as "terrorist offences" and "combating terror". An important document which reflects the overall sentiment of the European Council shortly after the 9/11 attacks, are the minutes of its extraordinary meeting on 21 September 2001[348]. In this document, the European Council conveys the perceived sense of urgency to take security measures, and states that the "*fight against terrorism will, more than ever, be a priority objective of the European Union*." The European Council demonstrates their solidarity with the US in stating to be totally supportive of the American people and interpreting the attacks as "*an assault on our open, democratic, tolerant and multicultural societies*." In this sense, the 9/11 attacks are framed as an attack on all Western democratic states, including EU Member States. Moreover, several terms and story lines used in the document seem to be adopted from documents and statements of the

[348] EU Council, Conclusions and Plan of Action of the extra-ordinary European Council meeting on 21 September 2001, Brussels, SN 140/01.

Bush administration. Terms such as the "fight against terrorism" and statements such as "*the actions must be targeted and may also be directed against States abetting, supporting or harbouring terrorists*" had been previously used by the Bush administration and were reproduced by the Council. In the minutes, the Council declares determination in taking actions to combat terrorism; it shows that it wants to act rapidly, visibly and decisively. Five key actions were formulated during the meeting: (a) enhancing police and judicial cooperation (e.g. through a European arrest warrant and the adoption of a common definition of terrorism), (b), the development of international legal instruments, (c) putting an end to the funding of terrorism, (d) strengthening air security and (e) coordinating the European Union's global action.

In the months following the publication of the proposed action plan of the European Commission, the EU's security dialogue was increasingly shaped by the debates in the European Parliament (EP). Several debates reflect a general support for the actions formulated by the Council. The debates however also show a growing criticism among Members of Parliament (MEPs) on the precise implementation and application of the actions. For example, the EP's debate of 6 February 2002[349] on the Council Framework Decision on Combating Terrorism[350] reveals that, although the majority of parties in the EP supported the decision to introduce an European arrest warrant[351], some of the MEPs pointed to the (potential) disregard of the European Council and the Bush administration for basic democratic freedoms. However, the discourse on the balance between security and fundamental freedoms seemed to be quite ambiguous. Whereas some MEPs stated that the counter-terrorism measures proposed by the Council were a prerequisite for safeguarding fundamental freedoms[352], others stated that the measures formed a threat for fundamental freedoms. When taking a closer look at the debate it would appear that while some MEPs implied that the detection and arrest of (potential) terrorists is needed for citizens e.g. in order to enable them to express freely their (Western) opinions others stated that the detection and arrest could be unjustly directed towards a (broad) group of citizens who oppose established institutions. In other words, the main question on which MEPs disagreed was the extent to which existing institutions should gain more power to detect and arrest a broader group of suspects.

This discussion on the extension of law enforcement powers is closely related to the question on how the actors directly involved framed and applied the term "terrorism". The 9/11 attacks caused the European Council to develop a generic definition of "terrorist offences" in its Framework Decision on combating terrorism. According to the Council, a generic definition of "terrorist offences" was needed in order to create a European judicial space in which Member States could respond in a more coordinated fashion to (potential) terrorist attacks. The Council defined "terrorist offences" as offences which "*are committed by an individual or a group against one or more countries, their institutions or people with the aim of intimidating them and seriously altering or destroying the political, economic, or social structures of a country*". This definition focuses on and criminalizes the 'serious' disordering

[349] European Parliament, Debate on Combating terrorism, 3-030 3-064, sitting of Wednesday, 6 February 2002.
[350] European Council, Council Framework Decision on combating terrorism, 2002/475/JHA, OJ L164, 22.6.2002, 13 June 2002, p.3.
[351] 14867/1/01 – C5-0680/2001 -2001/0215 (CNS).
[352] For instance one MEP: "*There is no greater risk to the freedom of thought, of expression and to the right of life itself, than violence expressed through terrorism*" Another MEP: "*Mr President I too feel that, in adopting the Watson report, we will be taking a step forwards in the creation of that area of freedom security and justice […]*". And another MEP: "[…] *we are rejecting a text […] which in the name of the fight against terrorism merely seeks to place the most basic democratic freedoms in jeopardy throughout the world […]* ".

of a society. However, what should be understand by 'serious' (and thus the gradation of several types of disruption of a society) remains unclear. Furthermore, the EP debates indicate that some measures which would in effect go beyond this definition (which were not only directed to individuals/groups whose intention is to disrupt a society but to a broader group of potential criminals) were presented by the European Council and/or Commission as anti-terrorism measures. In this sense, notion "terrorism" has in some instances been stretched. In the EP debate on combating terrorism, the European arrest warrant was for instance presented by the European Council as a measure to arrest potential terrorists, while the list of offences (article 2/2) included offences which could not be related directly to the definition of terrorist offences as formulated by the same Council (such as fraud, murder, racism, corruption, illicit trafficking in drugs)[353]. Some of the MEPs pointed to this discrepancy while stating that under the pretext of combating terrorism, the European arrest warrant provided a basis for arresting suspects for a far broader range of offences[354]. This example shows that in some instances incidents such as 9/11 were used as political momentum to achieve or speed up other goals (e.g. creating a European judicial area), all under the label of the "fight against terrorism".

Another major theme during several debates in the EP on combating terrorism, which was weaved into the dialogue concerned the perceived democratic deficit at the European level. Several MEPs pointed to the lack of influence of the EP on defining the "terrorist" problem and related solutions. One MEP for instance stated[355]: "*Mr President, the Council should realize that it is heading for a great row if it carries on as in its complex package of 27 December, making legal definitions of who is a terrorist without any democratic scrutiny*". And another MEP[356]: "*To get back to the debate, the European Parliament is, at last, going to vote on two fundamental issues: combating terrorism and the European arrest warrant. Of course, this vote is only a sort of belated attempt to comply with bureaucratic procedures in respect of decisions which have actually already been taken*". And another MEP[357]: "*Mr President, the European arrest warrant that is before us is an unqualified political, legal and procedural sham. It is a procedural sham because the framework decision is already prepared and drafted*." In line with this, another MEP[358]: "*Mr President, this is one of the most illiberal and dishonest measures ever to come out of the EU, one with potentially enormous consequences. It has nothing to do with citizens' freedoms and rights, and everything to do with a monstrous power-grab by Brussels*." Here the discussion is not about the content of the perceived problem but about the procedures. MEPs repeatedly stressed the perceived limitations to exert influence on policies concerning the fight against terrorism. This perceived limited influence in the security and privacy debate has been endorsed by

[353] European Council, Framework Decision on the European arrest warrant and the surrender procedures between Member States, 2002/584/JHA, 13 June 2002.
[354] One of the MEPs: "It is also a sham in substance, because its original purpose was to combat terrorism following the attacks of 11 September. In reality, the scope of the future arrest warrant was widened to include 32 offences, which means two things. The first is that we are proposing to change from using a system of extradition between States, which guarantees individual freedoms, to a single legal system, without the representatives of the people being involved in this change. The second is that, on the pretext of combating terrorism, the European arrest warrant will provide the basis for cracking down on the convictions that are included on the list in question. In the future, for example, for having criticised an immigration policy that a judge supports, or having declared one's national preference in one's country, or for having expressed an opinion that is deemed politically or historically incorrect, a patriot could be expelled from his country, arrested, and transferred to another country that has an unfamiliar language and legal system."
[355] European Parliament, Debate on Combating terrorism, 3-030 3-036, sitting of Wednesday, 6 February 2002.
[356] Ibid.
[357] Ibid.
[358] Ibid.

some scientists. Moreover, various scientists[359] stated that the European Commission did not had much influence in shaping the security discourse either as this discourse was highly influenced by the United States which applied unilateral and forceful norm advocacy. In particular, the discourse on the Passenger Name Records (PNR) reveals the power relations underlying the discourse. The PNR debate will be described in the following section.

Passenger Name Records

In the aftermath of 9/11, the Bush administration launched the US Aviation and Transportation Security Act (19 November 2001)[360], which requested that airlines flying from or through the United States share, before every departure, their passenger name records (PNR) data with the US Customs and Border Protection Bureau (CBP) and the Transportation Security Administration (TSA, Argomaniz, 2010:121). However, an important barrier for the implementation of this measure was the EU's Data Protection Directive 95/46/EC which impeded the transfer of EU citizen's data to the US as the required level of protection could not be ensured by the US. Subsequently, the US started a dialogue with the European Commission about the exchange of PNR. In this PNR dialogue between the US and the European Commission (Department of Justice and Home Affairs), the US seemed to play a dominant role. The US authorities announced their measure without discussion with European authorities about the content of the measure. The transmission of air passenger data to the US had never been on the agenda of the European Commission before (Argomaniz, 2010:123) and had not been mentioned in the section 'strengthening air security' action plan on combating terrorism[361]. Moreover, a study by Rees shows (2006:97) that the US used coercive means to force countries (including the EU) to comply with their measures; the US would be unwilling to provide countries with access to their territory unless they implemented the same security measures as the US. In other words, if the European Commission would not show its willingness to discuss PNR exchange, this could result in a severe disruption of transatlantic travel and trading.

The then European Commissioner for Internal Market and Services Bolkestein stated in a response to EP questions on the PNR exchange[362]*: "The Commission has taken the issue up with the United States side on several occasions since the publication of the implementing rules, which, after one postponement, entered into force on 5 February 2003. However, as a result of the démarches by the Commission, the United States' Customs agreed to waive the imposition of penalties on non-complying airlines until 5 March 2003. These penalties include severe fines and even the withdrawal of landing rights. In order to reconcile United States' requirements with the requirements of data protection law in the Union, a meeting took place on 17 and 18 February 2003 between senior officials of the Commission and the United States' Customs Service. As a result of those discussions, the two sides issued a Joint*

[359] E.g. Argomaniz, 2010.

[360] ATSA, Publ.L. 107-71, November 19, 2001.

[361] European Council, Conclusions and plan of action of the Extraordinary European Council meeting on 21 September 2001. On page 3 under the heading "Strengthening air security" it is stated: "The Europen Council calls upon the Transport Council to take the necessary measures to strengthen air transport security at its next meeting on 15 October, These measures will cover in particular: classification of weapons; technical training for crew; checking and monitoring of hold luggage; protection of cockpit access; quality control of security measures applied by Member States. Effective and uniform application of air security measures will be ensured in particular by a peer review to be introduced in the very near future."

[362] Answer of Mr Bolkenstein on 21 March 2003 to written question P-0602/03 by Joaquim Miranda (GUE/NGL) to the Commission on 25 February 2003.

Statement[363] *which sets out the steps that need to be taken to reach a mutually satisfactory solution that can provide legal certainty to all concerned. In particular, both sides agreed to work together towards a bilateral arrangement under which the Commission, in response to information and undertakings provided by the United States side about the way transferred data would be handled and protected in the United States, may take a decision under Article 25.6 of the Data Protection Directive*[364]*, on the adequacy of the level of protection ensured by the United States. Following the adoption of such decisions, Member States must take the necessary measures to comply."*

In October 2002, the Article 29 Data Protection Working Party (which consists of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission) issued an opinion in which it concluded that compliance with the US requirements by the Airlines would create problems in respect of Directive 95/46/EC on data protection[365]. Subsequently, on 13 June 2003, the Working Party published its opinion on the extent to which the US PNR measures complied with the European Directive on data protection[366]. The Working Party stated that the "*fight against terrorism is both a necessary and valuable element of democratic societies. Whilst combating terrorism, respect for fundamental rights and freedoms of the individuals including the right to privacy and data protection must be ensured*". Interestingly, in its statement the Working Party does not present security and privacy as a trade-off concept but stresses that both goals should be reached at the same time. According to the Working Party, PNR can be transferred when adequate safeguards are afforded, among which: transitional nature of an adequacy finding by the Commission, proportionality (e.g. type of data, retention dates), adequate method of transfer (e.g. push or pull data), limited purposes (limited to terrorism, no other serious criminal offences), effective enforcement of data subjects' rights and independent third-party supervision. The Working Party concluded that the Commission should establish a clear legal framework for the transfer of PNR in a way which would be compatible with data protection principles.

Based upon the published opinion of the Working Party, a fierce discussion emerged between the EP and the Commission on PNR data transfer with the US. On 13 March 2003, the EP adopted a critical resolution on the transfer of personal data by airlines in the case of transatlantic flights in which it stated (among others) that it regrets the *"failure of the Commission, given its role as guardian of the Treaties and Community law"*, and that the *"agreement between the US and Commission (joint declaration of 19 February 2003) lacks any legal basis and could be interpreted as an indirect invitation to authorities to disregard Community law"*[367]. The EP called upon the Commission to examine the legal problems. Throughout 2003, the EP (and the Working Party thought its opinions)[368] repeatedly urged the

[363] available on the Commission's website on: http://www.europa.eu.int/comm/external_relations/us/intro/pnr.htm

[364] Directive 95/46/EC of the 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 of such data, OJ L 281, 23.11.1995.

[365] Working Party on "transmission of Passenger Manifest Information and other data from Airlines to the United States", Opinion 6/2002, WP 66 of the Working Party, 24 October 2002.

[366] Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 11070/03/EN, WP78, Brussels, 2006.

[367] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2003-0097+0+DOC+XML+V0//EN

[368] Refered to on 29 January 2004 by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data in Article 29 of Directive 95/46/EC; also refered to on 17 February 2004 by the committee in Article 31 of that Directive.

Commission to renegotiate and strengthen the privacy requirements for PNR exchange. The incorporation of the opinions of the EP and Working Party into the Commission's proposals seem to have been limited. Only few of their recommendations can be traced back in the documents of the Commission. The Commission drafted a Decision in February 2004 declaring that the "Undertakings" (i.e. the proposed and negotiated agreement) provided by the US for access to PNR "are adequate"[369] under EC law (Article 25.6 of the 1995 Data Protection Directive.[370] It is stated in this draft Decision that: "*The US is a democratic country, governed by the rule of law and with a strong civil liberties tradition. The legitimacy of its law-making process and strength and independence of its judiciary are not in question. Press freedom is a further strong guarantee against the abuse of civil liberties. […] The Community is fully committed to supporting the US in the fight against terrorism. The Community should not interpret and apply its own rules in a way incompatible with this commitment or raise obstacles to US measures to protect its own borders unless these are clearly dictated by the law of the Community or the European Union*". In other words, according to the Commission, the fact that the counterpart is the US administration could in itself be a guarantee of high data protection standards.

In March 2004, the dialogue between the Commission and the EP reached a dead-lock as the Commission kept stating that the US-EU PNR agreement complied with Community law, whereas the majority of MEPs stated it would be a violation of Community law. On 31 March 2004 the EP adopted a new resolution which sought to refer the agreement to the European Court of Justice[371]. The key points of the Resolution were that according to the (majority of members of the) EP the Commission exceeded its executive powers in drafting the Adequacy Findings decision, it called upon the Commission to withdraw the draft decision, it reserved the right to appeal to the Court of Justice should the draft decision be adopted by the Commission and it reminded the Commission of the requirement for cooperation between institutions which is laid down in Article 10 of the Treaty. In other words, instead of a dialogue on the content of the PNR agreement the discourse shifted (again) towards a discussion on procedural matters.

In a debate previous to the EP voting on the Court's opinion, a large majority of MEPs claimed the agreement to be a serious violation of the fundamental right of European citizens to data protection. Several MEPs suggested the Commission should again negotiate the agreement and achieve a regulation with which terrorism could be combatted effectively while, at the same time, privacy legislation would be respected. According to them more guarantees for European citizens could be established, for instance by[372]: (a) specifying the data which could be legitimately transferred without risk (the Working Party suggested 19 items on 13 June 2003 referred to in Article 29 of Directive 95/46/EC1), (b) replacing the 'pull' system (which has no filters for sensitive data or for non-transatlantic flights) with the 'push system' (which enables airlines to transfer only legitimate data and only in respect of

[369] Art. 25 of the Data Protection Directive (95/46/EC) establishes that the transfer of personal data to a third country may only take place if the third country ensures an adequate level of protection. The Adequacy Finding decision of the Commission stated that the protection of data offered by the US is (according to the Commission) "adequate". A list of unilateral US undertakings was annexed to the decision.

[370] Draft Commission Decision, of […], on the adequate protection of personal data contained in the PNR of air passengers transferred to the Uniged States'Bureau of Customs and Border Protection (text with EEA relevance, 2004/…/EC).

[371] European Parliament, Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (2004/2011(INI)), 2004P5_TA-PROV(2004)0245, 31 March 2004.

[372] Ibid.

flights to US destinations), (c) negotiating an international agreement with the US which will offer genuine guarantees for passengers or, at the very least, the same protection as is afforded to US citizens. One of the major problems, according to some MEPs, was that whereas US citizens were protected by the US Privacy Act, European citizens were not protected at all as the US Privacy Act stated to be only applicable to US citizens. Other problems perceived by MEs were that the US did not have a data protection law which could protect European citizens and that the US could decide to share PNR data with other (third) countries.

There were two parties within the EP however, the European People's Party and the European Democrats (PPE-DE), which were of opposite opinion and framed the EU-US PNR agreement as a "this or nothing" dilemma. According to them the agreement was the best result the EU would be able to achieve in their negotiations with the US. One MEP for instance stated[373]: *"If the Americans do not get by this route the information they require, they will obtain it by other means, whether this involves questioning at the border, mandatory visas or interviews in Consulates-General. […] if we do not get this agreement, our citizens will be in no better a legal position as regards data protection; indeed they will be in a worse one, because we will have no influence whatever on what the Americans do with the data they obtain*." In addition, PPE-DE emphasized the need to act quickly which would not leave room for much discussion[374]: "*the […] opinion of the Court […] will only postpone the signing of the agreement and leave a legal vacuum in place in relation to the treatment of personal data by the US authorities […] We also believe, naturally, that this agreement can be improved but also that the fight against terrorism and cooperation with third countries in the field, with the US in this case, is a priority for the European Union. […], we need the agreement now […]*."

Like in many other debates, in the PNR debate prior to the voting on the referral to the Court, the perceived democratic deficit was recurrently being put forward by MEPs. Moreover, it seems that the PNR dialogue was – from the MEPs' perspective - supportive to the parallel discussion on the influence of the EP in the sense that some MEPs used the PNR debate to expose and stress the perceived power asymmetry between the EP and Commission. One of the MEPs for instance stated during the PNR debate about the EU-US agreement: "*There is a huge democratic deficit when the Commission comes forward with a proposal like this and does not give either the EP or national parliaments the chance to say yes or no*"[375]. Another MEP stated: "*it is indisputable, Commissioner Bolkestein, that by not entering into a real international agreement with the US, the Commission, has chosen to bypass Parliament's opinion. The fact that you have opted for a soft law instead of a real agreement already speaks volumes about the Commission's intentions to exclude democratic control of this agreement, and I find this particularly worrying*". And another MEP implied by her statement that with the recourse of the agreement to the Court of Justice the EP could show its legitimacy as a representative body: "*We in the House should now also demonstrate that we know how to stand up for our citizens and not be put under pressure by anybody*". In sum, the referral of the agreement to the Court of Justice was framed as a 'last resort' measure by MEPs to gain influence in the PNR debate and, at the same time, provided an opportunity for MEPs to stress perceived power inequalities and demonstrate their decisiveness to use all means to exercise their tasks as political representatives of European citizens.

On 21 April 2003, the EP voted to take the Commission to the Court of Justice for opinion under Article 300(6) over the proposed EU-US agreement to exchange PNR data (276 voted

[373] European Parliament, Sitting of Monday, 19 April 2004, l-037
[374] European Parliament, Sitting of Monday, 19 April 2004, l-043
[375] European Parliament, Sitting of Monday, 19 April 2004, l-039

in favour, 260 against, 13 abstentions). Fearing a Court ruling against the agreement, the Council demanded that the EP vote again, while applying the "urgency procedure"[376]. Having lost previous votes in the Parliament on the PNR agreement, the Council hoped that it could make use of the situation where 162 non-elected observers to the Parliament from the new Member States had gained member status for one single session, extending the plenary session to 788 members. By bringing forward the urgency request, the Council tried to change the former votes (which had a slight majority of 16 in favour of referring the agreement to Court). Yet, the EP voted against the Council's request for the urgency procedure (301 in favour, 343 against and 18 abstentions). Despite this repeated and clear "no" from the EP, the General Affairs Council of the EU meeting in Brussels (17 May 2004) adopted the EU-US international agreements which obliged European airlines to give access to PNR data to US agencies. This decision annulled the case that the EP had sent to the Court of Justice for an opinion on the legality of the agreement. However, the MEPs Graham Watson and Johanna Boogerd-Quaak called for the EP to exercise its rights under Article 230 of the EC Treaty to seek the annulment of both the EU-US agreement and the Adequacy Finding decision. The then EP president Pat Cox thereupon decided to adopt this request and appeal to the Court of Justice, on behalf of the EP. In an interview Pat Cox stated: "*This decision was taken after widescale consultation and reflects the concern felt by a large majority in the European Parliament on the need to defend European citizens' fundamental rights and freedoms. While naturally accepting that the US Administration is perfectly free to exercise its sovereign right to protect its own homeland, both the EU and the US must guard against a new form of creeping extra-territoriality. This issue must be addressed in the context of EU-US dialogue*."

On 22 November 2005, the Advocate-General of the European Court of Justice delivered its opinion on the court case[377]. Both the EU-US PNR agreement and the Adequacy Finding decision were annulled by the Court of Justice as their subject-matter was perceived by the Court to fall outside the scope of the data protection directive. According to the Court, the PNR data exchange essentially concerns the processing of data by law enforcement authorities, which should be covered by national bilateral agreements or by a EU third-pillar agreement with the US. In this sense, one could argue that the EP won a "pyrrhic" victory; the agreement and decision were annulled, but were referred to actors and procedures in which the EP had less influence. In the years following upon the court ruling, the same discussions seemed to have taken place between the EP and the Commission. In 2007 and 2012 new agreements between the EU and US were established. The agreements and the debates demonstrate an on-going struggle between the EP and the Commission, and between the Commission and the US authorities on the precise guarantees for PNR exchange. However, from 2009 onwards, the security and privacy discourse seem to have taken a turn in the sense that a growing discourse coalition emphasised the importance of the data protection of European citizens beyond the EU borders. This shift may be best revealed by looking at the

[376] The Council may ask the European Parliament to deliver its opinion under the urgency procedure laid down in Article 112 of the European Parliament's Rules of Procedure.

[377] European Court of Justice, Case C-317/04, EP versus Council of the European Union, Protection of individuals with regard to the processing of personal data – action for annulment – Council Decision 2004/496/EC – Agreement between the European Community and the United States of America on the processing and transfer of PNR (Passenger Name Records) data), Case C-318/04, European Parliament versus Commission of the European Communities, action for annulment – Commission Decision 2004/535/EC on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection – Directive 95/46/EC, 22 November 2005.

Stockholm Programme which was launched in May 2010 and which has as main aim to establish an open en secure Europe while serving and protecting citizens[378].

The Stockholm Programme

EU legislation covers 32 subject areas, one of which is 'Justice, Freedom and Security'. The Stockholm Programme sets out the European Union's (EU) priorities for this subject area for the period 2010-2014 and builds on the Tampere and Hague programmes[379]. The aim of the Stockholm programme is to meet future challenges and further strengthen the area of justice, freedom and security with actions focusing on the interests and needs of citizens[1]. Thus by its primary aims the programme captures both sides of the security-privacy debate.

A discourse analysis of the Stockholm programme is not the most dynamic of analyses because, in contrast to the debates in the aftermath of 9/11 en the PNR discourse, the Stockholm programme has only sparsely been a subject of debate in the European Parliament. The outlines of the Stockholm programme were first communicated in June 2009 [380] and stated that "*The main thrust of the new programme will be 'building a citizen's Europe'.* And that *'All action taken in the future should be centred on the citizen[..]'.* The formulation used by the Commission to state the primary aims of the programme raise some interesting questions. 'Building a citizen's Europe', to start with, logically implies that Europe as it is today is *not* a citizen's Europe, for if it was we would not need to build one. Furthermore, stating that 'in the future all actions should be centred on the citizen' hints in the same direction; apparently actions up till then had not been centered (enough) on this citizen. It is not very likely that the authors intended to convey the message that Europe is not a citizen's Europe, but rather aimed to connect their statements to fit a public consensus or at least a popular opinion held among EU officials. This could be the opinion that 'the European citizen' had not been sufficiently the focal point of earlier efforts, in general or in particular within the 'Justice, Freedom and Security' subject area.

Specifically regarding privacy and security the Communication states that *'The area of freedom, security and justice must above all be a single area in which fundamental rights are protected, and in which respect for the human person and human dignity, and for the other rights enshrined in the Charter of Fundamental Rights, is a core value. For example, the exercise of these freedoms and the citizen's privacy must be preserved beyond national borders, especially by protecting personal data; […] and citizens must be able to exercise their specific rights to the full, even outside the Union'.* The fact that 'privacy beyond national borders […] even outside the Union' is put forward as an example may illustrate that this has been an issue[381] in the period preceding the publication of this communication and states that 'privacy' should be a focal point of the more generic goals. Issues around the sharing of passenger information and bank transfers between the EU and the United States may lie at the basis of this example. Interestingly, 'privacy' as a concept is narrowed down to the protection of personal data as the communication states that '*The Union must secure a new comprehensive strategy to protect citizens' data within the EU and in its relations with other countries.'* The legal principles at stake however are the right to privacy *and* the right to data protection; two concepts that converge or diverge depending on the debate and the country in

[378] European Council, The Stockholm Programme – An open and secure Europe serving and protecting citizens, Official Journal of the European Union, C 115/1, 4.5.2010, Brussels, 22 November 2005.
[379] http://europa.eu/legislation_summaries/sitemap/index_en.htm
[380] Com (2009) 262 Final.
[381] As is illustrated by the discourse on PNR.

which they are under analysis[382]. With the scope of the Stockholm programme, and for the sake of clarity, the two concepts are perhaps best kept conceptually distinct as a narrow focus on data protection may hamper privacy protection. In relation to security the Communication states that "*It must also foresee and regulate the circumstances in which public authorities might need to restrict the application of these rules [regarding data protection] in the exercise of their lawful duties'*. This statement calls the trade-off between privacy and security but this trade-off is not explicitly addressed further in the document. Finally, technological developments are apparently seen as key source of privacy violations for they may warrant further legislative or non-legislative initiatives to maintain the effective application of the principles: purpose, proportionality and legitimacy of processing, limits on storage time, security and confidentiality, respect for the rights of the individual and control by an independent authority[383].

In November 2009, the Centre for European Policy Studies (CEPS) wrote the so-called INEX[384] policy brief discussing border security and the role of technology herein, in relation to the Stockholm programme. In the introduction, the authors noted that despite the emphasis that is put on citizens' freedoms and rights, and on the protection of their personal data and privacy, '*the [Stockholm] programme remains overtly oriented towards the reinforcement of the reliance on technology within the context of EU security policies, particularly computerised systems of information exchange and data processing. These, in turn, are largely defined in terms of the priorities and viewpoints of security professionals'*[385]. The point made here is not that privacy and the reliance on technology are automatically in conflict, but that these technologies are asymmetrically defined and prioritized. Such an asymmetrical approach is likely to result in asymmetrical solutions and it is exactly those solutions that need to be 'patched' after implementation as they often show too little regard for 'soft' aspects such as privacy. Another issue that the authors identify is the use of the word 'citizen'. When fundamental human rights are at stake, the word citizen may not be appropriate for it distinguishes – in the current context at least - between people living in the EU and people from outside the EU. They furthermore argue that while the circumstances under which the public authorities may interfere with the exercise of fundamental citizen rights, the possible interference of *private* entities is left aside – despite the fact that private companies are increasingly involved in the management of data at the European and national level[386]. While the objections that are brought forward by CEPS certainly struck a chord and need to be considered, they may be more about semantics than the content of the Stockholm programme.

In November 2009 the Stockholm Programme was also debated in the European Parliament[387], one month before the programme was to be adopted. The general attitude towards the programme as expressed in this debate was positive and the need to continuously balance measures aimed at creating security and measures aimed at protecting the rights of individuals was often stressed. This seems to correlate with the somewhat curiously worded aim of the Stockholm programme (i.e. building a citizen's Europe) and reflects an active awareness of the trade-off that plays such a large role in the security domain. Furthermore, the

[382] CEPS, *Global Data Transfers: The human Rights Implications*, 2010, p. 3.
[383] Com (2009) 262 Final, p.8.
[384] INEX is a three-year project on converging and conflicting ethical values in the internal/external security continuum in Europe, funded by the Security Programme of DG Enterprise of the European Commission's Seventh Framework Research Programme.
[385] INEX POLICY BRIEF NO. 3.
[386] Ibid.
[387] European Parliament, Debates, report of proceedings, Wednesday 25 November 2009.

fact that this tradeoff is so often referred to, may indicate that it had not received enough attention before. This was explicitly addressed by Guy Verhofstadt (who represented the ALDE group)[388] *'the basic point here is the balance between security and freedom. It is obvious that we have to protect our citizens against terrorism and organized crime, but maybe, after 9/11, we have put too much focus on security and protection. I think that the Stockholm Programme […] has to rebalance that towards respect for fundamental rights and also more openness in society.[…] it is more ambitious than the Tampere Programme and the Hague Programme, but with a more important focus on the fundamental rights of the people.'* This remark thus presents 'terrorism' as a driver that has - understandably but perhaps unrightfully- shifted the security-freedom balance too far into the direction of 'security'. Moreover this remark could also be interpreted as a plea to tip the balance in favor of 'freedom'. Interestingly, the subject 'terrorism' is thus in a way exposed as a 'false' driver, leading towards means optimization (the means being security) while the focus should be on the fundamental ends: the wellbeing of citizens and protecting their fundamental rights. The question that is evoked of course, is whether the Stockholm programme would be successful in this realignment. Some commentators believe it would not: *The Stockholm Programme gives people fewer rights, not more, because they have no control over how the data is used. There is no sign of an end to the monitoring of passengers, the controversial subject of data protection has not yet been resolved'* [389] With this remark the issue of data protection is (re)introduced into the debate, coupled to a specific case: the sharing of flight passenger data. While having *more* rights is in itself of course a hollow shell, the issue of data protection in general apparently remains controversial in relation to the Stockholm programme.

In May 2010, CEPS published another policy brief, specifically on the topic of data transfers and human rights [390]. Although this publication does not directly concern the Stockholm programme, it does exemplify the tension between privacy and security. In this brief CEPS describes how the question of privacy rose to the top of the EU agenda at the beginning of 2010. "*On 11 February 2010, the European Parliament rejected an interim agreement prepared by the EU Council and the US authorities that would have enabled agencies in the EU to continue to provide information to their US counterparts on all electronic bank transfers in Europe. The result was that the continued supply of this information to the US authorities was no longer lawful. The US authorities issued a press release expressing their disappointment and insisting on the importance of the information for anti-terrorism measures. The reason for the European Parliament's negative vote was the potential impact of the agreement on the privacy of EU citizens. The Parliament considered that the lack of satisfactory safeguards for the right to privacy made the proposed agreement unacceptable."* Some commentators (reacted to the rejection of the Swift agreement as an '*unnecessary move, which impedes the fight against financing terrorism*' [7]. Thus the trade-off in this case is specified as one between protecting privacy and helping the fight against terrorism. What is interesting in this specific case is that the privacy of *European* citizens is set against homeland security of (particularly) the *United States*, who stood to receive the data. In that sense it was not a direct trade-off for the EU. However by using the term 'fight against terrorism', the gains for the US are framed as gains for all as terrorism is of course also a European issue. Apparently the argument failed to convince Parliament; the trump card 'terrorism' had by now somehow devaluated, as it emerged from the discussion in the parliament presented earlier in this analysis. Another indication of the shift away from security and more in favour of fundamental freedoms.

[388] Ibid., p. 10.
[389] Page 16
[390] CEPS (2010) Global Data Transfers: The human Rights Implications

9.7 GENERAL CONCLUSIONS, REFLECTIONS AND HYPOTHESES

When taking a bird's eye view of the security and privacy discourse over the years, several key observations can be made. The first may be the dominant role of the US at the onset of the discourse, which set the stage for specific security measures and influenced strongly the course of the debate. Moreover, particularly in the first years after 9/11, one could question whether one could speak of a dialogue between EU and US authorities as the reciprocity between the two actors appears doubtful. The strong statement of the Bush administration immediately after the 9/11 attacks "*either you are with us or you are against us*" indicate a polarising stance taken by the US which left hardly any room for a dialogue on how US security should be strengthened. The US were willing to take drastic measures in case the EU would not cooperate on security measure. The pressure exerted by the US yielded from the fear for new attacks within the US administration and the will to minimize uncertainty on potential future attacks. Interesting in the interchange between the US and the EU (which also indicates asymmetry) is that often it implied a limitation of the privacy of EU citizens in order to protect the security of US citizens, and not vice versa.

In the first years after the 9/11 attacks, the Commission seemed to play a dominant role in the dialogue between the EP and the Commission. In the PNR case for instance, only limited suggestions and requests of the EP were incorporated into the proposals of the Commission. The Commission found itself in the difficult position between the EP and the US; the former pressing for more privacy guarantees and the latter for more access to data. Also here, the question can be posed whether one can speak of a discussion between the EP and Commission as there was only limited exchange of thoughts on the content of PNR policy. The key message of the Commission repeatedly was that because of the urgent need for anti-terrorism measures and the strong stance of the US on PNR more privacy guarantees (than those proposed by the Commission) were not feasible. The majority of MEPs repeatedly stressed that the PNR agreements between the US and EU would violate Europeans' fundamental rights. Instead of a dialogue in which relevant actors would build upon each other's' arguments, in the PNR debate between the EP and the Commission the actors involved mainly seemed to repeat their viewpoints. This deadlock between the actors involved may have also been caused by a parallel discourse on the perceived lack of influence by MEPs. Several MEPs found the influence of the EP on EU decision-making too limited (which they labelled as "democratic deficit") and used the PNR debate to demonstrate and stress the perceived democratic deficit.

Interestingly, from 2009 onwards, the security and privacy discourse seemed to take a turn in the sense that a growing discourse coalition emerged to emphasise the importance of the protection of European citizens' data beyond the EU borders. For example, the European Council's discourse on the Stockholm Programme stresses the importance of the European citizen's rights and interests and tips the freedom-security balance in favour of 'freedom'. Whereas in the wake of 9/11 'the war on terror' had a major influence on the privacy and security debate it seems as though it has lost some of its momentum in later years. The aims of the Stockholm Programme, the rejection of the SWIFT agreement, debates in the European parliament, all seem to point in the direction of rehabilitation of the citizen and his freedom(s) as focal point for policy. In the discourse (and even in today's discourse) it however remains unclear where the relevant actors draw the line between privacy and security. Security and privacy as concepts remains rather vague and privacy is often narrowed down to data protection.

9.8 HYPOTHESES FOR THE PRISMS SURVEY

Based upon the observations made in the previous paragraphs the following hypotheses can be formulated. These hypotheses should be verified through the work package 9 survey of the PRISMS project.

- The understanding of the notions 'security' and 'privacy' is predominantly shaped by a few, dominant actors.
- In the EU privacy and security discourse, the European citizen has limited influence.
- Whereas the interest of the EU citizens in 'security' declined over the past 10 years, their interest in 'privacy' increased (further operationalize this in work package 8; want to know what their precise interest is and why).
- The framing of the notions 'security' and 'privacy' is substantially influenced by incidents (can be determined by topics with high symbolic value) and may lack a more fundamental vision on these concepts.
- In today's EU privacy and security discourse, the complex notion privacy has as a strong focus on data protection
- From 2009 onwards, there has been a break with the discursive tradition (from 2001-2009) in the sense that discourses became more balanced (attention to both security and privacy)
- The security discourse has been much more institutionalized (translated into policies, rules, organisations) than the privacy discourse.

10 REFERENCES

10.1 ACADEMIC LITERATURE

Argomaniz, J., "When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms", in: Wolff, S., Wichmann, N. and G. Mounier, *The External Dimension of Justice and Home Affairs*, Routledge, New York, 2010, pp. 117-135.

Campbell, D., "Time is Broken: The Return of the Past in the Response to September 11", in: *Theory & Event*, 2002.

Catano, J.V., "Stylistics", in *The Johns Hopkins Guide to Literary Theory and Criticism*, The Johns Hopkins University Press, London, 2005.

Dryzek, J., *The politics of the earth: environmental discourse*, 2nd edition, Oxford University Press, London, 2005.

Foucault, Michel, *Madness and Civilization: A History of Insanity in the Age of Reason,* Translated by Richard Howard, Vintage Books, New York, 1965.

Foucault, Michel, *Power/Knowledge: Selected Interviews and other Writings 1972-1977*, Ed. Colin Gordon, Pantheon Books, New York, 1980.

Foucault, Michel, *The Archaeology of Knowledge,* translated by A.M. Sheridan Smith, Tavostock, London, 1972.

Foucault, Michel, *The Birth of the Clinic An Archaeology of Medical Perception,* translated by A.M. Sheridan Smith, Pantheon Books, New York, 1973.

Foucault, Michel, *The order of Things: An Archaeology of the Human Sciences*, Vintage Books, New York, 1970.

Frohmann, B. "The Power of Images: A Discourse Analysis of the Cognitive Viewpoint." , *Journal of Documentation,* 1992.

Fuchs, C., "Towards An Alternative concept of privacy", *Journal of Information, Communication and Ethics in Society*, Vol. 9, No. 4, 2011, pp. 220-237.

Hajer, M. and J. Uitermark, "Performing Authority: Discursive politics after the assassination of Theo van Gogh", in *Public Administration*, Vol. 86, nr. 1, 2007, pp. 5-19.

Hajer, M. and Laws, "Ordering through discourse", in Moran, M., Rein, M. and R. Goodin, The Oxford Handbook of Public Policy, Oxford University Press, London, 2006a, pp. 251-268.

Hajer, M., "Doing discourse analysis: coalitions, practices, meaning", in Van den Brink, and T. Metze, *Words matter in policy and planning, Discourse theory and method in the social sciences*, Labor Grafimedia, Utrecht, 2006b, pp. 65-74.

Hajer, Maarten, "Coalitions, practices, and meaning in environmental politics: from acid rain to BSE", in: Howard, D. and J. Torfing (eds.), *Discourse theory in European politics: identity, policy and governance*, Basingstoke: Palgrave Macmillan, 2005, pp. 297-315.

Hak, T. and N. Helsloot, *Michel Pêcheux, Automatic discourse analysis*, Rodopi, Amstedam, 1995.

Helsloot, N. and T. Hak, "Pêcheux's Contribution to Disourse Analysis", *Forum Qualitative Sozialforschung/ Forum Qualitative Social Research*, Vol. 8, No. 2, 2007, http://www.qualitative-research.net/index.php/fqs/article/view/242/535

Henry, P., "Theoretical issues in Pêcheux's Automatic discourse analysis (1969)", in: Hak, T. and N. Helsloot (Eds.), *Michel Pêcheux, Automatic discourse analysis*, Rodopi, Amstedam, 1995, pp. 21-40.

Hewitt, S., "Discourse Analysis and Public Policy Research", *Centre for Rural Economy Discussion Paper Series*, No 24, 2009.

House of Commons Home Affairs Select Committee, *A Surveillance Society?*, Fifth Report of Session 2009-10, HC 58-I, The Stationery Office, London, 8 June 2008.

House of Lords Constitution Committee, Surveillance: Citizens and the State, Second Report of Session 2008-09, HL Paper 18, The Stationery Office, London, 6 February 2009.

Howard, D. and J. Torfing, *Discourse theory in European politics: identity, policy and governance*, Palgrave Macmillan, Basingstoke, 2005.

Hynes, D., Michel Foucault's Archaeology of Knowledge, 2006.

Iatsko V., "Linguistic aspects of summarization", *Philologie im Netz*, No. 18, 2001.

Joint Committee on Human Rights, Legislative Scrutiny: Protection of Freedoms Bill, Eighteenth Report of Session 2010-12, HL Paper 195/ HC 1490, The Stationery Office Limited, London, 7 October 2011.

Kasper, D.V.S., "The Evolution (or Devolution) of Privacy", *Sociological Forum*, Vol. 20, No. 1, 2005, pp. 69-92.

Keller, R., "Diskurse und Dispositive analysieren. Die Wissensoziologisch Diskursanalyse als Beitrag zu einer wissenanalytischen Profilierung der Diskursforschung", *Forum Qualitative Sozialforschung*, Vol. 8. No. 2, Art. 19, 2007.

Landwehr, A., *Geschichte des Sagbaren, Einführung in die historische Diskursanalyse*, Diskord, Tübingen, 2001.

Ministry of Defence, *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security*, The Stationary Office, London, February 2012.

Pêcheux, Miche, *Analyse automatique du discours*, Dunod, Paris, 1969.

Pêcheux, Michel, "Ouverture du colloque", in Conein, B., Courtine, J., Gadet, F., Marandin, J. and M. Pêcheux, (eds.), *Matérialités discursives*, Presses Universitaires de Lille, Lille, 1981, pp. 15-18.

Pêcheux, Michel, *Les Vérités de La Police*, Maspero, Paris, 1975.

Pêcheux, Michel, Ueber die Rolle des Gedächtnisses als interdiskursives Material, *Das Argument,* Sonderband, No. 95, 1983, pp. 50-58.

Phillips N. and C. Hardy, Discourse Analysis – Investigating Processes of Social Construction, *Qualitative Research Methods,* Volume 50, SAGE Publications, Thousand Oaks-London-New Delhi, 2002.

Provost-Chauveau, G., Compte rendu de Michel Pêcheux, Analyse automatique du discours, *La Pensée*, No 151, 1970, pp. 135-138.

Rees, W., *Transatlantic counter-terrorism cooperation. The new imperative*, Routledge, Abingdon, 2006.

Sharp, L. and T. Richardson, Reflections on Foucauldian discourse analysis in planning and environmental policy research, *Journal of Environmental Policy & Planning*, Vol. 2, 2001, pp. 193-209.

Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge MA and London, 2008.

Spitzer, Leo, *Italienische Umgangssprache*, Kurt Schroeder Verlag, Bonn and Leipzig,1922.

Surveillance Studies Network, *A Report on the Surveillance Society For the Information Commissioner*, Information Commissioner's Office, September 2006.

Trognon, A., *Analyse de contenu et théorie de la signification*, dissertation, Université Paris VII, Paris, 1972.

Voloshinov, V.N., *Marxism and the philosophy of language*, Harvard University Press, Cambridge, 1973.

Winkel, G., "Foucault in the forest – A review of the use of 'Foucauldian' concepts in forest policy analysis", *Forest Policy and Economics*, No. 16, 2012, pp. 81-92.

Woezel, H. and M. Geier, "Sprachtheorie und Diskursanalyse in Frankreich", interview in *Das Argument,* No. 133, 1982, pp. 386-399.

10.2 News Reports

- NRC, 11 september 2001, Aanval op VS, Bush wil vergelding
- Volkskrant, 12 september 2001, Bush zweert wraak voor aanval
- Telegraaf, 12 september 2001, VS in staat van oorlog
- NRC, 2 november 2004, Filmmaker Theo van Gogh vermoord
- Telegraaf, 3 november 2004, Afgeslacht
- Volkskrant, 3 november 2004, Verdachte bekend bij AIVD
- NRC, 12 mei 2007, Bescherming privacy vereist meer sancties
- Volkskrant, 4 Augustus 2011, Hoe LinkedIn leden en reclame linkt
- Telegraaf, 13 augustus 2011, Bedrijven negeren privacyregels

10.3 Policy Documents

A full list of policy and other relevant documents consulted for the analysis in this chapter is provided in the supplement of this report (4.5/Netherlands and 4.2/European Union)

Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between Human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable 3.1: Draft analysis of privacy and security policy documents in the EU and US

Supplementary documentation

Authors:	Gabriela Bodea, Noor Huijboom, Sander van Oort, Merel Ooms, Bas van Schoonhoven, Tom Bakker, Livia Teernstra (TNO); Rachel L. Finn, David Bernard-Wills, David Wright (Trilateral); Charles D. Raab (University of Edinburgh)

Dissemination level:	Restricted to a group specified by the consortium
Deliverable type:	Report
Version:	1.0
Due date:	30 January 2013
Submission date:	28 March 2013

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

This document was developed within the PRISMS project (see http://prismsproject.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 (Fraunhofer ISI), co-ordinator,
- Trilateral Research & Consulting LLP,
- Dutch Organization for Applied Scientific Research (TNO),
- Vrije Universiteit Brussel (VUB),
- University of Edinburgh (UEdin),
- Eőtvős Károly Policy Institute (EKINT),
- Hogeschool Zuyd and
- Market & Opinion Research International Limited (Ipsos-MORI)

This document may be freely used, copied, and distributed provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The PRISMS partners shall take no liability for the completeness, correctness or fitness for use. This document is subject to updates, revisions, and extensions by the PRISMS consortium. Address questions and comments to: Michael.Friedewald@isi.fraunhofer.de

Document history

Version	Date	Changes
1.0	28 March 2013	

CONTENTS

1. POLICY DOCUMENTS 1

1.1 International organisations 1

1.2 European security and privacy policy documents 5

1.3 Other European policies 46

1.4 United Kingdom security and privacy policy documents 51

1.5 Netherlands security and privacy policy documents 64

1.6 France security and privacy documents 78

1.7 Italy security and privacy policy documents 91

1.8 Germany security and privacy policy documents 100

1.9 Romania security and privacy policy documents 109

1.10 USA security and privacy policy documents 110

B. SHORT ANALYSIS OF POLICY DOCUMENTS 121

1.11 International Organisations 121

1.12 European policy documents 123

1.13 UK policy documents 175

1.14 Netherlands policy documents 193

1.15 France policy documents 203

1.16 Italy policy documents 217

1.17 Germany policy documents 227

1.18 Romania policy documents 239

1.19 USA Policy documents 247

1 POLICY DOCUMENTS

1.1 INTERNATIONAL ORGANISATIONS

1.1.1 United Nations

2001

1. United Nations Security Council, Resolution 1373 (2001) on treats to international peace and security caused by terrorist acts, S/RES/1373 (2001), 29 September 2001.

2003

2. United Nations Security Council, Resolution 1456 (2003) on the issue of combating terrorism, S/RES/1456 (2003), 20 January 2003.

2004

3. United Nations General Assembly, Resolution 58/16: Responding to global threats and challenges, A/RES/58/16, 26 January 2004.

4. United Nations Economic and Social Council, Revised Draft Resolution on Genetic Privacy and Non-discrimination, E/2004/L.13/Rev.1, 19 July 2004.

2008

5. Hammarberg, Thomas, Protecting the right to privacy in the fight against terrorism, Commissioner for Human Rights, Issue Paper (2008)3, Strasbourg, 4 December 2008.

2009

6. United Nations Economic and Social Council, Principles and Guidelines on Confidentiality Aspects of Data Integration Undertaken for Statistical or Related Research Purposes, ECE/CES/2009/3, 27 March 2009.

7. Scheinin, Martin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, United Nations Human Rights Council, A/HRC/13/37, 28 December 2009.

2010

8. United Nations General Assembly, Resolution 64/211: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, A/RES/64/211, 17 March 2010.

2011

9. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Gov-*

ernmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Disarmament Study Series 33, United Nations, New York, December 2011. [Includes appendices containing background relevant UN Resolutions]

10. United Nations General Assembly, Resolution 66/63: Strengthening of security and cooperation in the Mediterranean region, A/RES/66/63, 13 December 2011.

2012

11. United Nations General Assembly, Resolution 66/171: Protection of human rights and fundamental freedoms while countering terrorism, A/RES/66/171, 30 March 2012.

1.1.2 Organization for Economic Cooperation and Development

2002

12. Organisation for Economic Cooperation and Development (OECD), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Recommendation of the Council, Paris, adopted 25 July 2002. www.oecd.org/dataoecd/16/22/15582260.pdf

2006

13. Organisation for Economic Cooperation and Development (OECD), *The Development of Policies for the Protection of Critical Information Infrastructures (CII)*, DSTI/ICCP/REG(2006)15/FINAL, OECD, Paris, 2006.

2007

14. Organisation for Economic Cooperation and Development (OECD), *Malicious Software (Malware): A Security Threat to the Internet Economy*, Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL, OECD, Paris, 2007.

15. Organisation for Economic Cooperation and Development (OECD), *The OECD DAC Handbook on Security System Reform (SSR): Supporting security and justice*, OECD, Paris, 2007. http://www.oecd.org/dataoecd/43/25/38406485.pdf

2008

16. Organisation for Economic Cooperation and Development (OECD), *The Future of the Internet Economy: A Statistical Profile*, OECD, Paris, 2008.

17. Organisation for Economic Cooperation and Development (OECD), Recommendation of the Council on the Protection of Critical Information Infrastructures, C(2008)35, OECD, Paris, 2008.

2011

18. Sommer, Peter, and Ian Brown, *Reducing Systemic Cybersecurity Risk*, OECD/IFP Project on "Future Global Shocks", OECD, Paris, 14 January 2011.

19. Organisation for Economic Cooperation and Development (OECD) "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", *OECD Digital Economy Papers*, No. 186, OECD Publishing, Paris, 23 Nov 2011. http://dx.doi.org/10.1787/5kg1zqsm3pns-en

1.1.3 North Atlantic Treaty Organisation (NATO)

2002

20. North Atlantic Treaty Organization (NATO), Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic, 21 November 2002. http://www.nato.int/cps/en/natolive/official_texts_19552.htm?selectedLocale=en

2006

21. North Atlantic Treaty Organization (NATO), *Comprehensive Political Guidance*, 29 November 2006.
http://www.nato.int/cps/en/SID-F1C88E7B-C0242A61/natolive/official_texts_56425.htm

2008

22. North Atlantic Treaty Organization (NATO), *Defending against cyber attacks*, 2008.
www.nato.int/issues/cyber_defence/practice.html

2009

23. North Atlantic Treaty Organization (NATO), Declaration on Alliance Security: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg / Kehl on 4 April 2009, 4 April 2009. http://www.nato.int/cps/en/natolive/news_52838.htm

2010

24. North Atlantic Treaty Organization (NATO), *Active Engagement, Modern Defence: Security Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, NATO Public Diplomacy Division, Brussels, Belgium, 18-19 November 2010.
http://www.nato.int/cps/en/SID-1E6BF7FC-AB8DCA17/natolive/topics_82705.htm

2011

25. North Atlantic Treaty Organization (NATO), *Defending the Networks: NATO policy on cyber defence*, 4 October 2011. http://www.nato.int/cps/en/natolive/75747.htm

26. North Atlantic Treaty Organization (NATO), *NATO's role in Energy Security*, 26 Oct 2011. http://www.nato.int/cps/en/natolive/topics_79941.htm

27. North Atlantic Treaty Organization (NATO), Briefing: Countering Terrorism, Brussels, 2011. http://www.nato.int/cps/en/natolive/topics_50313.htm

2012

28. North Atlantic Treaty Organization (NATO), Briefing: Tackling New Security Challenges, Brussels, 31 January 2012. http://www.nato.int/cps/en/natolive/topics_82708.htm

1.1.4 International Conference of Data Protection and Privacy Commissioners

2007

29. 29th International Conference of Data Protection and Privacy Commissioners, Resolution on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes, Montreal, 26-28 September 2007.

2008

30. 30th International Conference of Data Protection and Privacy Commissioners, Draft Resolution on Privacy Protection in Social Network Services, Strasbourg, 17 October 2008. http://www.privacyconference2011.org/htmls/adoptedResolutions/2008_Strasbourg/2008_E5.pdf

2009

31. 31st International Conference of Data Protection and Privacy Commissioners, *Joint Proposal on International Standards for the Protection of Privacy with Regard to the Processing of Personal Data*, Madrid, 5 November 2009. http://www.privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf **[part of short analysis]**

2011

32. 33rd International Conference of Data Protection and Privacy Commissioners, Resolution on The Use of Unique Identifiers in the Deployment of Internet Protocol Version 6 (IPv6), 2011/IWGDPT/RES/001, Mexico City, 2-3 November 2011. http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_IWGDPT_RES_001_Intnt_Prot_ENG.pdf

1.1.5 International Telecommunication Union (ITU)

2009

33. Ghernaouti-Hélie, Solange, *Cybersecurity Guide for Developing Countries*, Enlarged edition, ITU, Geneva, Release 2009. http://www.itu.int/ITU-D/cyb/publications/index.html

1.2 EUROPEAN SECURITY AND PRIVACY POLICY DOCUMENTS

1.2.1 Council of Europe

1987

34. Council of Europe, Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector, 17 September 1987.

1998

35. Parliamentary Assembly, Resolution 165: Right to Privacy, 1998. http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta98/ERES1165.htm

2001

36. Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, Strasbourg, 8 November 2001. http://conventions.coe.int/Treaty/EN/treaties/html/181.htm

37. Council of Europe, Convention on Cybercrime, Budapest, 23 November 2001. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG

2002

38. Parliamentary Assembly, Recommendation 1549: Air transport and terrorism: how to enhance security?, 23 January 2002. http://assembly.coe.int/Main.asp?link=http%3A%2F%2Fassembly.coe.int%2FDocuments%2FAdoptedText%2Fta02%2FEREC1549.htm

2004

39. Council of Europe, Guiding principles for the protection of personal data with regard to smart cards, adopted by the CDCJ[1] at its 79th Plenary on 11-14 May 2004. http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/reports_and_studies_of_data_protection_committees/P-Guiding_principles_smartcards_2004.asp#TopOfPage

2005

40. Committee of Ministers, Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, CM(2005)56 final, 13 May 2005. https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2005)56&Sector=secCM&Language=lanEnglish&Ver=final&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 **[part of short analysis]**

[1] European Committee on legal co-operation, one of the steering committees of the Council of Europe.

41. Parliamentary Assembly, Recommendation 1713: Democratic oversight of the security sector in member states, 23 June 2005. http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta05/erec1713.htm

42. Committee of Ministers, Recommendation of the Committee of Ministers to member states concerning identity and travel documents and the fight against terrorism, Rec(2005)7, 30 March 2005. http://www.coe.int/t/dlapil/codexter/otherTexts_en.asp

2008

43. Council of Europe, *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime*, Strasbourg, 2008.

44. Committee Members of the Council of Europe, Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, 20 Feb 2008. https://wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

2010

45. Cannataci, Joseph A., *Data Protection Vision 2020: options for improving European policy and legislation during 2010-2020: Study on Recommendation No. R (87) 15 of 17 September 1987 regulating the use of personal data in the police sector,* Council of Europe, T-PD-BUR(2010)12 Final, 4 November 2010. http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

46. Council of Europe, Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, CM/Rec(2010)13, 23 November 2010. https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2010)13&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

47. 30th Council of Europe Conference of Ministers of Justice, Resolution No. 3 on data protection and privacy in the third millennium, MJU-30 (2010) RESOL. 3 E, Istanbul, Turkey, 24 - 26 November 2010. http://www.coe.int/t/informationsociety/security/index_en.asp

2011

48. Parliamentary Assembly, Recommendation 1984: The protection of privacy and personal data on the Internet and online media, 2011. http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta11/EREC1984.htm

49. Parliamentary Assembly, Resolution 1843: The protection of privacy and personal data on the Internet and online media, 2011.

http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta11/ERES1843.htm **[part of short analysis]**

2012

50. Recommendation of the Committee of Ministers to member States on the protection of human rights with regard to social networking services (Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies) (CM/Rec(2012)4E) https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282012%294&Language=lanEnglish&Ver=original&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864

51. Council of Ministers, Internet Governance: Council of Europe Strategy 2012-2015, CM(2011)175 final, 15 March 2012. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

52. Council of Europe, Modernisation of Convention 108: proposals, T-PD-BUR(2012)01Rev2_en, Strasbourg, 27 April 2012. http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

1.2.2 European Parliament

Security policy documents

2000

53. European Parliament, Resolution on the progress made in 1999 in the implementation of the area of freedom, security and justice provided for in Article 2, fourth indent, of the Treaty on European Union, 15 February 2000.

54. European Parliament, Resolution on the establishment of a common European security and defence policy with a view to the European Council in Feira, 15 June 2000.

55. European Parliament, Resolution on the progress achieved in the implementation of the common foreign and security policy (C5-0255/2000 - 2000/2038 (INI)), 30 November 2000.

56. European Parliament, Resolution on the establishment of a common European security and defence policy after Cologne and Helsinki (2000/2005(INI)), 30 November 2000.

2001

57. European Parliament, Resolution on progress in establishing an Area of Freedom, Security and Justice (AFSJ) in the year 2000, 16 May 2001.

58. European Parliament, *Report on the existence of a global system for the interception of private and commercial communications (ECHELON) interception system*, 2001/2098(INI), 11 July 2001.

59. European Parliament, Recommendation of the European Parliament on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (2001/2070(COS)), 6 September 2001.

60. European Parliament, Resolution on the progress achieved in the implementation of the common foreign and security policy (C5-0194/2001 - 2001/2007(INI)), 25 October 2001.

61. European Parliament, Resolution on the Commission Green Paper Towards a European strategy for the security of energy supply (COM(2000) 769 - C5-0145/2001 - 2001/2071(COS)), 15 November 2001.

62. European Parliament, Proposal for a European Parliament and Council regulation on establishing common rules in the field of civil aviation security (COM(2001) 575 - C5-0481/2001 - 2001/0234(COD)), 29 November 2001.

63. European Parliament, Recommendation to the Council on an area of Freedom, Security and Justice: security at meetings of the European Council and other comparable events (2001/2167(INI)), 12 December 2001.

2002

64. European Parliament, Resolution on the progress made in 2001 towards the establishment of the area of freedom, security and justice provided for in Article 2, fourth indent, of the TEU, 7 February 2002.

65. European Parliament, Draft Council decision concerning security in connection with football matches with an international dimension (12175/1/2001 – C5-0067/2002 – 2001/0824(CNS)), 9 April 2002.

66. European Parliament, Resolution on the present state of the European Security and Defence Policy (ESDP) and EU-NATO relations, 10 April 2002.

67. European Parliament, Legislative resolution on the Council common position for adopting a European Parliament and Council regulation on establishing common rules in the field of civil aviation security (15029/4/2001 – C5-0033/2002 – 2001/0234(COD)), 14 May 2002.

68. European Parliament, Resolution on the progress achieved in the implementation of the common foreign and security policy (2002/2010(INI)), 26 September 2002.

69. European Parliament, Resolution on the Commission communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European policy approach (COM(2001) 298 – C5-0657/2001 – 2001/2280(COS)), 22 October 2002. **[part of short analysis]**

2003

70. European Parliament, Resolution on progress in 2002 in implementing an area of Freedom, Security and Justice (Articles 2 and 39 of the EU Treaty), 27 March 2003.
71. European Parliament, Resolution on the new European security and defence architecture - priorities and deficiencies (2002/2165(INI)), 10 April 2003.

72. European Parliament, Legislative resolution on the proposal for a directive of the European Parliament and the Council concerning measures to safeguard security of natural gas supply (COM (2002) 488 – C5-0449/2002 – 2002/0220(COD)), 23 September 2003.

73. European Parliament, Legislative resolution on the proposal for a European Parliament and Council regulation on enhancing ship and port facility security (COM(2003) 229 – C5-0218/2003 – 2003/0089(COD)), 19 November 2003.

74. European Parliament, Legislative resolution on the proposal for a European Parliament and Council regulation establishing the European Network and Information Security Agency (COM(2003) 63 – C5-0058/2003 – 2003/0032(COD)), 19 November 2003.

2004

75. European Parliament, Recommendation to the Council on cooperation in the European Union on preparedness and response to biological and chemical agent attacks (health security) (2003/2187(INI)), 9 March 2004.

76. European Parliament, Resolution on the progress made in 2003 in creating an area of freedom, security and justice (AFSJ) (Articles 2 and 39 of the EU Treaty), 11 March 2004.

77. European Parliament, Resolution on the outcome of the European Council meeting on 25-26 March 2004, 1 April 2004.

78. European Parliament, Legislative resolution on amendment of the legal basis and on the 'general orientation' of the Council with a view to adoption of a directive of the European Parliament and of the Council concerning measures to safeguard security of natural gas supply (15769/2003 – C5-0027/2004 – 2002/0220(COD)), 20 April 2004.

79. European Parliament, Recommendation to the Council and to the European Council on the future of the area of freedom, security and justice as well as on the measures required to enhance the legitimacy and effectiveness thereof (2004/2175(INI)), 14 October 2004. **[part of the short analysis]**

80. European Parliament, Legislative resolution on the proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116– C5-0101/2004 – 2004/0039(CNS)), 2 December 2004.

2005

81. European Parliament, Resolution on the annual report from the Council to the European Parliament on the main aspects and basic choices of CFSP, including the financial

implications for the general budget of the European Communities - 2003 (8412/2004 - 2004/2172(INI)), 14 April 2005.

82. European Parliament, Resolution on the European Security Strategy (2004/2167(INI)), 14 April 2005.

83. European Parliament, Legislative resolution on the amended proposal for a directive of the European Parliament and of the Council on enhancing port security (COM(2004)0393 -C6-0072/2004 - 2004/0031(COD)), 10 May 2005.

84. European Parliament, Resolution on progress made in 2004 in creating an area of freedom, security and justice (AFSJ) (Articles 2 and 39 of the EU Treaty), 8 June 2005.

85. European Parliament, Resolution on Security Research – The Next Steps (2004/2171(INI)), 23 June 2005.

86. European parliament, Legislative resolution on the proposal for a directive of the European Parliament and of the Council concerning measures to safeguard security of electricity supply and infrastructure investment (COM(2003)0740 – C5-0643/2003 – 2003/0301(COD)), 5 July 2005.

2006

87. European Parliament, Resolution on the annual report from the Council to the European Parliament on the main aspects and basic choices of CFSP, including the financial implications for the general budget of the European Union - 2004 (2005/2134(INI)), 2 February 2006.

88. European Parliament, Resolution on security of energy supply in the European Union, 23 March 2006.

89. European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on common rules in the field of civil aviation security (COM(2005)0429 – C6-0290/2005 – 2005/0191(COD)), 15 June 2006.

90. European Parliament, Resolution on the implementation of the European Security Strategy in the context of the ESDP (2006/2033(INI)), 16 November 2006.

91. European Parliament, Resolution on the progress made in the EU towards the Area of freedom, security and justice (AFSJ) (Articles 2 and 39 of the EU Treaty), 30 November 2006.

92. European Parliament, Legislative resolution on the proposal for a Council decision establishing the specific programme 'Prevention, Preparedness and Consequence Management of Terrorism' for the period 2007-2013 – General Programme 'Security and Safeguarding Liberties' (COM(2005)0124 – C6-0241/2005 – 2005/0034(CNS)), 14 December 2006.

93. European Parliament, Legislative resolution on the proposal for a Council decision establishing the Specific Programme "Prevention of and Fight against Crime' for the pe-

riod 2007-2013, General Programme 'Security and Safeguarding Liberties" (COM(2005)0124 – C6-0242/2005 – 2005/0035(CNS)), 14 December 2006. **[part of short analysis]**

94. European Parliament, Legislative resolution on the draft Council regulation establishing an Instrument for Nuclear Safety and Security Assistance (9037/2006 – C6-0153/2006 – 2006/0802(CNS)), 14 December 2006.

2007

95. European Parliament, Legislative resolution of 29 March 2007 on the initiative by the Republic of Austria with a view to the adoption of a Council decision amending Decision 2002/348/JHA concerning security in connection with football matches with an international dimension (10543/2006 – C6-0240/2006 – 2006/0806(CNS)), 29 March 2007.

96. European Parliament, Legislative resolution of 25 April 2007 on the Council common position for adopting a regulation of the European Parliament and of the Council on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (14039/1/2006 – C6-0041/2007 – 2005/0191(COD)), 25 April 2007.

97. European Parliament, Resolution of 23 May 2007 on the annual report from the Council to the European Parliament on the main aspects and basic choices of CFSP, including the financial implications for the general budget of the European Union – 2005 (2006/2217(INI)), 23 May 2007.

98. European Parliament, Legislative resolution of 7 June 2007 on the proposal for a Council decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005)0600 – C6-0053/2006 – 2005/0232(CNS)), 7 June 2007.

99. European Parliament, Resolution of 21 June 2007 on an area of freedom, security and justice: Strategy on the external dimension, Action Plan implementing the Hague programme (2006/2111(INI)), 21 June 2007. **[part of short analysis]**

100. European Parliament, Resolution of 5 September 2007 on Commission Regulation (EC) No 1546/2006 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security (introduction of liquids onto aircraft), 5 September 2007.

2008

101. European Parliament, Legislative resolution of 11 March 2008 on the joint text approved by the Conciliation Committee for a regulation of the European Parliament and of the Council on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (PE-CONS 3601/2008 – C6-0029/2008 – 2005/0191(COD)), 11 March 2008.

102. European Parliament, Resolution of 5 June 2008 on the implementation of the European Security Strategy and ESDP (2008/2003(INI)), 5 June 2008.

103. European Parliament, Resolution of 10 July 2008 on Space and security (2008/2030(INI)), 10 July 2008.

104. European Parliament, Resolution of 25 September 2008 on the annual debate on the progress made in 2007 in the Area of Freedom, Security and Justice (AFSJ) (Articles 2 and 39 of the EU Treaty), 25 September 2008.

105. European Parliament, Legislative resolution of 21 October 2008 on the proposal for a Council decision on the conclusion of a Memorandum of Cooperation between the International Civil Aviation Organisation and the European Community regarding security audits/inspections and related matters (COM(2008)0335 - C6-0320/2008 - 2008/0111(CNS)), 21 October 2008.

106. European Parliament, Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, 28 October 2008.

2009

107. European Parliament, Legislative resolution of 14 January 2009 on the proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (COM(2007)0619 – C6-0359/2007 – 2007/0216(COD)), 14 January 2009.

108. European Parliament, Resolution of 19 February 2009 on the annual report from the Council to the European Parliament on the main aspects and basic choices of the Common Foreign and Security Policy (CFSP) in 2007, presented to the European Parliament in application of point G, paragraph 43 of the Interinstitutional Agreement of 17 May 2006 (2008/2241(INI)), 19 February 2009.

109. European Parliament, Resolution of 19 February 2009 on the European Security Strategy and ESDP (2008/2202(INI)), 19 February 2009.

110. European Parliament, Resolution of 19 February 2009 on the role of NATO in the security architecture of the EU (2008/2197(INI)), 19 February 2009.

111. European Parliament, Recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI)), 26 March 2009.

112. European Parliament, Resolution of 17 September 2009 on external aspects of energy Security, 17 September 2009.

113. European Parliament, Resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme, 25 November 2009.

2010

114. European Parliament, Resolution of 10 March 2010 on the annual report from the Council to the European Parliament on the main aspects and basic choices of the Common Foreign and Security Policy (CFSP) in 2008, presented to the European Parliament in application of Part II, Section G, paragraph 43 of the Interinstitutional Agreement of 17 May 2006 (2009/2057(INI)), 10 March 2010.

115. European Parliament, Resolution of 10 March 2010 on the implementation of the European Security Strategy and the Common Security and Defence Policy (2009/2198(INI)), 10 March 2010.

116. European Parliament, Legislative resolution of 5 May 2010 on the proposal for a directive of the European Parliament and of the Council on aviation security charges (COM(2009)0217 – C7–0038/2009 – 2009/0063(COD)), 5 May 2010.

117. European Parliament, Legislative resolution of 21 September 2010 on the proposal for a regulation of the European Parliament and of the Council concerning measures to safeguard security of gas supply and repealing Directive 2004/67/EC (COM(2009)0363 – C7-0097/2009 – 2009/0108(COD)), 21 September 2010.

118. European Parliament, Resolution of 25 November 2010 on the 10th anniversary of UN Security Council Resolution 1325 (2000) on Women, Peace and Security, 25 November 2010.

119. European Parliament, Resolution of 14 December 2010 on strengthening chemical, biological, radiological and nuclear security in the European Union – an EU CBRN Action Plan (2010/2114(INI)), 14 December 2010.

2011

120. European Parliament, The annual report from the Council to the European Parliament on the main aspects and basic choices of the Common Foreign and Security Policy (CFSP) in 2009, presented to the European Parliament in application of Part II, Section G, paragraph 43 of the Inter-institutional Agreement of 17 May 2006, 11 May 2011.

121. European Parliament, Resolution of 11 May 2011 on the development of the common security and defence policy following the entry into force of the Lisbon Treaty (2010/2299(INI)), 11 May 2011.

122. European Parliament, Legislative resolution of 5 July 2011 on the amended proposal for a regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (COM(2010)0093 – C7-0046/2009 – 2009/0089(COD)), 5 July 2011.

123. European Parliament, Resolution of 6 July 2011 on aviation security, with a special focus on security scanners (2010/2154(INI)), 6 July 2011.

2012

124. European Parliament, Resolution of 16 February 2012 on the future of GMES (2012/2509(RSP)), 16 February 2012.

125. European Parliament, Resolution of 22 May 2012 on the European Union's Internal Security Strategy ((2010)2308 (INI)), 22 May 2012.

Privacy policy documents

2000

126. European Parliament and the Council, Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17 July 2000.

127. European Parliament, Resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000 - 2000/2144(COS)), 5 July 2000.

2001

128. European Parliament and the Council, Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12 Jan 2001.

129. European Parliament, Proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000) 385 - C5-0439/2000 - 2000/0189(COD)), 13 November 2001.

2002

130. European Parliament and the Council, Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24 Apr 2002.

131. European Parliament, Legislative resolution on the Council common position for adopting a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (15396/2/2001 – C5-0035/2002 – 2000/0189(COD)), 30 May 2002.

132. European Parliament and the Council, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002.

2006

133. European Parliament and the Council, Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13 Apr 2006.

134. European Parliament, Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM(2005)0475 – C6-0436/2005 – 2005/0202(CNS)), 14 June 2006.

135. European Parliament, Recommendation to the Council on the progress of the negotiations on the framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2006/2286(INI)), 14 December 2006.

2007

136. European Parliament, Legislative resolution of 7 June 2007 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (renewed consultation) (7315/2007 – C6-0115/2007 – 2005/0202(CNS)), 7 June 2007.

137. European Parliament, Legislative resolution of 23 September 2008 on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (16069/2007 – C6-0010/2008 – 2005/0202(CNS)), 23 September 2008.

138. European Parliament, Legislative resolution of 24 September 2008 on the proposal for a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)).

139. European Parliament, Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection, 23 October 2008.

2009

140. European Parliament, Legislative resolution of 6 May 2009 on the common position adopted by the Council with a view to the adoption of a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (16497/1/2008 – C6-0068/2009 – 2007/0248(COD)), 6 May 2009.

141. European Parliament and the Council, Regulation (EC) No 1211/2009 of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, OJ L 337, 18 December 2009.

142. European Parliament and the Council, Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18 December 2009.

143. European Parliament and the Council, Directive 2009/140/EC of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337, Vol. 52, 18 December 2009.

2011

144. European Parliament, Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)), 6 July 2011. **[part of short analysis]**

1.2.3 Council of the European Union

Security policy documents

2002

145. Council of the European Union, Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, OJ L 164, 22 June 2002, pp. 3-7. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:164:0003:0007:EN:PDF

2003

146. Council of the European Union, *A Secure Europe in a Better World, European Security Strategy*, Brussels, 12 December 2003. **[part of short analysis]**

2004

147. Council of the European Union, Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25 November 2004, pp. 1-11.

148. Council of the European Union, *Conceptual Framework on the European Security and Defence Policy (EDSP) Dimension of the Fight against Terrorism*, Brussels, November 2004.

149. Council of the European Union, *Note from the General Secretariat to the Delegations on the Hague Programme: strengthening freedom, security and justice in the European Union,* 16054/04, Brussels, 13 December 2004.

150. Council of the European Union, Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 29 December 2004, pp. 1-6.

2005

151. Council of the European Union, JHA Council Declaration on the EU Response to the London Bombings, Brussels, 13 July 2005.

152. Council of the European Union, Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69, 16 March 2005, pp. 67-72.

153. Council of the European Union, *The European Union Counter-Terrorism Strategy, Justice and Home Affairs Council meeting*, Brussels, 1 December 2005.

2006

154. Council of the European Union, *Updated EU Action Plan for Combating Terrorism*, Brussels, 13 February 2006.

155. Council of the European Union, Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13 April 2006, p. 54-63.

2007

156. Council of the European Union, Council Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks' (2007/124/EC, Euratom), OJ L 58, 24 February 2007, pp. 1-6.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0124:EN:NOT

157. Council of the European Union, Draft Council Conclusions adopting Strategic Orientations and Priorities on the security enhancement of explosives 15618/07, Brussels, 23 November 2007. http://ue.eu.int/policies/fight-against-terrorism/documents/related-documents?lang=en

2008

158. Council of the European Union, *Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection*, 9831/08, Note from the Council Presidency to COREPER, Brussels, 28 May 2008.
www.dhs.gov/xlibrary/assets/privacy/privacy_intl_hlcg_report_02_07_08_en.pdf

159. Council of the European Union, Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision), OJ L 210, 23 June 2008, pp. 1-11.

160. Council of the European Union, *Report on the Implementation of the European Security Strategy: Providing Security in a Changing World S407/08*, Brussels, 11 December 2008. http://ue.eu.int/eeas/security-defence/european-security-strategy?lang=en

161. Council of the European Union, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23 December 2008, p. 75-83.

2009

162. Council of the European Union, *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, Note from the Presidency to the General Affairs Council/European Council, 17024/09, Brussels, 2 December 2009.

2010

163. Council of the European Union, *Draft Internal Security Strategy for the European Union: "Towards a European Security Model"*, 5842/2/10, REV 2, Note from the Presidency to Delegations, Brussels, 23 February 2010.

164. Council of the European Union, The Stockholm Programme - An open and secure Europe serving and protecting citizens, 5731/10, Brussels, 3 March 2010. http://ue.eu.int/policies/fight-against-terrorism/documents/related-documents?lang=en **[part of short analysis]**

2012

165. Council of the European Union, EU Counter-Terrorism Strategy - Discussion paper 9990/12, Brussels, 23 May 2012. http://ue.eu.int/policies/fight-against-terrorism/documents/key-documents?lang=en

Privacy policy documents

2005

166. Council of the European Union, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, 13019/05, Brussels, 11 October 2005.

2007

167. Council of the European Union, Council Resolution on a Strategy for a Secure Information Society in Europe, 16708/06, Brussels, 27 February 2007.

2008

168. Council of the European Union, *EU-US High Level Contact Group on Data Protection and exchange of information - Future proceedings*, 6780/08, Brussels, 22 February 2008.

169. Council of the European Union, Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 9260/08, Brussels, 24 June 2008.

170. Council of the European Union, Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation - Privacy Directive, 14780/08, Brussels, 27 October 2008.

171. Council of the European Union, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on future networks and the Internet – Council conclusions, 15902/08, Brussels, 20 November 2008.

2009

172. Council of the European Union, Common position adopted by the Council on 16 February 2009 with a view to the adoption of a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, 16497/1/08 REV 1, Brussels, 16 February 2009.

173. High Level Contact Group on information sharing and privacy and personal data protection, *Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection*, Council of the European Union, 15851/09, Brussels, 23 November 2009.

174. Council of the European Union, Council Resolution on collaborative European approach on Network and Information Security – Adoption, 15841/09, Brussels, 8 December 2009.

2010

175. Council of the European Union, EU-US Agreement on the Transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Programme - Council declaration, 6567/10, Brussels, 16 February 2010.

2011

176. Council of the European Union, Council conclusions on the Communication from the Commission to the European Parliament and the Council - A comprehensive approach on personal data protection in the European Union, 5980/4/11 REV 4, Brussels, 15 February 2011.

177. Council of the European Union, Proposal for a Council Decision on the conclusion 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) 807 final, Brussels, 23 Nov 2011.

178. Council of the European Union, *Consultation on reform of Data Retention Directive: emerging themes and next steps*, 18620/11, Brussels, 15 December 2011.

2012

179. Council of the European Union, Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 8916/12, Brussels, 23 April 2012.

1.2.4 European Commission

Security policy documents

2003

180. European Commission, Communication to the Council and the European Parliament on Cooperation in the European Union on Preparedness and Response to Biological and Chemical Agent Attacks (Health Security), COM(2003) 320 final, Brussels, 2 June 2003.

2004

181. European Commission, Towards a programme to advance European security through Research and Technology, Communication on the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research, COM(2004) 72 final, Brussels, 3 Feb 2004.

182. European Commission, Area of Freedom, Security and Justice: Assessment of the Tampere programme and future orientations Communication to the Council and the European Parliament, COM(2004) 401 final Brussels, 2 June 2004.

183. European Commission, Security Research: The Next Steps, Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2004) 590 final, Brussels, 7 Sept 2004.

184. European Commission, Prevention, preparedness and response to terrorist attacks, Communication to the Council and the European Parliament, COM(2004) 698 final, Brussels, 20 Oct 2004.

185. European Commission, Preparedness and consequence management in the fight against terrorism, Communication to the Council and the European Parliament, COM(2004) 701 final, Brussels, 20 Oct 2004.

186. European Commission, Critical Infrastructure Protection in the fight against terrorism, Communication to the Council and the European Parliament, Brussels, COM(2004) 702 final, Brussels, 20 Oct 2004.

2005

187. European Commission, Establishing a framework programme on "Security and Safeguarding Liberties" for the period 2007-2013, Communication to the Council and the European Parliament, COM(2005) 124 final, Brussels, 4 April 2005. **[part of short analysis]**

188. European Commission, The Hague Programme: Ten priorities for the next five years The Partnership for European renewal in the field of Freedom, Security and Justice, Communication to the Council and the European Parliament, COM(2005) 184 final, Brussels, 10 May 2005.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0184:EN:HTML
[part of short analysis]

189. Commission Staff Working Document, Revised Action Plan on Terrorism, SEC(2005) 841, Brussels, 17 June 2005.

190. European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final, Brussels, 17 Nov 2005.

2006

191. European Commission, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment", Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2006) 251 final, Brussels, 31 May 2006.
http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf

192. Commission Staff Working Document, Annex to the Communication A strategy for a Secure Information Society – "Dialogue, partnership and empowerment" – Impact Assessment, Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM (2006) 656, 31 May 2006.

193. European Commission, Green Paper on detection technologies in the work of law enforcement, customs and other security authorities, COM(2006) 474 final, Brussels, 1 September 2006.

2007

194. Commission Staff Working Document, Results of the Public Online Consultation on Future Radio Frequency Identification Technology Policy, "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats" accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy Framework, SEC(2007) 312, Brussels, 15 Mar 2007.

195. European Commission, *Commission Activities in the Fight against Terrorism*, MEMO/07/98, Brussels, 12 March 2007.

196. European Commission, Communication to the European Parliament, the Council and the Committee of the Regions, Towards a general policy on the fight against cybercrime, COM(2007) 267 final, Brussels, 22 May 2007.

197. European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, COM(2007) 619 final, Brussels, 18 October 2007.

2008

198. European Commission, Report to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, COM(2008) 448 final, Brussels, 14 July 2008.

2009

199. European Commission, *Report on Cross-border e-Commerce in the EU*, SEC(2009) 283 final, European Commission, Brussels, 5 March 2009.

200. Commission Staff Working Document, Accompanying document to the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience", Summary of the Impact Assessment, SEC(2009) 400, Brussels, 30 March 2009.

201. European Commission, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection Brussels,

COM(2009) 149 final, 30 March 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

2010

202. European Commission, Proposal for a Regulation Of The European Parliament And The Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), COM(2010) 61 final, Brussels, 24 Feb 2010.

203. 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 Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) 8-9 February 2010, Brussels, 7 Apr 2010.

204. European Commission, Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 171 final, Brussels, 20 April 2010.

205. European Commission, Overview of information management in the area of freedom, security and justice, Communication to the European Parliament and the Council, COM(2010)385 final, Brussels, 20 July 2010.

206. European Commission, Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA, MEMO/10/463, Brussels, 30 September 2010.
http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463&format=HTML&aged=0&language=EN&guiLanguage=en

207. European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Communication to the European Parliament and the Council, Brussels, COM(2010) 673 final, 22 Nov 2010.

2011

208. 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 Feb 2011.

209. European Commission, Programming Mandate Addressed to CEN, CENELEC and ETSI to Establish Security Standards, M/487 EN, Brussels, 17th February 2011.

210. European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, “Achievements and next steps: towards global cyber-security”, COM(2011) 163 final, Brussels, 31 Mar 2011.

211. European Commission, Communication on migration, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2011) 248/3, Brussels, 4 May 2011.

212. European Commission, Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR), COM(2011) 873 final, Brussels, 12 December 2011.

Privacy policy documents

2000

213. European Commission, Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, COM(2000) 385 final, Brussels, 12 July 2000.

2003

214. European Commission, *First report on the implementation of the Data Protection Directive (95/46/EC)*, Report from the Commission, COM(2003) 265 final, Brussels, 15 May 2003

215. European Commission, The Role of eGovernment for Europe's Future, Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2003) 567 final, Brussels, 26 Sept 2003.

2004

216. Group of Personalities, *Research for a Secure Europe*, Report of the Group of Personalities in the field of Security Research, Office for Official Publications of the European Communities, Luxembourg, 2004.

2006

217. Commission Staff Working Document, Impact Assessment on the Review of the EU Regulatory Framework for electronic communications networks and services {COM(2006) 334 final}, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, SEC(2006) 817, Brussels, 28 June 2006.

2007

218. European Commission, Communication to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, Brussels, 7 Mar 2007.

219. European Commission, Radio Frequency Identification (RFID) in Europe: steps towards a policy framework, Communication to the European Parliament, the Council,

the European Economic and Social Committee and the Committee of the Regions, COM(2007) 96 final, Brussels, 15 March 2007.

220. European Commission, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007) 228 final, Brussels, 2 May 2007.

221. European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, COM(2007) 698 final, Brussels, 13 Nov 2007.

2008

222. European Commission, Communication on future networks and the internet, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2008) 594 final, Brussels, 29 Sept 2008.

2009

223. European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, COM(2009) 3200 final, Brussels, 12 May 2009.

224. European Commission, An area of freedom, security and justice serving the citizen, Communication to the European Parliament and the Council, COM(2009) 262 final, Brussels, 10 June 2009.

225. European Commission, Internet of Things — An action plan for Europe, Communication to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2009) 278 final, Brussels, 18 June 2009.

226. European Commission, A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations, COM(2009) 691 final, Brussels, 21 December 2009.

2010

227. European Commission, A Digital Agenda for Europe, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 245, Brussels, 19 May 2010. http://ec.europa.eu/europe2020/pdf/digital-agenda-communication-en.pdf

228. European Commission, Overview of information management in the area of freedom, security and justice, Communication from the Commission to the European Parliament

and the Council, COM(2010) 385 final, Brussels, 20 July 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0385:FIN:EN:PDF

229. European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4 Nov 2010.
http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104

2012

230. European Commission, Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25 Jan 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf

231. European Commission, Report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, COM(2012) 12/2, Brussels, 25 Jan 2012.
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_12_en.pdf

232. European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, Brussels, 25 Jan 2012. **[part of short analysis]**

233. European Commission, Proposal for a Directive of the European Parliament and of 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, COM(2012) 10 final, Brussels, 25 Jan 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf

234. Commission Staff Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of 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, SEC(2012) 72/2, Brussels, 25 Jan 2012.

1.2.5 European Security Research Advisory Board (ESRAB)

2006

235. ESRAB, *Meeting the challenge: the European Security Research Agenda, A report from the European Security Research Advisory Board*, Office for Official Publications of the European Communities, Luxembourg, September 2006.

1.2.6 European Security Research and Innovation Forum (ESRIF)

2007

236. European Commission, *The European Security Research and Innovation Forum (ESRIF) - Public-Private Dialogue in Security Research: The origin of Public Private Dialogue in security Research*, MEMO/07/346, Brussels, 11th September 2007. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/346

2009

237. European Security Research and Innovation Forum, *ESRIF Final Report*, December 2009. www.esrif.eu/documents/esrif_final_report.pdf

1.2.7 European Network and Information Security Agency (ENISA)

2006

238. European Network and Information Security Agency (ENISA), *Provider Security Measures Part 1*, 6 February 2006. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/anti-spam-measures/studies/provider-security-measures-1

239. European Network and Information Security Agency (ENISA), *Inventory of risk assessment and risk management methods*, 30 March 2006. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/inventory-of-risk-assessment-and-risk-management-methods

240. European Network and Information Security Agency (ENISA), *Road map*, 30 March 2006. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/road-map

241. European Network and Information Security Agency (ENISA), *Provider Security Measures Part 2*, 1 June 2006. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/anti-spam-measures/studies/provider-security-measures-2

242. European Network and Information Security Agency (ENISA), *Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools*, 1 June 2006.

243. European Network and Information Security Agency (ENISA), *CERT cooperation and its further facilitation by relevant stakeholders*, 1 December 2006.

2007

244. European Network and Information Security Agency (ENISA), *Risk Management & IT Security for Micro and Small Businesses*, 1 January 2007. http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/risk-management-it-security-for-micro-and-small-businesses

245. European Network and Information Security Agency (ENISA), *Methodology for evaluating usage and comparison of risk assessment and risk management items*, 26 April 2007. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/methodology-for-evaluating-usage-and-comparison-of-risk-assessment-and-risk-management-items

246. European Network and Information Security Agency (ENISA), *Reference source for threats, vulnerabilities, impacts and controls in IT risk assessment and risk management*, 26 April 2007. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/reference-source-for-threats-vulnerabilities-impacts-and-controls-in-it-risk-assessment-and-risk-management

247. European Network and Information Security Agency (ENISA), *Risk Management / Risk Assessment in European regulation, international guidelines and codes of practice*, 1 June 2007. http://www.enisa.europa.eu/activities/risk-management/current-risk/laws-regulation/downloads/risk-management-risk-assessment-in-european-regulation-international-guidelines-and-codes-of-practice

248. European Network and Information Security Agency (ENISA), *Information security awareness initiatives: Current practice and the measurement of success*, 1 July 2007. http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2007/kpi-study/en

249. European Network and Information Security Agency (ENISA), *Information security awareness: Local government and Internet service providers*, 1 August 2007. http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2007/loc-gov/en

250. European Network and Information Security Agency (ENISA), *Botnets – The Silent Threat*, 7 September 2007. http://www.enisa.europa.eu/activities/identity-and-trust/past-work-areas/botnets/botnets-2013-the-silent-threat

251. European Network and Information Security Agency (ENISA), *Online Social Networks*, 25 October 2007. http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/soc-net

252. European Network and Information Security Agency (ENISA), *Recommendations for Online Social Networks*, 14 November 2007.

http://www.enisa.europa.eu/activities/identity-and-trust/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks

253. European Network and Information Security Agency (ENISA), *Examining the Feasibility of a Data Collection Framework*, 15 November 2007. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting/data-collection/examining-the-feasibility-of-a-data-collection-framework

254. European Network and Information Security Agency (ENISA), *Reputation-based Systems: a security analysis*, 10 December 2007. http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/reputation-systems/reputation-based-systems-a-security-analysis

2008

255. European Network and Information Security Agency (ENISA), *Strengthening EU legislation*, 18 January 2008. http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/eu-leg

256. European Network and Information Security Agency (ENISA), *Security Economics and the Internal Market*, 31 January 2008. http://www.enisa.europa.eu/activities/stakeholder-relations/reports/econ-sec/economics-sec

257. European Network and Information Security Agency (ENISA), *Privacy Features of European eID Card Specifications*, 1 August 2008. http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/eid/pet

258. European Network and Information Security Agency (ENISA), *Stock taking report*, 19 September 2008. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/policies/stock-taking-of-national-policies/stock-taking-report

259. ENISA Ad Hoc Working Group on Privacy & Technology, *Technology-induced challenges in Privacy & Data Protection in Europe*, A report, October 2008. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe

260. European Network and Information Security Agency (ENISA), *Security awareness management in local governments: Approaches in Scandinavia*, 1 October 2008. http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2008/scandinavian-approaches-survey

261. European Network and Information Security Agency (ENISA), *Online Games and Virtual Worlds*, 28 October 2008. http://www.enisa.europa.eu/activities/identity-and-trust/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming

262. European Network and Information Security Agency (ENISA), *Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID)*, 11 November 2008.

http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/eid/mobile-eid

263. European Network and Information Security Agency (ENISA), *Web 2.0 Security and privacy*, 10 December 2008. http://www.enisa.europa.eu/activities/identity-and-trust/past-work-areas/web2sec/report

2009

264. European Network and Information Security Agency (ENISA), *Privacy Features of European eID Card Specifications*, 27 January 2009. http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/eid/eid-cards-en

265. European Network and Information Security Agency (ENISA), *Analysis of policies and recommendations*, 20 February 2009. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations

266. European Network and Information Security Agency (ENISA), *Being diabetic in 2011*, 1 March 2009. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/being-diabetic-2011

267. European Network and Information Security Agency (ENISA), *EFR Framework Handbook*, 9 March 2009. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/efr-framework-handbook

268. European Network and Information Security Agency (ENISA), *Good Practice Guide on Information Sharing*, 13 June 2009. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

269. European Network and Information Security Agency (ENISA), *Information security awareness in financial organisations - Guidelines and case studies*, 21 September 2009. http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2009/is-in-financial-organisations-09

270. European Network and Information Security Agency (ENISA), *Cloud Computing Risk Assessment*, 20 November 2009. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

271. European Network and Information Security Agency (ENISA), *Briefing: Quantum Key Distribution*, 27 November 2009. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/briefing-quantum-key-distribution

272. European Network and Information Security Agency (ENISA), *Good Practice Guide on Incident Reporting*, 10 December 2009.

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1

2010

273. European Network and Information Security Agency (ENISA), *National eIDs in pan-European e-Government Services*, 24 January 2010. http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/eid/egov

274. European Network and Information Security Agency (ENISA), *Security Issues in Cross-border Electronic Authentication*, 3 February 2010. http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/eid/xborderauth

275. European Network and Information Security Agency (ENISA), *Online as soon as it happens*, 8 February 2010. http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/onlineasithappens

276. European Network and Information Security Agency (ENISA), *Behavioural Biometrics*, 18 February 2010. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/behavioural-biometrics

277. European Network and Information Security Agency (ENISA), *Emerging and Future Risks Framework - Introductory Manual*, 1 March 2010. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/emerging-and-future-risks-framework-introductory-manual

278. European Network and Information Security Agency (ENISA), *Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology*, 12 April 2010. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology

279. European Network and Information Security Agency (ENISA), *Priorities for Research on Current and Emerging Network Trends*, 20 April 2010. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/procent

280. European Network and Information Security Agency (ENISA), *Incentives and Barriers to Information Sharing*, 8 September 2010. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing

281. European Network and Information Security Agency (ENISA), *Baseline Capabilities of National/Governmental CERTs: Part 2 Policy Recommendations*, 17 December 2010. http://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations

2011

282. European Network and Information Security Agency (ENISA), *Data breach notifications in the EU*, 13 January 2011. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn

283. European Network and Information Security Agency (ENISA), *Security and Resilience in Governmental Clouds*, 17 January 2011. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

284. European Network and Information Security Agency (ENISA), *Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments*, 31 January 2011. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/survey-pat

285. European Network and Information Security Agency (ENISA), *Bittersweet cookies: Some security and privacy considerations*, 2 February 2011. http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/cookies

286. European Network and Information Security Agency (ENISA), *EISAS Roadmap*, 16 February 2011. http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas_roadmap

287. European Network and Information Security Agency (ENISA), *Privacy, Accountability and Trust – Challenges and Opportunities*, 18 February 2011. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study

288. European Network and Information Security Agency (ENISA), *Fighting botnets: the need for global cooperation*, 15 April 2011. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/botnets/policy-statement

289. European Network and Information Security Agency (ENISA), *Cyber Europe 2010 Report*, 18 April 2011. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report

290. European Network and Information Security Agency (ENISA), *Managing Multiple Identities*, 20 April 2011. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/mami

291. European Network and Information Security Agency (ENISA), *A Security Analysis of Next Generation Web Standards*, 31 July 2011. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/web-security/a-security-analysis-of-next-generation-web-standards

292. European Network and Information Security Agency (ENISA), *Cyber security: Future challenges and opportunities*, 2 December 2011. http://www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities **[part of short analysis]**

293. European Network and Information Security Agency (ENISA), *Cyber Security Aspects in the Maritime Sector*, 19 December 2011. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1

2012

294. European Network and Information Security Agency (ENISA), *Study on data collection and storage in the EU*, 23 February 2012. http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection

295. European Network and Information Security Agency (ENISA), *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace*, May 2012.

1.2.8 Frontex

2010

296. Centre for the Study of Global Ethics (University of Birmingham), *Ethics of Border Security*, Frontex/64/2010, 1 January 2010. http://www.frontex.europa.eu/publications?c=research

297. Frontex, *Extract from the Annual Risk Analysis 2010*, Warsaw, March 2010. http://www.frontex.europa.eu/publications?c=risk-analysis

2011

298. Frontex, *Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Crossing Systems*, Warsaw, March 2011. http://www.frontex.europa.eu/publications?c=research

299. Frontex, *Operational and Technical Security of Electronic Passports*, Warsaw, July 2011. http://www.frontex.europa.eu/publications?c=research

300. Frontex, *Futures of Borders: A forward study of European border checks*, Frontex, December 2011. http://www.frontex.europa.eu/publications?c=research

2012

301. Frontex, *Annual Risk Analysis 2012*, Warsaw, April 2012. http://www.frontex.europa.eu/publications?c=risk-analysis

1.2.9 EU Agency for Fundamental Rights (FRA)

2008

302. European Union Agency for Fundamental Rights, FRA Opinion on proposal for a Council Framework decision on the use of Passenger Name Record (PNR), 28 October 2008. http://fra.europa.eu/fraWebsite/research/opinions/opn-passenger-name-record_en.htm

2009

303. European Union Agency for Fundamental Rights, FRA Opinion on The Stockholm Programme, 29 July 2009. http://fra.europa.eu/fraWebsite/research/opinions/op-stockholm-programme_en.htm

304. European Union Agency for Fundamental Rights, *FRA comments on the Presidency Draft Stockholm Programme*, 3 November 2009. http://fra.europa.eu/fraWebsite/research/opinions/op-pres-stockholm-programme_en.htm

2010

305. European Union Agency for Fundamental Rights, *The use of body scanners: 10 questions and answers*, 27 July 2010. http://fra.europa.eu/fraWebsite/research/opinions/op-bodyscanner_en.htm

2011

306. European Union Agency for Fundamental Rights, FRA Opinion on the draft Directive regarding the European Investigation Order (EIO), 23 February 2011. http://fra.europa.eu/fraWebsite/research/opinions/op-eio_en.htm

307. European Union Agency for Fundamental Rights, FRA presents opinion on proposal for Passenger Name Record (PNR) directive, Vienna, 14 June 2011. http://fra.europa.eu/fraWebsite/research/opinions/op-passenger-name-record_en.htm

1.2.10 Article 29 Data Protection Working Party

1998

308. Article 29 Data Protection Working Party, Recommendation 1/98 on Airline Computerised Reservation Systems (CRS), WP 10, Brussels, 28 April 1998.

1999

309. Article 29 Data Protection Working Party, Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications, WP 18, Brussels, 3 May 1999.

310. Article 29 Data Protection Working Party, Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, WP 25, Brussels, 7 September 1999.

2000

311. Article 29 Data Protection Working Party, Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000, WP 36, Brussels, 2 November 2000.

2001

312. Article 29 Data Protection Working Party, Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, WP 41, Brussels, 22 March 2001.

313. Article 29 Data Protection Working Party, Working Document on IATA Recommended Practice 1774 Protection for privacy and transborder data flows of personal data used in international air transport of passengers and of cargo, WP 49, Brussels, 14 September 2001.

314. Article 29 Data Protection Working Party, Opinion 9/2001 on the Commission Communication on "Creating a safer information society by improving the security of information infrastructures and combating computer-related crime", WP 51, Brussels, 5 November 2001.

315. Article 29 Data Protection Working Party, Opinion 10/2001 on the need for a balanced approach in the fight against terrorism, WP 53, Brussels, 14 December 2001. **[part of short analysis]**

2002

316. Article 29 Data Protection Working Party, Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data, WP 64, Brussels, 11 October 2002.

317. Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, WP 66, Brussels, 24 October 2002.

318. Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data by means of Video Surveillance, WP 67, Brussels, 25 November 2002.

2003

319. Article 29 Data Protection Working Party, Opinion 1/2003 on the storage of traffic data for billing purposes, WP 69, Brussels, 29 January 2003.

320. Article 29 Data Protection Working Party, Opinion 4/2003 of the Art. 29 Working Party Annex: Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration, WP 78, Brussels, 13 June 2003.

321. Article 29 Data Protection Working Party, Working document on biometrics, WP 80, Brussels, 1 August 2003.

2004

322. Article 29 Data Protection Working Party, Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines, WP 85, Brussels, 16 January 2004.

323. Article 29 Data Protection Working Party, Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), WP 87, Brussels, 29 January 2004.

324. Article 29 Data Protection Working Party, Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines, WP 88, Brussels, 11 February 2004.

325. Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, WP 89, Brussels, 11 February 2004.

326. Article 29 Data Protection Working Party, Joint Statement in response to the terrorist attacks in Madrid, WP 93, Brussels, 17 March 2004.

327. Article 29 Data Protection Working Party, Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, WP 95, Brussels, 22 June 2004.

328. Article 29 Data Protection Working Party, Opinion 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS), WP 96, Brussels, 11 August 2004.

329. Article 29 Data Protection Working Party, Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America, WP 97, Brussels, 30 September 2004.

330. Article 29 Data Protection Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism [Proposal presented by France, Ireland, Sweden and Great

Britain (Document of the Council 8958/04 of 28 April 2004)], WP 99, Brussels, 9 November 2004.

2005

331. Article 29 Data Protection Working Party, Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from airlines, WP 103, Brussels, 19 January 2005.

332. Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, WP 105, Brussels, 19 January 2005.

333. Article 29 Data Protection Working Party, Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final), WP 110, Brussels, 23 June 2005.

334. Article 29 Data Protection Working Party, Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology, WP 111, Brussels, 28 June 2005.

335. Article 29 Data Protection Working Party, Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, WP 112, Brussels, 30 September 2005.

336. Article 29 Data Protection Working Party, Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005) 438 final of 21.09.2005), WP 113, Brussels, 21 October 2005.

337. Article 29 Data Protection Working Party, Opinion 5/2005 on the use of location data with a view to providing value-added services, WP 115, Brussels, 25 November 2005.

338. Article 29 Data Protection Working Party, Opinion 6/2005 on the Proposals for a Regulation of the European Parliament and of the Council (COM (2005) 236 final) and a Council Decision (COM (2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final), WP 116, 25 November 2005.

2006

339. Article 29 Data Protection Working Party, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks and amending Directive 2002/58/EC, WP 119, Brussels, 25 March 2006.

340. Article 29 Data Protection Working Party, Opinion 4/2006 on the Notice of proposed rule making by the US Department of Health and Human Services on the control of communicable disease and the collection of passenger information of 20 November 2005 (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71) WP 121, Brussels, 14 June 2006.

341. Article 29 Data Protection Working Party, Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States, WP 122, Brussels, 14 June 2006.

342. Article 29 Data Protection Working Party, Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement, WP 124, Brussels, 27 September 2006.

343. Article 29 Data Protection Working Party, Opinion 9/2006 on the Implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data, WP 127, Brussels, 27 September 2006.

344. Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128, Brussels, 22 November 2006.

2007

345. Article 29 Data Protection Working Party, Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities, WP 129, 9 January 2007.

346. Article 29 Data Protection Working Party, Opinion 2/2007 on information to passengers about transfer of PNR data to US authorities; Annex: Short notice for travel between the European Union and the United States, WP 132, Brussels, 15 February 2007.

347. Article 29 Data Protection Working Party, Opinion No. 3/2007 on the Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications COM(2006) 269 final, WP 134, Brussels, 1 March 2007.

348. Article 29 Data Protection Working Party, Opinion Nº 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP 138, Brussels, 17 August 2007.

349. Article 29 Data Protection Working Party, Joint opinion on the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, WP 145, Brussels, 5 December 2007.

2008

350. Article 29 Data Protection Working Party, Letter to Commission Barrow enclosing the joint comments of the Article 29 Working Party and the Working Party on Police and Justice on the Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, namely: "Preparing the next steps in border management in the European Union", COM (2008) 69 final, "Examining the creation of a European Border Surveillance System (EUROSUR)" COM (2008) 68 final, and "Report on the evaluation and future development of the Frontex Agency" COM (2008) 67 final, WP 149, Brussels, 29 April 2008.

351. Article 29 Data Protection Working Party, Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), WP 150, Brussels, 15 May 2008.

352. Article 29 Data Protection Working Party, Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 2008, WP 151, Brussels, 24 June 2008.

2009

353. Article 29 Data Protection Working Party, Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), WP 159, Brussels, 10 February 2009.

354. Article 29 Data Protection Working Party, Opinion 8/2009 on the protection of passenger data collected and processed by duty-free shops at airports and ports, WP 167, Brussels, 1 December 2009.

355. Article 29 Data Protection Working Party, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009. **[part of short analysis]**

2010

356. Article 29 Data Protection Working Party, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, WP 172, Brussels, 13 July 2010.

357. Article 29 Data Protection Working Party, Opinion 5/2012 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 175, Brussels, 13 July 2010.

358. Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries WP 178, Brussels, 12 November 2010.

2011

359. Article 29 Data Protection Working Party, Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications; Annex: Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180, Brussels, 11 February 2011.

360. Article 29 Data Protection Working Party, Opinion 10/2011 on the 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, WP 181, Brussels, 5 April 2011.

361. Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, Brussels, 16 May 2011.

362. Article 29 Data Protection Working Party, Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, WP 186, Brussels, 13 June 2011.

2012

363. Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, WP 192, Brussels, 22 March 2012. **[part of short analysis]**

364. Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, WP 191, Brussels, 23 March 2012. **[part of short analysis]**

1.2.11 European Data Protection Supervisor (EDPS)

2005

365. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Council decision on the exchange of information from criminal records (COM (2004) 664 final of 13 October 2004), Brussels, 13 January 2005.

366. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM(2004)835 final), Brussels, 23 March 2005.

367. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API)/Passenger Name Record (PNR) data (COM(2005) 200 final), Brussels, 15 June 2005.

368. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final), Brussels, 26 September 2005. **[part of short analysis]**

369. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on three Proposals regarding the Second Generation Schengen Information System (SIS II) (COM (2005)230 final, COM (2005)236 final and COM (2005)237 final), Brussels, 19 October 2005.

370. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM (2005) 475 final), Brussels, 19 December 2005.

2006

371. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final), Brussels, 20 January 2006.

372. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM (2005) 490 final), Brussels, 28 February 2006.

373. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 1073/1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), Brussels, 27 October 2006.

374. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications (COM (2006) 269 final) —2006/0088 (COD), Brussels, 27 October 2006.

2007

375. European Data Protection Supervisor (EDPS), Opinion on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007) 96, Brussels, 20 December 2007.

376. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, Brussels, 20 December 2007.

377. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, Brussels, 25 July 2007.

378. European Data Protection Supervisor (EDPS), Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, Brussels, 27 April 2007.

379. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 515/97 on mutual assistance between administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (COM(2006) 866 final), Brussels, 22 February 2007.

380. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision establishing the European Police Office (Europol) — COM(2006) 817 final, Brussels, 16 February 2007.

2008

381. European Data Protection Supervisor (EDPS), Opinion on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (2008/C 110/01), Official Journal of the European Union, C 110/1, 1 May 2008.

382. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Brussels, 26 March 2008.

383. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of

personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Brussels, 10 April 2008.

384. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Initiative with a view to adopting a Council Decision concerning the strengthening of Eurojust and amending Decision 2002/187/JHA, Brussels, 25 April 2008.

385. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, Brussels, 23 June 2008.

386. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2008/…/JHA, Brussels, 16 September 2008.

387. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, Brussels, 11 November 2008.

388. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee towards a European e-Justice Strategy, Brussels, 19 December 2008.

2009

389. European Data Protection Supervisor (EDPS), Second opinion on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2009/C 128/04), Brussels, 9 January 2009.

390. European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen, (2009/C 276/02), Brussels, 10 July 2009.

391. European Data Protection Supervisor (EDPS), Opinion on the proposal for a Council Regulation amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban (2009/C 276/01), Brussels, 28 July 2009.

392. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (…/…) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a

third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (2010/C 92/01), Brussels, 7 October 2009.

393. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty (2010/C 70/02), Brussels, 7 December 2009.

2010

394. European Data Protection Supervisor (EDPS), Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels, 18 March 2010. www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation/OpinionsC/OC2010 **[part of short analysis]**

395. European Data Protection Supervisor (EDPS), Opinion on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), Brussels, 17 May 2010.

396. European Data Protection Supervisor (EDPS), Opinion on a Proposal for a Council Decision on the conclusion 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 purposes of the Terrorist Finance Tracking Program (TFTP II), Brussels, 22 June 2010.

397. European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice", Brussels, 30 September 2010.

398. European Data Protection Supervisor (EDPS), Opinion on the European Protection Order and European Investigation Order in criminal matters, Brussels, 5 October 2010.

399. European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, Brussels, 19 October 2010.

400. European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission to the European Parliament and the Council - "The EU Counter-Terrorism Policy: main achievements and future challenges", Brussels, 24 November 2010.

401. European Data Protection Supervisor (EDPS), Opinion on the Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…], Brussels, 15 December 2010.

402. European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission to the European Parliament and the Council - "EU Internal Security Strategy in Action: Five steps towards a more secure Europe", Brussels, 17 December 2010.

403. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), Brussels, 20 December 2010.

2011

404. European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", Brussels, 14 January 2011.

405. European Data Protection Supervisor (EDPS), Opinion on the 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, Brussels, 25 March 2011.

406. European Data Protection Supervisor (EDPS), Opinion on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), Brussels, 31 May 2011.

407. European Data Protection Supervisor (EDPS), Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration, Brussels, 7 July 2011.

408. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, Brussels, 15 July 2011.

409. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor, on the Proposal for a Regulation of the European Parliament and of the Council on European statistics on safety from crime, Brussels, 19 September 2011.

410. European Data Protection Supervisor (EDPS), Opinion on net neutrality, traffic management and the protection of privacy and personal data, Brussels, 7 October 2011.

411. European Data Protection Supervisor (EDPS), Opinion on the legislative package on the victims of crime, including a proposal for a Directive establishing minimum stand-

ards on the rights, support and protection of the victims of crime and a proposal for a Regulation on mutual recognition of protection measures in civil matters, OJ C 35/02, Brussels, 17 October 2011.

412. European Data Protection Supervisor (EDPS), Opinion on the Proposal for a Council Decision on the conclusion 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, Brussels, 9 December 2011.

2012

413. European Data Protection Supervisor (EDPS), Opinion on the data protection reform package, Brussels, 7 March 2012. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf **[part of short analysis]**

414. European Data Protection Supervisor (EDPS), Opinion on the proposal for a decision of the European Parliament and of the Council on serious cross-border threats to health, Brussels, 28 March 2012. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-28_Threats_health_EN.pdf

415. European Data Protection Supervisor (EDPS), Opinion on the 'Open-Data Package' of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents, Brussels, 18 April 2012.

416. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America, Brussels, 24 April 2012.

1.3 OTHER EUROPEAN POLICIES

1.3.1 Security and privacy-relevant transport policies

2006

417. European Commission, Keep Europe moving - Sustainable mobility for our continent: Mid-term review of the European Commission's 2001 Transport White Paper, Communication from the Commission to the Council and the European Parliament, COM(2006) 314 final, Brussels, 22 June 2006.

2007

418. European Commission, Freight Transport Logistics Action Plan, Communication from the Commission, COM(2007) 607 final, Brussels, 18 October 2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0607:EN:NOT

419. European Commission, Communication on a European Ports Policy, Communication from the Commission, COM(2007) 616 final, Brussels, 18 October 2007. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0616:EN:HTML:NOT

2009

420. European Commission, Strategic goals and recommendations for the EU's maritime transport policy until 2018, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, COM(2009) 8 final, Brussels, 21 January 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0008:EN:HTML:NOT

421. European Commission, A sustainable future for transport: Towards an integrated, technology-led and user Friendly System, Communication from the Commission, COM(2009) 279 final, Brussels, 17 June 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0279:EN:HTML:NOT

422. EDPS, Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes (2010/C 47/02), Brussels, 22 July 2009.

2011

423. DG Mobility and Transport, Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system, White Paper, COM(2011) 144 final, Brussels, 28 March 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0144:EN:NOT

424. European Commission, Accompanying the White Paper - Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system, Commission Staff Working Document, SEC(2011) 391 final, Brussels, 28 March 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011SC0391:EN:NOT

425. European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and the Council, COM(2011) 451 final, Brussels, 19 July 2011.

426. EDPS, Opinion of the European Data Protection Supervisor, on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and the Council, Brussels, 5 October 2011.

1.3.2 Security and privacy-relevant financial policies

2008

427. EU Financial Intelligence Units' Platform, *Report on Confidentiality and Data Protection in the Activity of FIUs*, Brussels, 28 April 2008.

2010

428. European Union, 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, OJ L 195, 27 July 2010, p. 5–14. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:22010A0727(01):EN:NOT

2011

429. EDPS, Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories, Brussels, 19 April 2011.

430. European Commission, Commission Staff Working Paper on Anti-money laundering supervision of and reporting by payment institutions in various cross-border situations, SEC(2011) 1178 final, Brussels, 4 October 2011.

2012

431. EDPS, Opinion of the European Data Protection Supervisor on the Commission proposals for a Directive of the European Parliament and of the Council on markets in financial instruments repealing Directive 2004/39/EC of the European Parliament and of the Council (Recast), and for a Regulation of the European Parliament and of the Council on markets in financial instruments and amending Regulation on OTC derivatives, central counterparties and trade repositories, Brussels, 10 February 2012.

432. European Commission, Report from the Commission to the European Parliament and the Council on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, COM(2012) 168 final, Brussels, 11 April 2012.

1.3.3 Security and privacy-relevant health policies

2002

433. European Commission, eEurope 2005: An information society for all, Communication from the Commission to the Council and the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2002) 263 final, Brussels, 28 May 2002.

2003

434. High Level Committee on Health, *Health Telematics Working Group of the High Level Committee on Health: Final Report*, Health & Consumer Protection Directorate-General, European Commission, April 2003.

2004

435. European Commission, e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area, Communication from the Commission to the Council and the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2004) 356 final, Brussels, 30 April 2004. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0356:EN:NOT

2005

436. DG Health and Consumer Protection, *Patient Safety – Making it Happen!*, Luxembourg Declaration on Patient Safety Luxembourg, European Commission, 5 April 2005.

437. European Commission, Healthier, safer, more confident citizens: a Health and Consumer protection Strategy, Communication from the Commission to the Council and the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2005) 115 final Brussels, 6 April 2005.

438. European Commission, i2010 – A European Information Society for growth and employment, Communication from the Commission to the Council and the European Parliament, the European Economic and Social Committee and the Committee of the Regions, COM(2005) 229 final, Brussels, 1 June 2005.

2008

439. European Commission, Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C(2008) 3282), OJ L 190, 18 July 2008, pp. 37–43. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008H0594:EN:NOT

440. European Commission, Communication from the Commission to the Council and the European Parliament, the European Economic and Social Committee and the Committee of Regions on telemedicine for the benefit of patients, healthcare systems and socie-

ty, COM(2008) 689 final, Brussels, 4 November 2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0689:EN:NOT

441. EDPS, Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, Brussels, 2 December 2008.

2009

442. European Commission, *2009 ICT Standardisation Work Programme*, 19 June 2009.

443. Council of the European Union, *Council Conclusions on Safe and efficient healthcare through eHealth*, 2980th Employment, Social Policy, Health and Consumer Affairs Council meeting, Brussels, 1 December 2009.

1.3.4 Security and privacy-relevant immigration policies

2000

444. European Parliament, Resolution on the report from the Commission to the Council and the European Parliament on the implementation of Directives 90/364/EEC , 90/365/EEC and 93/96/EEC (right of residence) and on the communication from the Commission to the Council and the European Parliament on the special measures concerning the movement and residence of citizens of the Union which are justified on grounds of public policy, public security or public health (COM(1999) 127, COM(1999) 372 - C5-0177/1999 , C5-0178/1999 - 1999/2157(COS)), 6 September 2000.

2007

445. Council of the European Union, Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7 August 2007, pp. 63–84. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0533:EN:NOT

2008

446. Council of the European Union, Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13 August 2008, pp. 129–136. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0633:EN:NOT

2009

447. European Commission, Commission Decision of 9 October 2009 laying down specifications for the resolution and use of fingerprints for biometric identification and verification in the Visa Information System (notified under document C(2009) 7435)

2009/756/EC, OJ L 270, 15 October 2009, pp. 14–17. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009D0756:EN:NOT

2010

448. European Commission, Commission Decision of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure (2010/261/EU), OJ L 112, 5 May 2010, pp. 31-37.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32010D0261:EN:NOT

449. European Commission, Commission Decision of 4 May 2010 on the Security Plan for the operation of the Visa Information System (2010/260/EU), OJ L 112, 5 May 2010, pp. 25–30.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32010D0260:EN:NOT

1.4 UNITED KINGDOM SECURITY AND PRIVACY POLICY DOCUMENTS

1.4.1 UK Parliament, House of Commons

2001

450. House of Commons Defence Committee, The Threat from Terrorism, Second Report of Session 2001-02, HC 348, The Stationery Office Limited, London, 18 December 2001.

2002

451. House of Commons Defence Committee, Defence and Security in the UK, Sixth Report of Session 2001-02, HC 518, The Stationery Office Limited, London, 24 July 2002.

2004

452. House of Commons Home Affairs Committee, Identity Cards, Fourth Report of Session 2003-04, HC 130-I, The Stationery Office, London, 30 July 2004.

2006

453. House of Commons, Report of the Official Account of the Bombings in London on 7th July 2005, HC 1087, The Stationery Office, London, 11 May 2006.

454. House of Commons Science and Technology Committee, Identity Card Technologies: Scientific Advice, Risk and Evidence, HC 1032, The Stationery Office, London, 4 August 2006.

2008

455. House of Commons Justice Committee, Protection of Private Data, First Report of Session 2007-08, HC 154, The Stationery Office Limited, London, 3 January 2008.

456. House of Commons Home Affairs Committee, A Surveillance Society?, Fifth Report of Session 2009-10, HC 58-I, The Stationery Office, London, 8 June 2008. **[part of short analysis]**

457. House of Commons Home Affairs Committee, A Surveillance Society: Information Commissioner's Response to the Committee's Fifth Report of Session 2007-08, Second Special Report of Session 2007-08, HC 1124, The Stationery Office, London, 5 December 2008.

2009

458. House of Commons Home Affairs Committee, Project CONTEST: The Government's Counter-Terrorism Strategy, Ninth Report of Session 2008-09, HC 212, The Stationery Office, London, 7 July 2009.

459. House of Commons Home Affairs Committee, The E-Borders Programme, Third Report of Session 2009-10, HC 170, The Stationery Office, London, 18 December 2009.

2010

460. House of Commons Home Affairs Committee, The Home Office's Response to Terrorist Attacks, Sixth Report of Session 2009-10, HC 117-I, The Stationery Office, London, 2 February 2010.

461. House of Commons Home Affairs Committee, The National DNA Database, Eighth Report of Session 2009-10, HC 222-I, The Stationery Office, London, 8 March 2010.

462. House of Commons Home Affairs Committee, The Government's Approach to Crime Prevention, Tenth Report of Session 2009-10, HC 242-I, The Stationery Office, London, 23 March 2010.

463. House of Commons Home Affairs Committee, Counter-Terrorism Measures in British Airports, Ninth Report of Session 2009-10, HC 311, The Stationery Office, London, 24 March 2010.

464. House of Commons Communities and Local Government Committee, Preventing violent extremism, Sixth Report of Session 2009-10, HC 65, The Stationery Office Limited, London, 30 March 2010.

465. House of Commons Home Affairs Committee, UK Border Agency: Follow-up on Asylum Cases and E-Borders Programme, Twelfth Report of Session 2009-10, HC 406, The Stationery Office, London, 07 April 2010.

2011

466. House of Commons Home Affairs Committee, The Work of the UK Border Agency, Fourth Report of the Session 2010-12, HC 587-I, The Stationery Office, London, 11 January 2011.

467. House of Commons Home Affairs Committee, Information Commissioner's Annual Report to the House of Commons, etc., Fourth Special Report of Session 2010-12, HC 702, The Stationery Office, London, 01 March 2011 [this contains the SSN's Update Report on Surveillance].

468. House of Commons Home Affairs Committee, The Work of the UK Border Agency: etc., Eighth Special Report of Session 2010-12, HC 1027, The Stationery Office, London, 16 May 2011.

469. House of Commons Home Affairs Committee, The Work of the UK Border Agency (November 2010-March 2011), Ninth Report of Session 2010-12, HC 929, The Stationery Office Limited, London, 02 June 2011.

470. House of Commons Defence Committee, The Strategic Defence and Security Review and the National Security Strategy, Sixth Report of Session 2010-12, HC 761, The Stationery Office Limited, London, 03 August 2011.

471. House of Commons Defence Committee, The Strategic Defence and Security Review, First Report of Session 2010-12, HC 345, The Stationery Office Limited, London, 15 September 2011.

472. House of Commons Home Affairs Committee, New landscape of policing, Fourteenth Report of Session 2010-12, HC 939, The Stationery Office Limited, London, 23 September 2011.

473. House of Commons Justice Committee, Referral fees and the theft of personal data: evidence from the Information Commissioner, Ninth Report of Session 2010-12, HC 1473, The Stationery Office Limited, London, 27 October 2011.

474. House of Commons Home Affairs Committee, The work of the UK Border Agency (April-July 2011), Fifteenth Report of Session 2010–12, HC 1497-I, The Stationery Office Limited, London, 04 November 2011.

475. House of Commons Home Affairs Committee, Policing large scale disorder: lessons from the disturbances of August 2011, Volume I, Sixteenth Report of Session 2010–12, HC 1456, The Stationery Office Limited, London, 22 December 2011.

2012

476. House of Commons Home Affairs Committee, UK border controls, Seventeenth Report of Session 2010–12, HC 1647, The Stationery Office Limited, London, 20 January 2012.

477. House of Commons Science and Technology Committee, Malware and cyber crime, Twelfth Report of Session 2010–12, HC 1537, The Stationery Office Limited, London, 2 February 2012.
http://www.publications.parliament.uk/pa/cm201012/cmselect/cmsctech/1537/1537.pdf

478. House of Commons Defence Committee, Developing Threats: Electro-Magnetic Pulses (EMP), Tenth Report of Session 2010-12, HC 1552, 22 February 2012.

479. House of Commons Home Affairs Committee, Work of the UK Border Agency (August-December 2011), Twenty-first Report of Session 2010-12, HC 1722, The Stationery Office Limited, London, 11 April 2012.

1.4.2 UK Parliament, House of Lords

2001

480. House of Lords Constitution Committee, Anti-Terrorism, Crime and Security Bill, Second Report of Session 2001-02, HL Paper 41, The Stationery Office, London, 23 November 2001.

2002

481. House of Lords Constitution Committee, Crime (International Co-operation) Bill, First Report of Session 2002-03, HL Paper 27, The Stationery Office, London, 17 December 2002.

2003

482. House of Lords European Committee, Europol's role in fighting crime, Fifth Report of Session 2002-03, HL Paper 43, The Stationery Office, London, 6 February 2003.

483. House of Lords European Committee, Proposals for a European Border Guard, Twenty-ninth Report of Session 2002-03, HL Paper 133, The Stationery Office, London, 10 July 2003.

2004

484. House of Lords European Committee, Judicial Cooperation in the EU: the role of Eurojust, Twenty-third Report of Session 2003-04, HL Paper 138, The Stationery Office, London, 21 July 2004.

2005

485. Joint Committee on Human Rights, Identity Cards Bill, Fifth Report of Session 2004-05, HL Paper 35/ HC 283, The Stationery Office Limited, London, 2 February 2005.

486. House of Lords Constitution Committee, Prevention of Terrorism Bill, Second Report of Session 2004-05, HL Paper 66, The Stationery Office, London, 3 March 2005.

487. Joint Committee on Human Rights, Prevention of Terrorism Bill, Tenth Report of Session 2004-05, HL Paper 68/ HC 334, The Stationery Office Limited, London, 4 March 2005.

488. House of Lords European Committee, After Madrid: The EU's response to terrorism, Fifth Report of Session 2004-05, HL Paper 90, The Stationery Office, London, 8 March 2005.

489. House of Lords Constitution Committee, Serious Organised Crime and Police Bill, Third Report of Session 2004-05, HL Paper 65, The Stationery Office, London, 8 March 2005.

490. House of Lords Constitution Committee, Identity Cards Bill, Fifth Report of Session 2004-05, HL Paper 82, The Stationery Office, London, 17 March 2005.

491. House of Lords European Committee, The Hague Programme: a five year agenda for EU justice and home affairs, Tenth Report of Session 2004-05, HL Paper 984 The Stationery Office, London, 23 March 2005.

492. House of Lords Constitution Committee, Identity Cards Bill, Third Report of Session 2005-06, HL Paper 44, The Stationery Office, London, 24 October 2005.

493. House of Lords Constitution Committee, Terrorism Bill, Fourth Report of Session 2005-06, HL Paper 82, The Stationery Office, London, 14 December 2005.

2007

494. House of Lords European Committee, Schengen Information System II (SIS II), Ninth Report of Session 2006-07, HL Paper 49, The Stationery Office, London, 2 March 2007.

495. House of Lords European Committee, Prüm: an effective weapon against terrorism and crime?, Eighteenth Report of Session 2006-07, HL Paper 90, The Stationery Office, London, 9 May 2007.

496. House of Lords European Committee, The EU/US Passenger Name Record (PNR) Agreement, Twenty-first Report of Session 2006-07, HL Paper 108, The Stationery Office, London, 5 June 2007.

497. House of Lords Science and Technology Committee, *Personal Internet Security*, Fifth Report of Session 2006–07, HL Paper 165-I, The Stationery Office Limited, London, 10 August 2007.

2008

498. House of Lords European Committee, FRONTEX: The EU external borders agency, Ninth Report of Session 2007-08, HL Paper 60, The Stationery Office, London, 5 March 2008.

499. Joint Committee on Human Rights, Data Protection and Human Rights, Fourteenth Report of Session 2007-08, HL Paper 72/ HC 132, The Stationery Office Limited, London, 14 March 2008.

500. Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights (Tenth Report): Counter-Terrorism Bill, Twentieth Report of Session 2007-08, HL Paper 108/ HC 554, The Stationery Office Limited, London, 14 May 2008.

501. House of Lords European Committee, The Passenger Name Record (PNR) Framework Decision, Fifteenth Report of Session 2007-08, HL Paper 106, The Stationery Office, London, 11 June 2008.

502. House of Lords Science and Technology Committee, Personal Internet Security: Follow-up, Fourth Report of Session 2007-08, HL Paper 131, The Stationery Office Limited, London, 8 July 2008.

503. House of Lords Constitution Committee, Counter-Terrorism Bill: The Role of Ministers, Parliament and the Judiciary, Tenth Report of Session 2007-08, HL Paper 167, The Stationery Office, London, 5 August 2008.

504. Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights (Thirteenth Report): Counter-Terrorism Bill, Thirtieth Report of Session 2007-08, HL Paper 172/ HC 1077, The Stationery Office Limited, London, 8 October 2008.

505. House of Lords European Committee, EUROPOL: coordinating the fight against serious and organised crime, Report of Session 2007-08, HL Paper 183, The Stationery Office, London, 12 November 2008.

506. House of Lords European Committee, Adapting the EU's approach to today's security challenges –the Review of the 2003 European Security Strategy, Thirty-first Report of Session 2007-08, HL Paper 190, The Stationery Office, London, 21 November 2008.

2009

507. House of Lords Constitution Committee, Surveillance: Citizens and the State, Second Report of Session 2008-09, HL Paper 18, The Stationery Office, London, 6 February 2009. **[part of short analysis]**

508. House of Lords European Committee, Civil Protection and Crisis Management in the European Union, Sixth Report of Session 2008-09, HL Paper 43, The Stationery Office, London, 11 March 2009.

509. Joint Committee on Human Rights, Legislative Scrutiny: Coroners and Justice Bill, Eighth Report of Session 2008-09, HL Paper 57/ HC 362, The Stationery Office Limited, London, 20 March 2009.

510. Joint Committee on Human Rights, Demonstrating respect for rights? A human rights approach to policing protest, Seventh Report of Session 2008-09, HL Paper 47-I/ HC 320-I, The Stationery Office Limited, London, 23 March 2009.

511. House of Lords Constitution Committee, Policing and Crime Bill, Sixteenth Report of Session 2008-09, HL Paper 128, The Stationery Office, London, 2 July 2009.

512. House of Lords European Committee, The Stockholm Programme: home affairs, Twenty-fifth Report of Session 2008-09, HL Paper 175, The Stationery Office, London, 9 November 2009

513. House of Lords European Committee, Money laundering and the financing of terrorism, Nineteenth Report of Session 2008-09, HL Paper 132-I, The Stationery Office, London, 22 July 2009.

2010

514. House of Lords European Union Committee, Protecting Europe against large-scale cyber-attacks, HL Paper 68, The Stationary Office, London, 2010.

515. Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights (Sixteenth Report): Annual Renewal of Control Orders Legislation 2010, Ninth Report of Session 2009-10, HL Paper 64/ HC 395, The Stationery Office Limited, London, 26 February 2010.

516. Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights (Seventeenth Report): Bringing Human Rights Back In, Sixteenth Report of Session 2009-10, HL Paper 86/ HC 111, The Stationery Office Limited, London, 9 March 2010.

517. House of Lords Constitution Committee, Crime and Security Bill, Thirteenth Report of Session 2009-10, HL Paper 107, The Stationery Office, London, 25 March 2010.

518. Joint Committee on Human Rights, Legislative Scrutiny: Identity Documents Bill, Second Report of Session 2010-11, HL Paper 36/ HC 515, The Stationery Office Limited, London, 12 October 2010.

2011

519. House of Lords European Union Committee (Sub-Committee F), Money laundering, data protection for suspicious activity reports, Sixth Report of Session 2010-12, HL Paper 82, The Stationery Office, London, 20 January 2011.

520. Joint Committee on Human Rights, Terrorism Prevention and Investigation Measures Bill, Sixteenth Report of Session 2010-12, HL Paper 180/ HC 1432, The Stationery Office Limited, London, 19 July 2011.

521. Joint Committee on Human Rights, The Terrorism Act 2000 (Remedial) Order 2011: Stop and Search without Reasonable Suspicion (second Report), Seventeenth Report of Session 2010-12, HL Paper 192/ HC 1483, The Stationery Office Limited, London, 13 September 2011.

522. House of Lords Constitution Committee, Terrorism Prevention and Investigation Measures Bill, Nineteenth Report of Session 2010-12, HL Paper 198, The Stationery Office, London, 15 September 2011.

523. Joint Committee on Human Rights, Legislative Scrutiny: Protection of Freedoms Bill, Eighteenth Report of Session 2010-12, HL Paper 195/ HC 1490, The Stationery Office Limited, London, 07 October 2011. **[part of short analysis]**

524. Constitution Committee, Protection of Freedoms Bill, Twentieth Report of Session 2010-1, HL Paper 215, The Stationery Office Limited, London, 03 November 2011.

2012

525. Joint Committee on Privacy and Injunctions, Privacy and injunctions, First Report of Session 2010-12, HL Paper 273/ HC 1443, The Stationery Office Limited, London, 27 March 2012.

526. Joint Committee on Human Rights, The Justice and Security Green Paper, Twenty-fourth Report of Session 2010-12, HL Paper 286/ HC 1777, The Stationery Office Limited, London, 04 April 2012.

1.4.3 HM Government

2003

527. HM Government, The Privacy and Electronic Communications (EC Directive) Regulations 2003, 2003. http://www.legislation.gov.uk/uksi/2003/2426/contents/made

528. HM Government, Countering International Terrorism: The United Kingdom's Strategy, Presented to Parliament by the Prime Minister and the Secretary of State for the Home Department by Command of Her Majesty, The Stationary Office, July 2006.

529. HM Government, A Strong Britain in an Age of Uncertainty: The National Security Strategy, The Stationary Office, London, 2010.
http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy

530. HM Government, Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, The Stationary Office, London, 2010.
http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf

1.4.4 Cabinet Office

2002

531. Cabinet Office, *The United Kingdom and The Campaign against International Terrorism*, Progress Report, 9 September 2002.

2008

532. The Cabinet Office, The National Security Strategy of the UK: Security in an Interdependent World, TSO, London, 2008.

http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf

2009

533. UK Office of Cyber Security, Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space, Parliament Command Paper 7642, London, 2009.

534. UK Cabinet Office, *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*, 2009. www.cabinetoffice.gov.uk/media/349103/strategic-framework.pdf

2010

535. The Secretary of State for the Home Department, *Cyber Crime*, The Stationary Office, London, 2010. http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf

2011

536. Detica and the Office of Cyber Security and Information Assurance, *The Cost of Cyber Crime*, Surrey, February 2011.

537. The Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, The Stationary Office, London, 2011. http://www.getsafeonline.org/media/CyberSecurityWeb.pdf

538. The Cabinet Office, US - UK Cyber Communique, 25 May 2011. http://www.cabinetoffice.gov.uk/resource-library/us-uk-cyber-communique

539. Francis Maude, "Making Travel Safer in Cyberspace", Minister for the Cabinet Office and Cyber Security, London, 1 June 2011. http://www.cabinetoffice.gov.uk/news/making-travel-safer-cyberspace

1.4.5 Ministry of Defence

2003

540. Ministry of Defence, Delivering Security in a Changing World: Defence White Paper, The Stationary Office, London, December 2003. http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/

2004

541. Ministry of Defence, *Delivering Security in a Changing World: Future Capabilities*, The Stationary Office, London, July 2004. http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/PolicyStrategyAndPlanning.htm

2005

542. Secretary of State for Defence, Defence Industrial Strategy: Defence White Paper, The Stationary Office, London, 2005. http://merln.ndu.edu/whitepapers/UnitedKingdom-2005.pdf

2006

543. Ministry of Defence, *Defence Technology Strategy for the Demands of the 21st Century*, The Stationary Office, London, 2006. http://www.mod.uk/nr/rdonlyres/27787990-42bd-4883-95c0-b48bb72bc982/0/dts_complete.pdf

2011

544. Ministry of Defence, *Defence Reform*, The Stationary Office, London, 2011. http://www.mod.uk/NR/rdonlyres/B4BA14C0-0F2E-4B92-BCC7-8ABFCFE7E000/0/defence_reform_report_struct_mgt_mod_27june2011.pdf

545. Ministry of Defence, *The Strategy for Defence*, The Stationary Office, London, 2011. http://www.mod.uk/NR/rdonlyres/0A42D98D-99B0-4939-8635-98E172EBCADC/0/stategy_for_defence_oct2011.pdf

2012

546. Ministry of Defence, *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security*, The Stationary Office, London, February 2012. **[part of short analysis]**

1.4.6 Home Office

2002

547. Welsh, Brandon C., and David P. Farrington, *Crime prevention effects of closed circuit television: a systematic review*, Home Office Research Study 252, Home Office Research, Development and Statistics Directorate, August 2002.

548. John Wheeler, *Airport Security*, Home Office Report, 30 October 2002.

2004

549. Home Office, *Counter-terrorism Powers: Reconciling Security and Liberty in an Open Society: A Discussion Paper*, February 2004.

2007

550. Home Office, *The United Kingdom Security & Counter-Terrorism Science & Innovation Strategy*, 2007.

551. Home Office, *Cutting Crime: A new partnership 2008-11*, July 2007.

552. Graeme Gerrard, Garry Parkins, Ian Cunningham, Wayne Jones, Samantha Hill And Sarah Douglas, *National CCTV Strategy, Home Office and the Association of Chief Police Officers (ACPO)*, October 2007.

2009

553. Home Office, *London 2012: Olympic and Paralympic Safety and Security Strategy*, July 2009.

554. Home Office, *The United Kingdom's Science and Technology Strategy for Countering International Terrorism*, August 2009.

2010

555. Home Office, The United Kingdom's Strategy for Countering Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism, March 2010

2011

556. Home Office, *The UK's opt-in to Council Decision to sign and conclude the EU-Australia PNR Agreement – WMS*, 5 September 2011. http://www.homeoffice.gov.uk/publications/about-us/parliamentary-business/written-ministerial-statement/uk-opt-in-eu-australia/?view=Standard&pubID=940357

2012

557. Home Office, UK's opt-in to the EU PNR Agreement with the US, Written ministerial statement, 27 February 2012. http://www.homeoffice.gov.uk/publications/about-us/parliamentary-business/written-ministerial-statement/eu-pnr-agreement-wms/?view=Standard&pubID=1009861

1.4.7 Information Commissioner's Office (ICO)

558. Information Commissioner's Office, *The Guide to Data Protection*, Information Commissioner's Office, Cheshire, no date. https://www.ico.gov.uk/tools_and_resources/request_publications.aspx

2006

559. Information Commissioner's Office, *What price privacy?: The unlawful trade in confidential personal information*, The Stationary Office, London, May 2006.

560. Surveillance Studies Network, *A Report on the Surveillance Society For the Information Commissioner*, Information Commissioner's Office, September 2006. http://www.ico.gov.uk/about_us/research/reports_to_parliament.aspx **[part of short analysis]**

561. Information Commissioner's Office, *What price privacy now?: The first six months progress in halting the unlawful trade in confidential personal information*, Information Commissioner's Office, December 2006.

http://www.ico.gov.uk/about_us/research/reports_to_parliament.aspx

2008

562. Information Commissioner's Office, *CCTV Code of Practice*, Information Commissioner's Office, Cheshire, January 2008.
https://www.ico.gov.uk/tools_and_resources/request_publications.aspx

2009

563. Information Commissioner's Office, *Information Commissioner's Annual Report 2008/09*, The Stationary Office, July 2009.
http://www.ico.gov.uk/about_us/performance/annual_reports.aspx

564. Information Commissioner's Office, Information Commissioner's response to "Protecting the Public in a Changing Communication Environment": A consultation by the Home Office, 15 July 2009.
http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

2010

565. Information Commissioner's Office, *Information Commissioner's Annual Report 2009/10: Upholding information rights in a changing environment*, The Stationary Office, July 2010. http://www.ico.gov.uk/about_us/performance/annual_reports.aspx

566. Information Commissioner's Office, The Information Commissioner's response to the Home Office consultation paper on the retention, use and destruction of DNA data and fingerprints, 7 August 2009.
http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

567. Information Commissioner's Office, The Information Commissioner's response to the consultation on 'Policing in the 21st Century: reconnecting police and the people', 20 September 2010.
http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

568. Information Commissioner's Office, The Information Commissioner's response to the Ministry of Justice's call for evidence on the current data protection legislative framework, 6 October 2010.
http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

569. Surveillance Studies Network, *Information Commissioner's report to Parliament on the state of surveillance*, Information Commissioner's Office, November 2010. http://www.ico.gov.uk/about_us/research/reports_to_parliament.aspx

570. Information Commissioner's Office, The Information Commissioner's response to the Home Office consultation "The Regulation of Investigatory Powers Act 2000 ('RIPA'): monetary penalties and consents for interception", 17 December 2010. http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

571. Information Commissioner's Office, *Privacy Notices Code of Practice*, Information Commissioner's Office, Cheshire, December 2010.
https://www.ico.gov.uk/tools_and_resources/request_publications.aspx

572. Information Commissioner's Office, *Upholding Information Rights for All: A guide to the legislation the ICO regulates*, Information Commissioner's Office, Cheshire, December 2010.
https://www.ico.gov.uk/tools_and_resources/request_publications.aspx

2011

573. Information Commissioner's Office, The Information Commissioner response to The Council of Europe's consultation on The Modernisation of Convention 108, 3 March 2011. http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

574. Information Commissioner's Office, The Information Commissioner's response to the Consultation on the Code of recommended practice for local authorities on data transparency, 14 March 2011.
http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

575. Information Commissioner's Office, The Information Commissioner's Submission to the Home Affairs Committee's Call for Evidence on the New Landscape of Policing, 31 March 2011.
http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

576. Information Commissioner's Office, The Information Commissioner's response to the Consultation on Smart Metering Spring Package – Addressing Consumer Protection Issues, 8 April 2011.
http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

577. Information Commissioner's Office, The Information Commissioner's response to the Home Office consultation on a code of practice relating to surveillance cameras, 25 May 2011. http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

578. Information Commissioner's Office, *Data Sharing Code of Practice*, Information Commissioner's Office, Cheshire, May 2011.
https://www.ico.gov.uk/tools_and_resources/request_publications.aspx

579. Information Commissioner's Office, *Information Commissioner's Annual Report and Financial Statements: Information is the currency of democracy*, The Stationary Office, July 2011. http://www.ico.gov.uk/about_us/performance/annual_reports.aspx

580. Information Commissioner's Office, Commission on a Bill of Rights Discussion paper - do we need a Bill of Rights? Response from the Information Commissioner's Office, 11 November 2011.
http://www.ico.gov.uk/about_us/consultations/consultation_responses.aspx

1.5 NETHERLANDS SECURITY AND PRIVACY POLICY DOCUMENTS

1.5.1 Kabinet (Cabinet, i.e. Prime Minister and Ministers)

2000

581. Cabinet of the Netherlands, Informatie- en communicatietechnologie; Kabinetsstandpunt met betrekking tot het advies *ICT en het recht om anoniem te zijn* van de Raad voor het openbaar bestuur [Goverments opinion on the report *ICT and the right to be anonymous* – unofficial translation], 24 July 2000. http://www.parlement.com/9353000/1f/j9vvhy5i95k8zxl/vi3ai7q9qzzk

2007

582. Cabinet of the Netherlands, Wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de verbetering van de mogelijkheden van de inlichtingen- en veiligheidsdiensten om onderzoek te doen naar en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid [Changes to the Law on Security and Intelligence Agencies 2002 with regards to improving capabilities of these agencies to perform inquiries and take measures against terrorism and other dangers to national security – unofficial translation], 10 July 2007. https://zoek.officielebekendmakingen.nl/kst-30553-7.html

2008

583. Cabinet of the Netherlands, Kabinetsstandpunt inzake de aanbevelingen in onderzoeksrapport 'Bestuur, recht en veiligheid: bestuursrechtelijke bevoegdheden voor openbare ordehandhaving en terrorismebestrijding' [Official position government – report on governance, rule of law and the fight against terrorism – unofficial translation], 6 May 2008. https://zoek.officielebekendmakingen.nl/kst-28684-134-b2.html

2009

584. Cabinet of the Netherlands, Evaluatie Wet bescherming persoonsgegevens; Kabinetsstandpunt inzake advies Commissie Brouwer-Korf en evaluatie van de Wet bescherming persoonsgegevens [Government opinion regarding advice by Commission Brouwer-Korf and evaluation of the data protection law – unofficial translation], November 2009.
https://zoek.officielebekendmakingen.nl/kst-31051-5.html

2011

585. Cabinet of the Netherlands, Verwerking en bescherming persoonsgegevens; Brief regering; Notitie inzake privacybeleid. Kabinetsstandpunt inzake gegevensverwerking en gegevensbescherming en een nadere visie op de Europese en internationale ontwikkeling op het gebied van gegevensverwerking. [Official position of the Dutch Government on issues of data processing, data protection and security – unofficial translation], 31 May 2011.
https://zoek.officielebekendmakingen.nl/kst-32761-1.html

586. Cabinet of the Netherlands, Informatie- en communicatietechnologie (ICT); Brief regering; Kabinetsreactie op WRR-rapport iOverheid: de rol van de overheid in de iS-amenleving [Answer Dutch Gov to the report iGovernment – role of the Government in the iSociety – unofficial translation], 27 October 2011. https://zoek.officielebekendmakingen.nl/kst-26643-211.html

1.5.2 Eerste Kamer (Senate, i.e. First Chamber of Parliament)

2001

587. Senate of the Netherlands, Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten [Rules concerning inquiries office and security office and adaption of some bills in response to 9/11– unofficial translation], 16 November 2001.
http://www.parlement.com/9353000/1f/j9vvhy5i95k8zxl/vi3ajuje46zy?start_00h=20

2002

588. Senate of the Netherlands, Gezamenlijke behandeling van de wetsvoorstellen: - Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten: Wet op de inlichtingen- en veiligheidsdiensten, Verandering in de Grondwet van de bepalingen over het binnentreden in woningen [Rules concerning inquiry office and security office and changes in the Constitution concerning entering houses – unofficial translation], 5 February 2002. https://zoek.officielebekendmakingen.nl/h-ek-20012002-905-919.html

2003

589. Senate of the Netherlands, Voortzetting van de behandeling van het wetsvoorstel Wijziging van de artikelen 139f en 441b van het Wetboek van Strafrecht (uitbreiding strafbaarstelling heimelijk cameratoezicht) [Continuation of the debate regarding the bill on penalising secret video surveillance – unofficial translation], 6 May 2003. https://zoek.officielebekendmakingen.nl/h-ek-20022003-736-742.html

2004

590. Senate of the Netherlands, Wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens [Senate discussion on the handling of (personal) data by police and justice – unofficial translation], 2 April 2004.
https://zoek.officielebekendmakingen.nl/h-ek-20032004-1030-1037.html

591. Senate of the Netherlands, Parlementaire behandeling van het wetsvoorstel Regeling van DNA-onderzoek bij veroordeelden [Parliamentary discussion of a law on handling DNA information and tests by convicted criminals – unofficial translation], 29 September 2004.
https://zoek.officielebekendmakingen.nl/h-ek-20032004-2214-2222.html

2009

592. Senate of the Netherlands, Ontwerpbesluiten Unie-Verdrag; Verslag schriftelijk overleg over bodyscans op Europese luchthavens [Debate following the answer of the Minister of Justice to public outcry re use of body scans at airports – unofficial translation], 9 January 2009.
https://zoek.officielebekendmakingen.nl/kst-20082009-23490-EG.html

2010

593. Senate of the Netherlands, Evaluatie Wet bescherming persoonsgegevens; Verslag van een Schriftelijk Overleg [Written evaluation of the Dutch Data Protection Law – unofficial translation], 8 June 2010.
https://zoek.officielebekendmakingen.nl/kst-31051-A.html

2011

594. Senate of the Netherlands, Evaluatie Wet bescherming persoonsgegevens; Verslag van een expertmeeting inzake de rol van de overheid bij digitale dataverwerking [Evaluation of the Data Protection Law – notes of the expert meeting organised by the Upper Chamber of Parliament with chair Article 29, EDPS, etc. – unofficial translation], 22 March 2011.
https://zoek.officielebekendmakingen.nl/kst-31051-B.html **[part of short analysis]**

1.5.3 Tweede Kamer (Second Chamber of Parliament)

2000

595. Parliament of the Netherlands, *Rapport Commissie Grondrechten in het digitale tijdperk* [Report of the Commission Constitutional rights in the digital era – unofficial translation], May 2000.
http://www.ivir.nl/dossier/grondrechten/bronnen/rapport_gdt_samenvatting_5-00.pdf

596. Parliament of the Netherlands, Wijziging wetten ivm nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II); Verslag van het voorbereidend onderzoek door de vaste commissie van Justitie [Research in support of proposed law changes re developments brought about by the information society – computer crime – unofficial translation], 27 September 2000.
https://zoek.officielebekendmakingen.nl/kst-26671-6.html

597. Parliament of the Netherlands, Wetgeving voor de elektronische snelweg; Notitie 'Internationalisering en Recht in de Informatiemaatschappij' [Note regarding laws for the digital highway – unofficial translation], 30 May 2000. https://zoek.officielebekendmakingen.nl/kst-25880-10.html

2001

598. Parliament of the Netherlands, Bestrijding internationaal terrorisme; Verslag algemeen overleg op 17 oktober 2001, over terrorismebestrijding en veiligheid [Fighting international terrorism; report of a general meeting about fighting terrorism and security – unofficial translation], 1 November 2001. https://zoek.officielebekendmakingen.nl/kst-27925-19.html **[part of short analysis]**

599. Parliament of the Netherlands, Criminaliteitsbeheersing; Verslag nota-overleg [Controlling criminality: report of meeting – unofficial translation], 8 November 2001. https://zoek.officielebekendmakingen.nl/kst-27834-11.html

600. Parliament of the Netherlands,Wijz. van o.a. Wetboek van Strafvordering i.v.m. aanpassing bevoegdheden vorderen gegevens telecommunicatie; Memorie van toelichting [Changes in the criminal code with respect to adaptions in the power to claim information from telecommunications – unofficial translation], 2 November 2001. https://zoek.officielebekendmakingen.nl/kst-28059-3.html

2002

601. Parliament of the Netherlands, Wijziging artikelen 139f en 441b Wetboek van Strafrecht (uitbreiding strafbaarstelling heimelijk cameratoezicht); Nota n.a.v. het verslag [Extension of penalisation of covert video surveillance – unofficial translation], 9 January 2002. https://zoek.officielebekendmakingen.nl/kst-27732-6.html

602. Parliament of the Netherlands, Grootschalig afluisteren van moderne telecommunicatiesystemen; Verslag algemeen overleg op 29 november 2001 [Content document: technical and legal assessment of the privacy directive – unofficial translation], 7 February 2002. https://zoek.officielebekendmakingen.nl/kst-27591-3.html

603. Parliament of the Netherlands, Wijz. van o.a. Wetboek van Strafvordering i.v.m. aanpassing bevoegdheden vorderen gegevens telecommunicatie; Verslag [Changes in the criminal code with respect to the power to claim information from telecommunications – unofficial translation], 3 April 2002 https://zoek.officielebekendmakingen.nl/kst-20022003-28059-187a.html

604. Parliament of the Netherlands, Wet justitiële gegevens; Verslag wetgevingsoverleg op 25 maart 2002 [Judicial information act; report of a legislation meeting – unofficial translation], 5 April 2002. https://zoek.officielebekendmakingen.nl/kst-24797-23.html

605. Parliament of the Netherlands, Integriteit Financiële sector en terrorismebestrijding; Lijst van vragen en antwoorden [Integrity of the financial sector and fighting terrorism: list of questions and answers – unofficial translation], 10 April 2002. https://zoek.officielebekendmakingen.nl/kst-28106-4.html

606. Parliament of the Netherlands, Behandeling van het wetsvoorstel Wijziging van de artikelen 139f en 441b van het Wetboek van Strafrecht (uitbreiding strafbaarstelling heimelijk cameratoezicht) [Expansion of penalisation covert video surveillance – unofficial translation], 4 September 2002.
https://zoek.officielebekendmakingen.nl/h-tk-20012002-5584-5607.html

607. Parliament of the Netherlands, Naar een veiliger samenleving; Lijst van vragen en antwoorden [To a more secure society: list of questions and answers – unofficial translation], 5 December 2002. https://zoek.officielebekendmakingen.nl/kst-28684-3.html

2003

608. Parliament of the Netherlands, Wijziging Telecommunicatiewet i.v.m. implementatie richtlijnen 97/66/EG en 2002/58/EG bescherming persoonlijke levenssfeer; Memorie van toelichting [Changes in the Telecommunications Act concerning implementation of 97/66/EG en 2002/58/EG protection of private life – unofficial translation], 24 June 2003. https://zoek.officielebekendmakingen.nl/kst-28962-3.html

609. Parliament of the Netherlands, Wet op de uitgebreide identificatieplicht; Memorie van toelichting [Law concerning extensive obligation to carry identification – unofficial translation], 29 September 2003. https://zoek.officielebekendmakingen.nl/kst-29218-3.html

610. Parliament of the Netherlands, Wet op de uitgebreide identificatieplicht; Advies en nader rapport [Law concerning extensive obligation to carry identification: advice and report – unofficial translation], 29 September 2003. https://zoek.officielebekendmakingen.nl/kst-29218-5.html

611. Parliament of the Netherlands, Behandeling van het wetsvoorstel Vaststelling van de begrotingsstaat van het Ministerie van Justitie (VI) voor het jaar 2004 [Consideration of the bill concerning settlement of the budgettary state of the Ministry of Justice for the year 2004 – unofficial translation], 28 October 2003. https://zoek.officielebekendmakingen.nl/h-tk-20032004-943-984.html

612. Parliament of the Netherlands, Voortzetting van de behandeling van het wetsvoorstel Wijziging en aanvulling van het Wetboek van Strafrecht en enige andere wetten in verband met terroristische misdrijven (Wet terroristische misdrijven) [Consideration of the bill concerning changes and additions to the Criminal Code and other laws in connection to terrorist offences – unofficial translation], 4 December 2003. https://zoek.officielebekendmakingen.nl/h-tk-20032004-2333-2362.html

613. Parliament of the Netherlands, Wet op de uitgebreide identificatieplicht; Verslag wetgevingsoverleg [Law concerning extensive obligation to carry identification; report of a meeting – unofficial translation], 18 December 2003. https://zoek.officielebekendmakingen.nl/kst-29218-21.html

2004

614. Parliament of the Netherlands, Wijziging van de Wet justitiële gegevens in verband met het verstrekken van een afschrift van een vonnis of een arrest aan de verdachte en zijn raadsman of een derde. [Update to criminal law with regards to providing information to suspects, their lawyers or others – unofficial translation], 9 January 2004. https://zoek.officielebekendmakingen.nl/kst-28886-5.html

615. Parliament of the Netherlands, Debat over de brief van de minister van Justitie inzake het algemeen kader herziening Wetboek van Strafvordering [Debate on a letter from the Minister of Justice with regards to a revision of criminal law – unofficial translation], 11 February 2004. https://zoek.officielebekendmakingen.nl/h-tk-20032004-3197-3224.html

616. Parliament of the Netherlands, Wijziging van de Gemeentewet en de Wet politieregisters in verband met de invoering van regels omtrent het gebruik van camera's ten behoeve van toezicht op openbare plaatsen [Update to municipality and police register laws with regards to camera surveillance in public spaces – unofficial translation], 1 March 2004. https://zoek.officielebekendmakingen.nl/kst-29440-3.html

617. Parliament of the Netherlands, Bestrijding internationaal terrorisme [Combating international terrorism; answers by the government to questions posed by Parliament – unofficial translation], 4 March 2004. https://zoek.officielebekendmakingen.nl/kst-27925-118.html

618. Parliament of the Netherlands, Wetsvoorstel Regeling van DNA-onderzoek bij veroordeelden [Parliamentary discussion of DNA information of convicted criminals – unofficial translation], 26 March 2004. https://zoek.officielebekendmakingen.nl/h-tk-20032004-3916-3944.html

619. Parliament of the Netherlands, Wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens [Parliamentary discussion of the handling of (personal) data by police and justice – unofficial translation], 19 April 2004. https://zoek.officielebekendmakingen.nl/kst-29441-5.html

620. Parliament of the Netherlands, Wijziging van de Gemeentewet en de Wet politieregisters in verband met de invoering van regels omtrent het gebruik van camera's ten behoeve van toezicht op openbare plaatsen. [Parliamentary discussion of camera surveillance – unofficial translation], 26 April 2004. https://zoek.officielebekendmakingen.nl/kst-29440-5.html

621. Parliament of the Netherlands, Derde voortgangsrapportage over de uitvoering van het Veiligheidsprogramma. [Third progress report on the national security programme – unofficial translation], 7 June 2004. https://zoek.officielebekendmakingen.nl/kst-28684-29.html

622. Parliament of the Netherlands, Parlementsdiscussie: naar een veiliger samenleving. [Parliamentary discussion with ministers of justice, internal affairs and economic affairs on security of society – unofficial translation], 23 June 2004. https://zoek.officielebekendmakingen.nl/kst-28684-32.html

623. Parliament of the Netherlands, Wetsvoorstel Wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens. [Parliamentary discussion of update to criminal law with regards to powers for demanding information by police and justice – unofficial translation], 10 November 2004. https://zoek.officielebekendmakingen.nl/h-tk-20042005-806-822.html

624. Parliament of the Netherlands, Bestrijding internationaal terrorisme; Verslag van een hoorzitting van 24 mei 2004 over de strijd tegen het internationaal terrorisme [Parliamentary debate on combating international terrorism – unofficial translation], 28 June 2004. http://www.parlement.com/9353000/1f/j9vvhy5i95k8zxl/vi3amh2l0bz6

625. Parliament of the Netherlands, Debat over de moord op de heer Th. van Gogh. [Debate on the murder of movie-maker Theo van Gogh by an Islamic extremist – unofficial translation], 25 November 2004.
https://zoek.officielebekendmakingen.nl/h-tk-20042005-1278-1332.html

626. Parliament of the Netherlands, Vaststelling van de begrotingsstaten van het Ministerie van Justitie (VI) voor het jaar 2005. [Report of a discussion on the budget of the Internal Affairs and Justice departments between de respective ministers and Parliament commissions – unofficial translation], 30 December 2004. https://zoek.officielebekendmakingen.nl/kst-29800-VII-29.html

2005

627. Parliament of the Netherlands, Wijziging van de wet op de inlichtingen- en veiligheidsdiensten 2002 in verband met de invoering van een nieuw stelsel van bewaking en beveiliging; Memorie van toelichting [Revised law for the intelligence and security services – unofficial translation], 12 April 2005. https://zoek.officielebekendmakingen.nl/kst-30070-3.html

628. Parliament of the Netherlands, Wijziging Sv en Sr ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven; Memorie van toelichting [Extended investigative powers in the context of the fight against terrorism – unofficial translation], 23 June 2005.
https://zoek.officielebekendmakingen.nl/kst-30164-3.html

629. Erasmus Universiteit Rotterdam, *'Wie wat bewaart die heeft wat'* [Report to Parliament into data retention by the Erasmus University – unofficial translation], 29 June 2005. https://zoek.officielebekendmakingen.nl/kst-23490-379-b1.html

2006

630. Parliament of the Netherlands, Wet bestuurlijke maatregelen nationale veiligheid; Advies en nader rapport [Law administrative measures national security; Advice Council of State – unofficial translation], 9 May 2006.

631. Parliament of the Netherlands, Behandeling van het wetsvoorstel Regels inzake de verwerking van politiegegevens (Wet politiegegevens) (30327) [Debate: Law police data – unofficial translation], 30 June 2006.
https://zoek.officielebekendmakingen.nl/h-tk-20052006-5665-5672.html

2007

632. Parliament of the Netherlands, Behandeling van het wetsvoorstel Regels inzake het opleggen van beperkende maatregelen aan personen met het oog op de bescherming van de nationale veiligheid en inzake het weigeren of intrekken van beschikkingen met het oog op de bescherming van de nationale veiligheid (Wet bestuurlijke maatregelen nationale veiligheid) [Parliamentary debate – law proposal administrative measures national security – unofficial translation], 13 March 2007. https://zoek.officielebekendmakingen.nl/h-tk-20062007-2826-2873.html

2008

633. Parliament of the Netherlands, Evaluatie Wet bescherming persoonsgegevens; Verslag algemeen overleg gehouden op 22 november 2007 [Evaluation of the Dutch Data Protection Law – unofficial translation], 23 January 2008. https://zoek.officielebekendmakingen.nl/kst-31051-2.html

634. Parliament of the Netherlands, Naar een veiliger samenleving; Verslag nota-overleg over rechtshandhaving en internetmisbruik [Report & debate – law enforcement and internet crime – unofficial translation], 28 May 2008. https://zoek.officielebekendmakingen.nl/kst-28684-149.html

635. Parliament of the Netherlands, Rechtsstaat en Rechtsorde; Verslag algemeen overleg gehouden op 19 juni 2008 over o.a. evaluatie privacygedragscode particuliere rechercheburaus [Report of general meeting about evaluation of privacy code of conduct of private detectives – unofficial translation], 7 August 2008. https://zoek.officielebekendmakingen.nl/kst-29279-79.html

636. Parliament of the Netherlands, Ontwerp-Kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken [Debate proposed EC Framework Decision on the protection of personal data that are handled in cooperation between the police and the judiciary system – unofficial translation], 14 November 2008. https://zoek.officielebekendmakingen.nl/kst-23490-529-b1.html

2009

637. Parliament of the Netherlands, Ontwerpbesluiten Unie-Verdrag; Verslag algemeen overleg gehouden op 11 maart 2009 [Debate draft Lisbon Treaty – PNR, anti-terrorism – unofficial translation], 7 April 2009. https://zoek.officielebekendmakingen.nl/kst-23490-552.html

638. Commissie evaluatie antiterrorismebeleid ("Commissie Suyver"), *Naar een integrale evaluatie van antiterrorismemaatregelen* [*Evaluation of anti-terrorism measures from a human rights perspective* – unofficial translation], May 2009. https://zoek.officielebekendmakingen.nl/blg-25780.pdf

639. Parliament of the Netherlands, Wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen; Nota n.a.v. het verslag [Changes to the Data Protection Law concerning the lessening of administrative burdens, changes to recover legal shortages – unofficial translation], 19 June 2009. https://zoek.officielebekendmakingen.nl/kst-31841-8.html

640. Parliament of the Netherlands, Evaluatie van hoofdstuk 13 van de Telecommunicatiewet [Evaluation of chapter 13 Telcom Law; wiretapping – unofficial translation], 7 September 2009. https://zoek.officielebekendmakingen.nl/kst-30517-14.html

2010

641. Parliament of the Netherlands, Evaluatie Wet bescherming persoonsgegevens; Verslag van een algemeen overleg; Verslag van een algemeen overleg, gehouden op 3 februari 2010, inzake persoonsgegevens [Debate / oral evaluation of the Dutch Data Protection Law – unofficial translation], 18 March 2010. https://zoek.officielebekendmakingen.nl/kst-31051-7.html

642. Parliament of the Netherlands, AIVD; Verslag van een algemeen overleg; Verslag van een algemeen overleg, gehouden op 15 september 2010, inzake AIVD-onderwerpen [Debate on the topic of the functioning of the intelligence agency; data storage, monitoring, data mining, commercial contractors, etc. – unofficial translation], 12 October 2010. https://zoek.officielebekendmakingen.nl/kst-30977-36.html

643. Schreijenberg, A., Homburg, G.H.J, Regioplan Beleidsonderzoek, *Eindrapport Evaluatie vijf jaar cameratoezicht op Openbare Plaatsen* [*Final report: Five year evaluation CCTV in public spaces* – unofficial translation], Study commissioned by the two Chambers of Parliament, November 2010. http://www.regioplan.nl/media/pdf/id/873/file_name/1985-steeds-meer-beeld-vijf-jaar-cameratoezicht.pdf

644. Raad voor het openbaar bestuur (Council for Public Governance), ROB-advies Veiligheid en vertrouwen [Advice to Parliament re security & trust – unofficial translation], November 2010. http://www.robrfv.nl/documenten/migratie/boekje_advies_veiligheid_en_vertrouwen.pdf **[part of short analysis]**

645. Parliament of the Netherlands, Antwoord vragen Thieme over Nederland als koploper bij het opvragen van telecomgegevens [Parliamentary Q&A regarding the almost 3 million requests for telecom data by (special) investigation units – unofficial translation], 3 December 2010. https://zoek.officielebekendmakingen.nl/ah-tk-20102011-685.html

2011

646. Parliament of the Netherlands, Behandeling van het wetsvoorstel Wijziging van de Telecommunicatiewet in verband met de aanpassing van de bewaartermijn voor telecommunicatiegegevens met betrekking tot internettoegang, e-mail over het internet en internettelefonie (32185) en het wetsvoorstel Wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen [Parliamentary debate – proposed law changing the current telecommunications law – unofficial translation], 18 July 2011. https://zoek.officielebekendmakingen.nl/h-tk-20102011-93-2.html

647. Parliament of the Netherlands, Verwerking en bescherming persoonsgegevens; Verslag van een algemeen overleg, gehouden op 15 september 2011, inzake notitie privacybeleid [Personal data processing and protection – Minister for Security & Justice, Minister of Internal Affairs and the relevant Permanent Commissions of the Lower

Chamber of Parliament – unofficial translation], 19 October 2011. https://zoek.officielebekendmakingen.nl/kst-32761-2.html

648. Parliament of the Netherlands, Vaststelling van de begrotingsstaten van het Ministerie van Veiligheid en Justitie (VI) voor het jaar 2012; Verslag van een schriftelijk overleg; Verslag van een schriftelijk overleg inzake naleving van voorschriften rond bevragingen van identificerende gegevens via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) [Budget Ministry for Security and Justice – unofficial translation], 21 December 2011.
https://zoek.officielebekendmakingen.nl/kst-33000-VI-66.html

1.5.4 Ministerie van Justitie/Ministerie van Veiligheid en Justitie (Ministry of Justice / in 2010 name changed to Ministry of Security and Justice)

2001

649. Ministry of Justice, Grootschalig afluisteren van moderne telecommunicatiesystemen; Notitie over de technische en juridische aspecten van grootschalig afluisteren van moderne telecommunicatiesystemen [Large scale tapping of modern telecommunucation systems – unofficial translation], Ministry of Justice, 29 January 2001. http://retro.nrc.nl/W2/Lab/Echelon/doc010120.html

2003

650. Ministry of Justice, Onderzoek bewaren verkeersgegevens door Telecommunicatieaanbieders [Investigation concerning the storage of traffic information by telecommunication providers – unofficial translation], 19 December 2003. https://www.wodc.nl/onderzoeksdatabase/bewaren-verkeersgegevens-fase-1-2-en-3.aspx?cp=44&cs=6802&action=0

2004

651. Ministry of Justice, Wijziging Regeling particuliere beveiligingsorganisaties en rechercheburеaus [Update to regulation on private investigation agencies], May 2004. https://zoek.officielebekendmakingen.nl/stcrt-2004-100-p11-SC65120.html

652. Ministry of Justice, Ministry of the Interior, Naar een veiliger samenleving - Vierde voortgangsrapportage over de uitvoering van het Veiligheidsprogramma door in brief van de Minister van Justitie en van Binnenlandse Zaken en KoninkrijksrelatiesS. [Progress report on the execution of the national security programme – unofficial translation], 5 November 2004.

653. Willem Pompe Instituut voor Strafrechtswetenschappen, *De Wet bijzondere opsporingsbevoegdheden eindevaluatie* [*Evaluation of the 2000 Special Powers of Investigation Ac*t – unofficial translation], Report commissioned by the Ministry of Justice, 15 December 2004. https://zoek.officielebekendmakingen.nl/kst-29940-1-b2.html

2005

654. Willem Pompe Instituut voor Strafrechtswetenschappen, *Evaluatie wet bijzondere politieregisters* [*Evaluation law special police databases* – unofficial translation], Report commissioned by the Ministry of Justice, 17 February 2005. https://zoek.officielebekendmakingen.nl/kst-30001-1-b1.html

655. Ministry of Justice, Ministry of the Interior, Naar een veiliger samenleving; de vijfde voorgangsrapportage over de uitvoering van het Veiligheidsprogramma [Minister of Justice, Minister for Internal Affairs – *Towards a safer society – 5th annual report* – unofficial translation], 31 May 2005. https://zoek.officielebekendmakingen.nl/kst-28684-51.html

2007

656. Gerrit-Jan Zwenne, G-J, Duthler, A-W, Groothuis, M, Kielman, H, , Koelewijn, W en Mommers L, Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse [First evaluation of the Dutch Data Protection Law – unofficial translation], report commissioned by WODC/Ministry of Justice, December 2007. https://zoek.officielebekendmakingen.nl/kst-31051-1-b1.html

2008

657. Hulst, R.C. van der en Neve, R.J.M., *High-tech crime, soorten criminaliteit en hun daders* [*High-tech crime, types and perpetrators* – unofficial translation], report commissioned by the Ministry of Justice/WODC, 2008. http://www.wodc.nl/images/ob264_volledige tekst_tcm44-105995.pdf

2009

658. Commissie Veiligheid en persoonlijke levenssfeer ("de commissie Brouwer-Korf"), [Personal data treatment for increased security – advice to the Ministry of Justice – unofficial translation], Ministry of the Interior, January 2009. https://zoek.officielebekendmakingen.nl/kst-28684-199-b1.html **[part of short analysis]**

659. Ministry of Justice, Besluit politiegegevens bijzondere opsporingsdiensten [Expanding access to police data to special public investigation agencies – unofficial translation], 16 July 2009. https://zoek.officielebekendmakingen.nl/stb-2009-305.html

2011

660. Ministry of Security and Justice[2], De Nationale Cyber Security Strategie (NCSS) [The National Strategy for Cyber Security], February 2011. http://english.nctb.nl/Images/cyber-security-strategy-uk_tcm92-379999.pdf

[2] New name from 2011 onwards.

661. Adviescollege toetsing regeldruk, *Armslag voor de politieprofessional* [Advice to the Ministry of Security and Justice regarding reducing administrative burdens of the police – unofficial translation], 2011. http://www.actal.nl/wp-content/uploads/Rapport_Armslag_voor_de_politieprofessional1.pdf

662. Ministry of Security and Justice. Juridisch kader Cyber Security [Legal framework for cyber security – unofficial translation], December 2011. https://zoek.officielebekendmakingen.nl/blg-147059.html

1.5.5 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Ministry of Internal Affairs and Relations of State)

2003

663. Ministry of the Interior, *Eindrapport onderzoek naar bestuurlijke bevoegdheden in het buitenland ter voorkoming van verstoring van de openbare orde* [*Final report of investigation after governmental authorisation abroad to avoid disturbing of the public order* – unofficial translation], 19 March 2003.

2004

664. Ministry of the Interior, De AIVD in verandering. [Evaluation of national intelligence agency – unofficial translation], 18 November 2004. https://zoek.officielebekendmakingen.nl/kst-29876-1-b1.html

2005

665. Ministry of the Interior, *Veiligheid in ontwikkeling* [*Security in development* – unofficial translation], 28 September 2005. https://zoek.officielebekendmakingen.nl/kst-28684-60-b1.html

666. Ministry of the Interior, Democratische Controle Inlichtingen- en veiligheidsdiensten [Democratic control of intelligence and security agencies – unofficial translation], 21 December 2005. https://zoek.officielebekendmakingen.nl/kst-29876-8-b1.html

2006

667. Ministry of the Interior, Verantwoording Project High Tech Crime (NHTCC), [Accountability of Project High Tech Crime – unofficial translation], 30 May 2006. https://zoek.officielebekendmakingen.nl/kst-26671-24-b1.html

668. Ministry of the Interior, Eerste inventarisatie van contraterrorismebeleid: Duitsland, Frankrijk, Italië, Spanje, het Verenigd Koninkrijk en de Verenigde Staten [Counterterrorism policy in Germany, France, Italy, Spain, the UK – unofficial translation], 18 July 2006. https://zoek.officielebekendmakingen.nl/kst-29754-76-b1.html

2007

669. Koops, B-J (ed.), Leenes, R. (ed.) en Hert, P.de, *Onderzoeksrapport 'Constitutional Rights and New Technologies'* [*Report of investigation 'Constitutional Rights and New Technologies'* – unofficial translation], Report commissioned by the Ministry of the In-

terior , TILT – Tilburg Insti tute for Law, Technolog y, and Society, February 2007. http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2007/03/20/onderzoeksrapport-internationale-vergelijking-van-grondrechten-in-de-digitale-samenleving/crant-report-2007def.pdf

670. Adviescommissie Informatiestromen Veiligheid, *Data voor daadkracht: Gegevensbestanden voor veiligheid: observaties en analyse* [*Data decisiveness. Data safety: observations and analysis* – unofficial translation], report commissioned by the Ministry of the Interior, Ministry of Defense, Ministry of Justice, April 2007. https://zoek.officielebekendmakingen.nl/kst-30800-VII-65-b1.html **[part of short analysis]**

671. Ministry of the Interior, Veiligheid in ontwikkeling [Security in development – unofficial translation], November 2007. http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2007/12/20/veiligheid-in-ontwikkeling-geactualiseerde-versie/veiligheidinontwikkeling.pdf

672. Ministry of the Interior, Instellingsbesluit Adviescommissie Veiligheid en persoonlijke levenssfeer [Decision to set up the committee 'Security and personal life' – unofficial translation], 17 December 2007. https://zoek.officielebekendmakingen.nl/stcrt-2007-244-p9-SC83467.html

1.5.6 Ministerie van Economische Zaken (Ministry of Economic Affairs)

2001

673. Ministry of Economic Affairs, Informatie- en communicatietechnologie; Nota Kwetsbaarheid op internet (KWINT) [Information- and communicationtechnology: note about vulnerability on the Internet – unofficial translation], report to parliament, Ministry of Economic Affairs, 17 July 2001. https://zoek.officielebekendmakingen.nl/kst-26643-30.html

2005

674. Ministry of Economic Affairs, De toekomst van de elektronische communicatie [The future of electronic communications – unofficial translation], 12 July 2005. https://zoek.officielebekendmakingen.nl/kst-26643-65-b1.html

1.5.7 Ministerie van Sociale Zaken en Werkgelegenheid (Ministry for Social Affairs and Employment)

2008

675. Inspectie Werk en Inkomen, Handhaving: Preventie boven repressie [Enforcement: prevention before repression – unofficial translation], Ministry for Social Affairs and Employment, July 2008. http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2008/07/01/iwi-rapport-handhaving-preventie-boven-repressie/129-2008-3-12195.pdf

1.5.8 Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) (Dutch Review Committee on the Intelligence and Security Services)

2011

676. Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), *Jaarverslag CTIVD 2010-2011* [*Annual report Dutch Security & Intelligence agencies* – unofficial translation], 4 May 2011. https://zoek.officielebekendmakingen.nl/blg-111483.html

677. Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), Toezichtsrapport CTIVD inzake de door de AIVD uitgebrachte ambtsberichten in de periode van oktober 2005 tot en met mei 2010 [Supervisor's analysis of AIVD's reporting during the period 2005-2010 – unofficial translation], September 2011. https://zoek.officielebekendmakingen.nl/blg-138452.html

1.5.9 Staatscommissie Grondwet (Constitutional Commission)

2010

678. Staatscommissie Grondwet, *Rapport Staatscommissie Grondwet* [*Informational rights in the digital era* – unofficial translation], November 2010. https://zoek.officielebekendmakingen.nl/blg-86969.pdf

1.5.10 College van Procureurs-Generaal (Board of Attorney Generals)

2004

679. College van procureurs-generaal. Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden [Directives on handling personal data related to crime by public prosecution – unofficial translation], 18 November 2004. https://zoek.officielebekendmakingen.nl/stcrt-2004-223-p9-SC67490.html

2006

680. College van procureurs-generaal, Aanwijzing voorlichting opsporing en vervolging (Citeertitel) [Information, detection and investigation – communication policy for/by police & the public prosecutor with a view to increasing transparency and legitimacy – unofficial translation], 22 December 2006. https://zoek.officielebekendmakingen.nl/stcrt-2006-250-p19-SC78595.html

1.5.11 Nationale Ombudsman (National Ombudsman)

2005

681. Nationale Ombudsman, Jaarverslag Nationale Ombudsman 2004; Verslag Jaarverslag Nationale Ombudsman 2003 [The National Ombudsman - yearly report – unofficial translation], 8 March 2005. https://zoek.officielebekendmakingen.nl/kst-30030-2.html

1.5.12 College Bescherming Persoonsgegevens (Data Protection authority)

2005

682. College Bescherming Persoonsgegevens, *Rapport ACTII, bevindingen betreffende de zelfevaluatie door het College Bescherming Persoonsgegevens* [*Self-evaluation DPA* – N.B. published Dec. 2004 – unofficial translation], 18 August 2005. https://zoek.officielebekendmakingen.nl/kst-29800-VI-163-b1.html

2007

683. College Bescherming Persoonsgegevens, Advies College bescherming persoonsgegevens op wetsontwerp implementatie Europese Richtlijn Dataretentie [Advice Dutch DPA re the implementation of the Data Retention Directive – unofficial translation], 19 September 2007.
https://zoek.officielebekendmakingen.nl/kst-31145-3-b8.html

2008

684. College Bescherming Persoonsgegevens, *Jaarverslag 2007* [*Year overview report 2007* – unofficial translation], Den Haag 2008.

2009

685. College Bescherming Persoonsgegevens, *Jaarverslag 2008* [*Year overview report 2008* – unofficial translation], Den Haag 2009.

2010

686. College Bescherming Persoonsgegevens, *Jaarverslag* 2009 [*Year overview report 2009* – unofficial translation], Den Haag 2010.

1.5.13 ECP.NL – Platform voor de Informatiesamenleving (Platform for the Information Society)

2008

687. ECP.NL, *Ambient intelligence, persoonsgegevens en consumentenbescherming* [*Ambient intelligence, personal data and consumer protection* – unofficial translation], 4 June 2008. https://zoek.officielebekendmakingen.nl/kst-31200-XIII-57-b1.html

1.6 FRANCE SECURITY AND PRIVACY DOCUMENTS

1.6.1 Sénat (Senate)

2008

688. M. Romani, Roger, *Cyberdéfense: Un nouvel enjeu de sécurité nationale* [*Cyber defence: A new national security issue* -- unofficial translation], Rapport d'information, la

Commission des Affaires Etrangères, Sénat, 8 juillet 2008. http://www.senat.fr/notice-rapport/2007/r07-449-notice.html

689. M. Bodin Claude, *Rapport visant à prolonger l'application des articles 3, 6 et 9 de la loi n° 2006-64 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* [*Report to extend the application of Articles 3, 6 and 9 of the Law No. 2006-64 on the fight against terrorism and adopting different measures for security and border control* -- unofficial translation], Enregistré à la Présidence de l'Assemblée nationale, 19 novembre 2008. http://www.assemblee-nationale.fr/13/rapports/r1263.asp

2010

690. Cointat, M. Christian, *Rapport sur la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique* [*Report on the Proposed Legislation to Better Protect the Right to Privacy in the Digital Age* -- unofficial translation], Sénat, 24 février 2010. http://www.senat.fr/rap/l09-330/l09-3300.html

2011

691. Sénat, *Révision du livre blanc sur la défense et la sécurité nationale : quelles évolutions du contexte stratégique depuis 2008?* [*Revision of the White Paper on defence and national security: what are the evolutions of the strategic context since 2008?* -- unofficial translation], Rapport d'information, Commission des Affaires Etrangères, de la Défense et des Forces Armées, 16 décembre 2011. http://www.senat.fr/rap/r11-207/r11-207.html

2012

692. Sutour, M. Simon, *Rapport sur la Résolution Européenne sur la proposition de règlement relatif à la protection des personnes physiques à l'égard du* traitement *des* données à caractère personnel *et à la* libre circulation *de ces données* [*Report on the European resolution on the protection of individuals with regard to the processing of personal data and on the free movement of such data* -- unofficial translation], Sénat, 29 février 2012. http://www.senat.fr/rap/l11-446/l11-4460.html

1.6.2 *Assemblée nationale Française (National Assembly of France)*

2003

693. Cabal, Christian, *Rapport sur les méthodes scientifiques d'identification des personnes à partir de données biométriques* [*Report on scientific methods for personal identification using biometric data* -- unofficial translation], Office Parlementaire d'Évaluation des Choix Scientifiques et Technologies, Assemblée nationale, 16 juin 2003. http://www.assemblee-nationale.fr/12/rap-off/i0938.asp

2004

694. Delattre, M. Francis, *Rapport relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* [*Report on the protection of individ-*

uals with regard to the processing of personal data -- unofficial translation]**,** Commission des Lois Constitutionnelles, de la Législation et de l'Administration Générale de la République sur le Projet de Loi, Modifié par le Sénat, Assemblée Nationale, 13 avril 2004. http://www.assemblee-nationale.fr/12/rapports/r1537.asp

2009

695. Batho, Delphine et M. Jacques Alain Bénisti, *Rapport d'information sur les fichiers de police* [*Information report on police records* -- unofficial translation], Enregistré à la Présidence de l'Assemblée nationale, mars 2009. http://www.assemblee-nationale.fr/13/rap-info/i1548.asp

2010

696. Senat, Proposition de loi, visant à mieux garantir le droit à la vie privée à l'heure du numérique, [Proposed legislation to better protect the right to privacy in the digital age -- unofficial translation], 23 mars 2010. http://www.assemblee-nationale.fr/13/propositions/pion2387.asp **[part of short analysis]**

2011

697. Bloche, Patrick, and Patrice Verchère, *Rapport d'information sur les droits de l'individu dans la révolution numérique* [*Report on individual rights in the digital revolution* -- unofficial translation**],** Assemblée Nationale, 22 juin 2011. http://www.assemblee-nationale.fr/13/rap-info/i3560.asp

2012

698. Assemblée Nationale, Résolution Européenne sur la proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [European resolution on the protection of individuals with regard to the processing of personal data and on the free movement of such data -- unofficial translation], 23 mars 2012. http://www.assemblee-nationale.fr/13/ta/ta0888.asp

1.6.3 Secrétariat général de la défense et de la sécurité nationale (The General Secretariat for Defence and National Security) (Prime Minister's Office)

2005

699. Premier Ministre, Décret n° 2005-1726 relatif aux passeports électroniques [Decree No. 2005-1726 on electronic passports -- unofficial translation], 30 décembre 2005. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000268015&dateTexte=&categorieLien=id

2006

700. Pierre Lasbordes, *La sécurité des systèmes d'information, un enjeu majeur pour la France* [*Security of information systems: a major issue for France* -- unofficial transla-

tion], Secrétariat générale de la défense et de la sécurité nationale, janvier 2006. http://www.ladocumentationfrancaise.fr/rapports-publics/064000048/index.shtml

2007

701. Premier Ministre, Décret n° 2007-1890 portant création d'un traitement automatisé de données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement et modifiant la partie réglementaire du code de l'entrée et du séjour des étrangers et du droit d'asile [Decree n° 2007-1890 creating automated processing of personal data relating to foreigners subject of repatriations, and amending the regulatory part of the code of entry and residence of foreigners and asylum seekers -- unofficial translation], décembre 2007.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000017765626&dateTexte=&categorieLien=id

2008

702. Premier Ministre, Décret n° 2008-632 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE » [Decree No. 2008-632 establishing an automatic processing of personal data referred to as "EDVIGE" -- unofficial translation], 27 juin 2008.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019103207&dateTexte=&oldAction=rechJO

2010

703. Premier Ministre, Décret n° 2010-615 du 7 juin 2010 portant création de traitements automatisés de données à caractère personnel relatifs à l'identification biométrique des personnes écrouées, dénommés « BIOAP » [Decree No. 2010-615 of 7 June 2010 establishing the automatic processing of personal data relating to biometric identification of people incarcerated, referred to as "BIOAP" -- unofficial translation], 9 juin 2010.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022320605&dateTexte=&categorieLien=id

2011

704. Premier Ministre, Décret n° 2011-340 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique [Decree n° 2011-340 establishing processing personal data relating to information management and the prevention of harm to public safety -- unofficial translation], 30 mars 2011.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023781834&fastPos=4&fastReqId=1417980413&categorieLien=id&oldAction=rechTexte

1.6.4 Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration (Minstry of the Interior)

2005

705. M. Breton Thierry, *Chantier sur la lutte contre la cybercriminalité* [*Report on the fight against cybercrime* -- unofficial translation], Ministère de l'intérieur, de la Sécurité Intérieure et des Libertés Locales, avril 2005. http://www.ladocumentationfrancaise.fr/rapports-publics/054000263/index.shtml

2008

706. Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, Arrêté portant création d'un traitement automatisé de données à caractère personnel relatif aux personnes interdites de stade [Decree establishing an automated processing of personal data on persons banned from stadiums -- unofficial translation], août 2008. http://rb.juris-clas-seur.com/actualite/journalofficiel/affichage_jo.html?n1=140&n2=0&type_jo=0&nJ=204&d=4+septembre+2007&pos_max=140&cle_jo=20070904&pos=21&num_doc_jo=JON07000026332M001

707. Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, Le livre blanc sur la défense et la sécurité nationale, [The French white paper on defence and national security – unofficial translation], Paris, 17 juin 2008. http://archives.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html **[part of short analysis]**

2009

708. Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, Règlement Relatif à l'Ordre de Base National des Systèmes d'Information et de Communication de la Sécurité civile [Regulations relative to the national base order of information systems and communication of the civil security -- unofficial translation], Direction de la sécurité civile, Paris, 8 décembre 2009. http://www.interieur.gouv.fr/sections/a_l_interieur/defense_et_securite_civiles/materiels-equipements/telecom/obnsic/downloadFile/attachedFile/OBNSIC.pdf?nocache=1270955282.71

709. Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales, la Garde des sceaux, Ministre de la justice, et le Ministre de la défense, Arrêté du 16 juin 2009 portant création d'un système dénommé « PHAROS » (plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) [Decree of 16 June 2009 establishing a system called "PHAROS" (platform harmonization, analysis, fusions and orientation of alerts) -- unofficial translation], 20 juin 2009. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020763903&dateTexte=&categorieLien=id

710. Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales, Ministre de la défense et le Ministre du budget, des comptes publics et de la fonction publique, Arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules [Decree of 18 May 2009 establishing an automated processing of vehicles data control -- unofficial translation], 27 mai 2009. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020665029

2011

711. Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, Arrêté portant autorisation de traitements automatisés de données à caractère personnel dénommés « nouvelle main courante informatisée » [Decree authorizing the automatic processing of personal data referred to as "new computerised police log book" -- unofficial translation], 22 juin 2011. http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024317261&categorieLien=id

2012

712. Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, Arrêté autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « automatisation du registre des entrées et sorties des recours en matière de contravention » (ARES) [Decree authorizing the creation of an automated processing of personal data referred to as "automatisation of the entries and exits registry in terms of fines" (ARES) -- unofficial translation], mars 2012. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025516896

1.6.5 Le Ministre du budget, des comptes publics et de la fonction publique (Ministry Of Budget, Public Accounts And Civil Administration)

2008

713. Le Ministre du budget, des comptes publics et de la fonction publique, Arrêté relatif à la mise en service par la direction générale des finances publiques d'un traitement automatisé d'identification des personnes physiques et morales dénommé « PERS » [Decree relating to the commissioning by the Public Finances General Directorate of an automated processing identifying individuals and legal entities referred to as "PERS" -- unofficial translation], janvier 2008. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=CCD62DE2836182A797132A98F853FA70.tpdjo06v_3?cidTexte=LEGITEXT000023688434&dateTexte=20120706

1.6.6 Ministère de l'enseignement supérieur et de la recherche (Ministry of Higher Education and Research)

2008

714. Ministère de l'enseignement supérieur et de la recherche, *"Intelligence Ambiante": Défis et Opportunités, Document de réflexion conjoint du comité d'experts «Informa-*

tique Ambiante» du département ST2I du CNRS et du Groupe de Travail «Intelligence Ambiante» du Groupe de Concertation Sectoriel (GCS3), *["Ambient Intelligence": Challenges and opportunities, document of joint reflection of the expert committee "informatic ambiant" of the ST2I CNRS department of the Groupe de Concertation Sectoriel (GCS3)* -- unofficial translation], 14 octobre 2008. http://iihm.imag.fr/publs/2008/RapportIntellAmbiante.V1.2finale.pdf

1.6.7 Secrétariat d'etat à la prospective et au développement de l'economie numérique, (Secretary Of State And Prospective Development Of The Digital Economy)

2010

715. Secrétariat d'etat à la prospective et au développement de l'economie numérique, Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche [Charter of right to be forgotton in the collaborative sites and search engines -- unofficial translation], octobre 2010.

1.6.8 Direction centrale de la sécurité des systèmes d'information (French Network and Information Security Agency)

2006

716. Secrétariat générale de la défense et de la sécurité nationale, *Orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information* [*Guidelines for research and development in terms of security of information systems* -- unofficial translation], Agence nationale de la sécurité, des systèmes d'information, Paris, 30 novembre 2006. http://www.ssi.gouv.fr/fr/ssi/la-ssi-en-france/orientation-de-la-recherche-en-securite-des-systemes-d-information.html **[part of short analysis]**

2008

717. Secrétariat générale de la défense et de la sécurité nationale, *Orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information* [*Guidelines for research and development in terms of security of information systems* -- unofficial translation], Agence nationale de la sécurité, des systèmes d'information, Paris, 10 avril 2008. http://www.ssi.gouv.fr/fr/ssi/la-ssi-en-france/orientation-de-la-recherche-en-securite-des-systemes-d-information.html

2009

718. Secrétariat générale de la défense et de la sécurité nationale, *Référentiel Général de Sécurité* [The General Security Regulatory Framework -- unofficial translation], Agence nationale de la sécurité des systèmes d'information, Paris, 6 mai 2010. http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/ **[part of short analysis]**

1.6.9 L'Autorité de régulations des communications électroniques et des postes (French Electronic Communications and Postal Regulatory Authority)

2010

719. L'Autorité de régulations des communications électroniques et des postes, *Neutralité de l'internet et des réseaux: Propositions et recommandations* [*Internet and network neutrality: Proposals and recommendations* -- unofficial translation], septembre 2010. http://www.arcep.fr/index.php?id=8652#c20177

1.6.10 La Haute autorité pour la diffusion des oeuvres et la protection des droits sur internet (The High Authority for Transmission of Creative Works and Copyright Protection on the Internet)

2010

720. La Haute autorité pour la diffusion des oeuvres et la protection des droits sur internet, *Rapport d'activité 2010* [*2010 Annual report* -- unofficial translation], septembre 2011. http://www.ladocumentationfrancaise.fr/rapports-publics/114000603-rapport-d-activite-2010-de-la-haute-autorite-pour-la-diffusion-des-oeuvres-et-la

1.6.11 Observatoire national de la délinquance et des réponses pénales (National Monitoring Centre of Delinquency and Penal Responses)

2008

721. Observatoire national de la délinquance et des réponses pénales, *Rapport: Mieux contrôler les fichiers de police pour protéger les libertés* [*Report: A better monitoring of police records to protect freedoms* -- unofficial translation], décembre 2008. http://www.ladocumentationfrancaise.fr/rapports-publics/084000748/index.shtml

1.6.12 Institut national des hautes etudes de sécurité et de la justice (National Institute of Advanced Security and Justice Studies)

2006

722. Institut national des hautes études de sécurité, *Fichiers de police et de gendarmerie : comment améliorer leur contrôle et leur gestion?* [*Police and gendarmerie records: how to improve their monitoring and management?* -- unofficial translation], décembre 2006. http://www.ladocumentationfrancaise.fr/rapports-publics/064000885/index.shtml

2008

723. Institut national des hautes études de sécurité, *La vidéo protection Conditions d'efficacité et critères d'évaluation* [*Video Requirements for effective protection and Evaluation Criteria* -- unofficial translation], juillet 2008. http://www.interieur.gouv.fr/sections/a_votre_service/video-protection/documentations/evaluation/conditions-d-efficacite-criteres-d-evaluation/

1.6.13 Commission nationale de l'information et des libertés (CNIL) (National Commission for Information Freedom)

2001

724. Commission nationale de l'information et des libertés (CNIL), *21e Rapport d'Activité 2000 [21st Activity Report 2000* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2001.
http://www.ladocumentationfrancaise.fr/rapports-publics/014000460/index.shtml

2002

725. Commission nationale de l'information et des libertés (CNIL), *22e Rapport d'Activité 2001 [22nd Activity Report 2001* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2002.
http://www.ladocumentationfrancaise.fr/rapports-publics/024000377/index.shtml

726. Commission nationale de l'information et des libertés (CNIL), Délibération portant avis sur le projet d'arrêté du ministre de la justice portant création dans certains établissements pénitentiaires d'un traitement automatisé de données nominatives ayant pour objet la gestion des personnes placées sous surveillance électronique [Deliberation giving an opinion on the draft decree of the Minister of Justice to establish in some prisons an automated processing of personal data for the purpose of managing persons under electronic surveillance -- unofficial translation], juin 2003.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653788&fastReqId=1934524374&fastPos=15

727. Commission nationale de l'information et des libertés (CNIL), Délibération n° 2003-034 du 19 juin 2003 portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance [Deliberation No. 2003-034 of 19 June 2003 adopting a recommendation on the storage and use of credit card number in the field of distance selling -- unofficial translation], août 2003.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000598063&dateTexte=&categorieLien=id

728. Commission nationale de l'information et des libertés (CNIL), *23e Rapport d'Activité 2002 [23rd Activity Report 2002* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2003.
http://www.ladocumentationfrancaise.fr/rapports-publics/034000366/index.shtml

2004

729. Commission nationale de l'information et des libertés (CNIL), Délibération portant avis sur un traitement de la Régie Autonome des Transports Parisiens ayant pour finalité l'exploitation des données de validation des passes NAVIGO [Deliberation giving an opinion on treatment of Paris Transport Authority whose purpose is the use of data validation of NAVIGO passes -- unofficial translation], avril 2004.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653150&fastReqId=1934524374&fastPos=14

730. Commission nationale de l'information et des libertés (CNIL), *La cybersurveillance des salariés [Cyber surveillance of employees* -- unofficial translation], Paris, 2004. http://www.cnil.fr/en-savoir-plus/rapports-dactivite/autres-ouvrages/

731. Commission nationale de l'information et des libertés (CNIL), *24e Rapport d'Activité 2003 [24th Activity Report 2003* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2004.
http://www.ladocumentationfrancaise.fr/rapports-publics/044000252/index.shtml

2005

732. Commission nationale de l'information et des libertés (CNIL), Délibération portant avis sur le projet de décret instituant le passeport électronique et sur les modifications apportées au traitement DELPHINE permettant l'établissement, la délivrance et la gestion des passeports [Deliberation giving an opinion on the draft decree establishing the electronic passport and on changes to the treatment DELPHINE, Issuance and management of passports -- unofficial translation], novembre 2005. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017652180&fastReqId=933812714&fastPos=7

733. Commission nationale de l'information et des libertés (CNIL), *25e Rapport d'Activité 2004 [25th Activity Report 2004* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2005.
http://www.ladocumentationfrancaise.fr/rapports-publics/054000256/index.shtml

2006

734. Commission nationale de l'information et des libertés (CNIL), Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en oeuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public [Deliberation 2006-066 of 16 March 2006 adopting a recommendation on the implementation of devices in order to geolocate motor vehicles used by employees of a private or public organisation -- unofficial translation], 3 mai 2006.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000815113&dateTexte=&categorieLien=id

735. Commission nationale de l'information et des libertés (CNIL), *26e Rapport d'Activité 2005 [26th Activity Report 2005* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2006.
http://www.ladocumentationfrancaise.fr/rapports-publics/064000317/index.shtml

2007

736. Commission nationale de l'information et des libertés (CNIL), Délibération autorisant la mise en oeuvre, par le ministère de l'Économie, des Finances et de l'Industrie, d'un traitement automatisé de données à caractère personnel ayant pour objet l'identification des contribuables, dénommé "PERS" [Deliberation authorising the implementation, by the Ministry of Economy, Finance and Industry, of an automated processing of person-

al data in order to identify taxpayer, referred to as "PERS" -- unofficial translation], 10 juillet 2007.
http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017651939

737. Commission nationale de l'information et des libertés (CNIL), *27e Rapport d'Activité 2006 [27th Activity Report 2006* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2007.
http://www.ladocumentationfrancaise.fr/rapports-publics/074000422/index.shtml

2008

738. Commission nationale de l'information et des libertés (CNIL), *28e Rapport d'Activité 2007 [28th Activity Report 2007* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2008.
http://www.ladocumentationfrancaise.fr/rapports-publics/084000197/index.shtml

2008

739. Commission nationale de l'information et des libertés (CNIL), Délibération n°2008-174 du 16 juin 2008 portant avis sur un projet de décret en Conseil d'Etat portant création au profit de la direction centrale de la sécurité publique d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE » [Deliberation No. 2008-174 of 16 June 2008 giving an opinion on a draft decree of the Council of State in favor of establishing the Central Directorate of Public Security of automated processing of personal data referred to as "EDVIGE"-- unofficial translation], juillet 2008.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000019796251&fastReqId=636228208&fastPos=1

2009

740. Commission nationale de l'information et des libertés (CNIL), Délibération n° 2009-200 du 16 avril 2009 portant avis sur sept articles du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure [Deliberation No. 2009-200 of 16 April 2009 giving an opinion on seven articles of the bill orientation and programming for the performance of Homeland Security -- unofficial translation], avril 2009.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023972513&fastReqId=1934524374&fastPos=9

741. Commission nationale de l'information et des libertés (CNIL), Délibération n°2009-355 du 11 juin 2009 portant avis sur un projet de décret en Conseil d'Etat portant création de l'application relative à la prévention des atteintes à la sécurité publique [Deliberation No. 2009-355 of 11 June 2009 giving an opinion on a draft Order in Council of State establishing the application on the prevention of harm to public safety -- unofficial translation], juin 2009.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000021335762&fastReqId=1934524374&fastPos=7

742. Commission nationale de l'information et des libertés (CNIL), Délibération n° 2009-494 du 17 septembre 2009 portant avis sur le projet de décret modifiant les articles R.

611-10 et R. 611-13 du code de l'entrée et du séjour des étrangers et du droit d'asile dans le but de pouvoir confier à des prestataires agréés le recueil des données biométriques des demandeurs de visa [Deliberation of 17 September 2009 giving an opinion on the draft decree amending articles R. 611-10 and R. 611-13 of the Code of the Entry and Stay of Aliens and Asylum in order to entrust to approved service providers gathering of biometric data from visa applicants -- unofficial translation], september 2009.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000022683235&fastReqId=1934524374&fastPos=4

743. Commission nationale de l'information et des libertés (CNIL), *29e Rapport d'Activité 2008 [29th Activity Report 2008* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2009.
http://www.ladocumentationfrancaise.fr/rapports-publics/094000211/index.shtml

2010

744. Commission nationale de l'information et des libertés (CNIL), Délibération n° 2010-096 du 8 avril 2010 portant recommandation relative à la mise en œuvre, par les compagnies d'assurance et les constructeurs automobiles, de dispositifs de géolocalisation embarqués dans les véhicules [Deliberation No. 2010-096 of April 8, 2010 recommendating on the implementation, by insurance companies and automakers, of geolocation devices installed in vehicles -- unofficial translation], 19 mai 2010.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022227831

745. Commission nationale de l'information et des libertés (CNIL), *Guide de la sécurité des données personnelles [Guidebook of personnal data security* -- unofficial translation], 2010. http://www.cnil.fr/en-savoir-plus/guides/

746. Commission nationale de l'information et des libertés (CNIL), *30e Rapport d'Activité 2010 [30th Activity Report 2009* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2010. http://www.cnil.fr/en-savoir-plus/rapports-dactivite/accessible/non/

2011

747. Commission nationale de l'information et des libertés (CNIL)**,** Délibération n° 2011-066 portant avis sur un projet d'arrêté autorisant la création du traitement automatisé de données à caractère personnel dénommé « automatisation du registre des entrées et sorties des recours en matière de contravention » (ARES) [Deliberation No. 2011-066 giving an opinion on a draft decree authorizing the creation of automated processing of personal data referred to as "automated registry entries and exits in terms of fines" (ARES) -- unofficial translation], 3 mars 2011.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025517386

748. Commission nationale de l'information et des libertés, Délibération n°2011-125 du 5 mai 2011 portant avis sur un projet d'arrêté relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé « nouvelle main courante informatisée » [Deliberation giving an opinion on the draft decree on the implementation of treatment

of personal data referred to as "new handrail computerized" -- unofficial translation], mai 2011.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000024323031&fastReqId=2002721686&fastPos=135

749. Commission nationale de l'information et des libertés (CNIL), Délibération n°2011-180 du 16 juin 2011 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par des organismes financiers relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi qu'à l'application des sanctions financières [Deliberation No. 2011-180 of 16 June 2011 authorizing single treatment of personal data implemented by financial institutions related to the fight against money laundering and terrorist financing and the application of sanctions financial -- unofficial translation], juin 2011.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000024323084&fastReqId=1670802383&fastPos=107

750. Commission nationale de l'information et des libertés (CNIL), Délibération n° 2011-204 du 7 juillet 2011 portant avis sur un projet de décret en Conseil d'Etat relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé « traitement de procédures judiciaires » (TPJ) [deliberation n° 2011-204 of 7 july 2011 giving an opinion on a draft decree in Council of State relating to the implementation of a treatment of personal data referred to as "treatment of judicial proceedings" (TPJ) -- unofficial translation], juillet 2011.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000025807193&fastReqId=343505489&fastPos=92

751. Commission nationale de l'information et des libertés (CNIL), Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004 [Law of 6 January 1978 on information technology, data files and civil liberties amended by the act of 6 August 2004 relative to the protection of individuals with regard to the processing of personal data -- unofficial translation], septembre 2011. http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/

752. Falque-Pierrotin, Isabelle, *Note d'observations concernant la proposition de loi relative à la protection de l'identité* [*Note and comments on the draft law on the protection of identity -- unofficial translation*], CNIL, 25 octobre 2011. http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-cnil-rend-publiques-ses-observations-sur-la-proposition-de-loi-relative-a-lidentite/

753. Commission nationale de l'information et des libertés (CNIL), *Guide des professionnels de la santé* [*Guidebook for health professionals* -- unofficial translation], 2011. http://www.cnil.fr/dossiers/sante/

754. Commission nationale de l'information et des libertés (CNIL), *31e Rapport d'Activité 2010 [31st Activity Report 2010* -- unofficial translation], Direction de l'information légale et administrative, Paris, 2011.
http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_rapport_annuel_%202010.pdf

2012

755. Commission nationale de l'information et des libertés (CNIL), Délibération portant autorisation unique de traitements de données à caractère personnel contenues dans des informations publiques aux fins de communication et de publication par les services d'archives publiques [Resolution authorizing single treatment of personal data contained in public information for purposes of communication and publication by the public archives -- unofficial translation], 12 avril 2012. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025753449

756. Commission nationale de l'information et des libertés (CNIL), *Vidéosurveillance / vidéoprotection: les bonnes pratiques pour des systèmes plus respectueux de la vie privée* [*Video surveillance / CCTV: best practices for systems more respectful of privacy* -- unofficial translation], Communiqué de presse, juin 2012. http://www.cnil.fr/dossiers/scolarite-mineurs/actualites/accessible/non/article/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de/ **[part of short analysis]**

757. Commission nationale de l'information et des libertés (CNIL), *Videoprotection dans les lieux publics : les bonnes pratiques* [*CCTV in public places: good practices* -- unofficial translation], Paris, 21 juin 2012. http://www.cnil.fr/dossiers/scolarite-mineurs/actualites/accessible/non/article/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de/

1.7 ITALY SECURITY AND PRIVACY POLICY DOCUMENTS

1.7.1 Parlamento Italiano (Italian Parliament)

2003

758. Italian Government, Personal Data Protection Code, Legislative Decree no. 196, 30 June 2003. http://www.garanteprivacy.it/garante/document?ID=1894006

2011

759. Italian Government, "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" [Guidelines on the use of personal data by public authorities – unofficial translation], *Gazzetta Ufficiale della Republica Italiana*, No. 64, March 2011, pp. 33 - 47. http://www.interno.it/mininterno/export/sites/default/it/assets/files/20/0100_garante_1.pdf

1.7.2 Presidenza della Republica (Italian Presidency)

1999

760. Decreto del Presidente della Repubblica No. 318: Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a

norma dell'articolo 15, comma 2, della legge n. 675 del 31 dicembre 1996 [Presidential decree No 318: Regulation on minimum security measures for processing personal data following article 15, comma 2, of la n. 675, 31 December 1996 – unofficial translation], 28 luglio 1999.
http://www.garanteprivacy.it/garante/doc.jsp?ID=45703

2007

761. Legislative decree No. 144: Implementing Directive 2004/82/EC on the Obligation of Carriers to Communicate Passenger Data, 2 August 2007, *Official Journal*, No. 206, 5 September 2007. http://www.garanteprivacy.it/garante/doc.jsp?ID=1670149

2008

762. Legislative decree No. 109: Transposition of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communication Services or Public Communications Networks and Amending Directive 2002/58/EC, 30 May 2008.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1670046

2010

763. Presidential Decree No. 178: Regulations on setting up and management of the public register of subscribers opting out of the use of their phone numbers for the purposes of commercial selling and/or promotions, 7 September 2010, *Official Journal*, No. 256, 2 November 2010. http://www.garanteprivacy.it/garante/doc.jsp?ID=1788873

1.7.3 Presidenza del Consiglio dei Ministry (Italian Council of Ministers)

2006

764. Italian Council of Ministers, Decreto del presidente del consiglio dei ministry No. 312: Regolamento concernente il trattamento dei dati sensibili e giudiziari presso la Presidenza del Consiglio dei Ministri [Decree of the Italian Council of Ministers No 312: regulation concerning the use of personal sensible and judicial data at the Presidency of Council of Ministers – unofficial translation], 30 novembre 2006. http://www.privacy.it/reg.pcm%20dati%20sens.html

2007

765. Italian Council of Ministers, *Relazione sulla Political dell'Informazione sulla Sicurezza-2007* [*Report on the Information Policy on Security-2007* – unofficial translation], 2007.
http://www.senato.it/service/PDF/PDFServer?tipo=BGT&id=299179

2008

766. Prime Minister's Office, Indirizzi Operativi per la Gestione delle Emergenze [Directive on the Policy and Management of Emergencies – unofficial translation], 2008. http://www.governo.it/backoffice/allegati/41254-5023.pdf

767. Prime Minister's Office, Indirizzi e Direttiva Generali [General Directive and Directions – unofficial translation], 2008. http://www.governo.it/Presidenza/controllo_strategico/doc/direttive%20di%20indirizzo/Direttiva_Prodi_1.pdf

768. Prime Minister's Office, Indirizzi Operativi per la Gestione delle Emergenze [Directive on the Policy and Management of Emergencies – unofficial translation], 2008. http://www.governo.it/backoffice/allegati/41254-5023.pdf

769. Italian Council of Ministers, *Relazione sulla Political dell'Informazione sulla Sicurezza-2008* [*Report on the Information Policy on Security-2008* – unofficial translation], 2008. http://www.ansa.it/documents/1236688838515_relazionesicurezza2008.pdf

2010

770. Italian Council of Ministers, *Relazione sulla Political dell'Informazione sulla Sicurezza-2010* [*Report on the Information Policy on Security-2010* – unofficial translation], 2010. http://www.sicurezzanazionale.gov.it/web.nsf/relazione2010/relazione_2010.pdf **[part of the short analysis]**

771. Prime Minister's Office, Direttiva del Presidente del Consiglio dei Ministri [Directive on the main Objectives of Italian Government – unofficial translation], 2010. http://www.governo.it/Presidenza/controllo_strategico/doc/direttive%20di%20indirizzo/direttiva_pcm_2010.pdf

2011

772. Italian Council of Ministers, *Relazione sulla Political dell'Informazione sulla Sicurezza-2011* [*Report on the Information Policy on Security-2011* – unofficial translation], 2011. http://www.sicurezzanazionale.gov.it/web.nsf/pagine/relazione/2011/relazione-politica-informazione-sicurezza-2011.pdf

1.7.4 Ministro della Difesa (Italian Defence Ministry)

2000

773. Italian Defence Ministry, *Nota Aggiuntiva allo Stato di Previsione della Difesa per l'anno* 2001 *[Additional Note on the Provision of Defence for 2001* – unofficial translation*],* 2000. http://www.difesa.it/Approfondimenti/Nota-aggiuntiva/Documents/58570_na_2001.pdf

2002

774. Italian Defence Ministry, *Libro Bianco, 2002* [The White Paper, 2002 – unofficial translation], Centro Studi per la Pace, Rome, 2002. http://files.studiperlapace.it/spp_zfiles/docs/20060816165432.pdf **[part of short analysis]**

2005

775. Italian Defence Ministry, *Il Concetto Strategico del Capo di Stato Maggiore della Difesa* [The Chief of the Italian Defence Staff Strategic Concept], Società Editrice Imago Media srl, Rome, 2005. http://merln.ndu.edu/whitepapers/Italy2005.pdf

2006

776. Italian Defence Ministry, *Nota Aggiuntiva allo Stato di Previsione della Difesa per l'anno* 2009 [*Additional Note on the Provision of Defence for 2006* – unofficial translation], 2006.
http://www.difesa.it/Approfondimenti/Nota-aggiuntiva/Documents/86808_NotaAggiuntiva2006.pdf

2009

777. Italian Defence Ministry, *Nota Aggiuntiva allo Stato di Previsione della Difesa per l'anno* 2009 [*Additional Note on the Provision of Defence for 2009* – unofficial translation], 2009. http://www.difesa.it/NR/rdonlyres/5EF11493-59DD-4FB7-8485-F4258D9F5891/0/Nota_Aggiuntiva_2009.pdf

2011

778. Italian Defence Ministry, *Nota Aggiuntiva allo Stato di Previsione della Difesa per l'anno* 2011 [*Additional Note on the Provision of Defence for 2011* – unofficial translation], 2011.
http://www.difesa.it/Approfondimenti/Nota-aggiuntiva/Documents/NA2011edMarzo.pdf

1.7.5 Ministro degli Affari Esteri (Italian Foreign Ministry)

2006

779. Italian Foreign Ministry, *Direttiva Generale per l'Azione Amministrativa e per la Gestione dei Centri di Responsabilità del Ministero degli Affari Esteri per l'anno 2006* [General Directive on Administrative Priorities and Management of Italian Foreign Ministry Centres for 2006 – unofficial translation], 2006. http://www.governo.it/Presidenza/controllo_strategico/doc/direttive_2006/Direttiva_2006Esteri.pdf

2008

780. Italian Foreign Ministry, *Rapporto 2020, le Scelte di Politica Estera* [2020 Report, the choice of Foreign Policy – unofficial translation], 2008. http://www.esteri.it/mae/doc/Rapporto2020_SceltePoliticaEstera_090408.pdf

1.7.6 Ministro degli Affari Interni (Italian Ministry of Internal Affairs)

2008

781. Italian Ministry of Internal Affairs, Direttiva Generale per L'Attivita' Amministrativa per la Gestione Relative all'anno 2008 [General Directive on Administrative Priorities and Objectives for 2009 – unofficial translation], 2008. http://www.interno.it/mininterno/export/sites/default/it/assets/files/15/0950_Direttiva_2008_Ministro.pdf

782. Italian Ministry of Internal Affairs, *Rapporto sulla Criminalita' in Italia* [*Report on Criminality in Italy* – unofficial translation] 2008. http://www.interno.it/mininterno/export/sites/default/it/assets/files/14/0900_rapporto_criminalita.pdf

2009

783. Italian Ministry of Internal Affairs, Direttiva Generale per L'Attivita' Amministrativa per la Gestione Relative all'anno 2009 [General Directive on Administrative Priorities and Objectives for 2010 – unofficial translation], 2009. http://www.interno.it/mininterno/export/sites/default/it/assets/files/16/0736_Direttiva_2009.pdf

2011

784. Italian Ministry of Internal Affairs, Direttiva Generale per L'Attivita' Amministrativa per la Gestione Relative all'anno 2011 [General Directive on Administrative Priorities and Objectives for 2012 – unofficial translation], 2011. http://www.interno.it/mininterno/export/sites/default/it/assets/files/21/0658_Direttiva_generale_2011.pdf

2012

785. Italian Ministry of Internal Affairs, Direttiva Generale per L'Attivita' Amministrativa per la Gestione Relative all'anno 2012 [General Directive on Administrative Priorities and Objectives for 2012 – unofficial translation], 2012. http://www.interno.it/mininterno/export/sites/default/it/assets/files/22/0160_Direttiva_generale_Ministro_2012.pdf 15

1.7.7 Garante per la Protezione dei Dati Personali (Italian Data Protection Authority)

1998

786. Garante per la Protezione dei Dati Personali, Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities, Pursuant to Section 25 of Act no. 675 of 31.12.96, *Official Journal*, No. 179, 3 August 1998. http://www.garanteprivacy.it/garante/doc.jsp?ID=1565746

2001

787. Garante per la Protezione dei Dati Personali, Code of conduct and professional practice Regarding the processing of personal data For historical purposes, *Official Journal*, No. 80, 5 April 2001.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1565819

2002

788. Garante per la Protezione dei Dati Personali, *Annual Report for the Year 2001 – Summary*, 2002. http://www.garanteprivacy.it/garante/doc.jsp?ID=1751047 **[part of short analysis]**

789. Garante per la Protezione dei Dati Personali, Code of conduct and professional practice applying to the processing of personal data for statistical and scientific research purposes within the framework of the national statistical system, *Official Journal*, No. 230, 10 October 2002.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1565879

790. Garante per la Protezione dei Dati Personali, MMS and Data Protection, 17 March 2003. http://www.garanteprivacy.it/garante/doc.jsp?ID=1672134

791. Garante per la Protezione dei Dati Personali, Spamming: How to Lawfully Email Advertising Messages, 29 May 2003. http://www.garanteprivacy.it/garante/doc.jsp?ID=1589969

2004

792. Garante per la Protezione dei Dati Personali, Disposizioni in materia di comunicazione e di propaganda politica [Decision on communication and political propaganda – unofficial translation], 12 Febbraio 2004.
http://www.interno.it/mininterno/export/sites/default/it/sezioni/servizi/legislazione/privacy/legislazione_523.html

793. Garante per la Protezione dei Dati Personali, Balancing of interests: data collection by CRAs without consent, 16 November 2004.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1671380

2005

794. Garante per la Protezione dei Dati Personali, Loyalty Cards and Safeguards for Consumers: Guidelines applying to loyalty programmes, 24 February 2005. http://www.garanteprivacy.it/garante/doc.jsp?ID=1109624

795. Garante per la Protezione dei Dati Personali, Code of conduct and professional practice applying to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments, *Official Journal*, No. 56, 9 March 2005. http://www.garanteprivacy.it/garante/doc.jsp?ID=1079077

796. Garante per la Protezione dei Dati Personali, "Smart (RFID) Tags": Safeguards Applying to Their Use, 9 March 2005. http://www.garanteprivacy.it/garante/doc.jsp?ID=1121107

797. Garante per la Protezione dei Dati Personali, Prior Checking: Use of Fingerprints for Assiduity Control at the Workplace – Provision of July 21, 2005, 21 July 2005. http://www.garanteprivacy.it/garante/doc.jsp?ID=1166892

798. Garante per la Protezione dei Dati Personali, Access to Telephone Data: Safeguards Applying to Incoming Calls, 3 November 2005. http://www.garanteprivacy.it/garante/doc.jsp?ID=1299003

799. Garante per la Protezione dei Dati Personali, Access to Restricted Areas in Certain Companies: For a Proportionate Use of Fingerprints - Decision of November 23, 2005, 23 November 2005. http://www.garanteprivacy.it/garante/doc.jsp?ID=1671299

2006

800. Garante per la Protezione dei Dati Personali, Unsolicited Telephone Services: Enhancing the Safeguards for Citizens, *Official Journal*, No. 54, 6 March 2006. http://www.garanteprivacy.it/garante/doc.jsp?ID=1290823

801. Garante per la Protezione dei Dati Personali, Limitations and Safeguards Applying to Taking of Fingerprints and Image Acquisition by Banks - Provision of 27 October 2005, *Official Journal*, No. 68, 22 March 2006. http://www.garanteprivacy.it/garante/doc.jsp?ID=1276947

802. Garante per la Protezione dei Dati Personali, Need for Enhanced Security Measures in Processing Telephone Traffic Data - Decision of 1 June 2006, 1 June 2006. http://www.garanteprivacy.it/garante/doc.jsp?ID=1303462

803. Garante per la Protezione dei Dati Personali, Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector, 23 November 2006. http://www.garanteprivacy.it/garante/doc.jsp?ID=1427027

2007

804. Garante per la Protezione dei Dati Personali, Annual Report for the Year 2006 – Summary, 2007. http://www.garanteprivacy.it/garante/doc.jsp?ID=1750262

805. Garante per la Protezione dei Dati Personali, General Authorisation for the Processing of Genetic Data, 22 February 2007. http://www.garanteprivacy.it/garante/doc.jsp?ID=1395420

806. Garante per la Protezione dei Dati Personali, Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context, 1 March 2007. http://www.garanteprivacy.it/garante/doc.jsp?ID=1408680

807. Garante per la Protezione dei Dati Personali, Guiding Principles on the Processing of Employees' Personal Data in the Public Sector, 14 June 2007. http://www.garanteprivacy.it/garante/doc.jsp?ID=1693793

808. Garante per la Protezione dei Dati Personali, "Guidelines for the Processing of Customers' Data in the Banking Sector - 25 October 2007", *Official Journal*, No. 273, 23 November 2007. http://www.garanteprivacy.it/garante/doc.jsp?ID=1478096

2008

809. Garante per la Protezione dei Dati Personali, Measures Concerning Itemised Billing - Decision dated 13 March 2008, 13 March 2008. http://www.garanteprivacy.it/garante/doc.jsp?ID=1522362

810. Garante per la Protezione dei Dati Personali, Secure Retention of Telephone and Internet Traffic Data, *Official Journal*, No. 189, 13 August 2008. http://www.garanteprivacy.it/garante/doc.jsp?ID=1542849

811. Garante per la Protezione dei Dati Personali, Electrical and Electronic Waste and Data Protection, 9 December 2008.

812. Garante per la Protezione dei Dati Personali, Code of Practice Applying to the Processing of Personal Data Performed with a View to Defence Investigations, *Official Journal*, No. 275, 24 November 2008. http://www.garanteprivacy.it/garante/doc.jsp?ID=1569165

813. Garante per la Protezione dei Dati Personali, Simplifying the Security Measures Set Forth in the Technical Specifications Contained in Annex B to the Data Protection Code – 27 November 2008, Official Journal, No. 287, 9 December 2008. http://www.garanteprivacy.it/garante/doc.jsp?ID=1619241

814. Garante per la Protezione dei Dati Personali, "Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator", *Official Journal*, No. 300, 24 December 2008. http://www.garanteprivacy.it/garante/doc.jsp?ID=1628774

2009

815. Garante per la Protezione dei Dati Personali, Measures Imposed on the Controllers of Databases Set up from Telephone Subscriber Directories Compiled Prior to 1 August 2005 Following the Derogations Introduced by Section 44 of Decree no. 207/2008 – 12 March 2009, *Official Journal*, No. 66, 20 March 2009. http://www.garanteprivacy.it/garante/doc.jsp?ID=1613568

816. Garante per la Protezione dei Dati Personali, Profiling and Electronic Communications Decision by the Italian DP Authority dated 25 June 2009, *Official Journal*, 11 July 2009. http://www.garanteprivacy.it/garante/doc.jsp?ID=1636001

817. Garante per la Protezione dei Dati Personali, Guidelines on the Electronic Health Record and the Health File, *Official Journal*, No. 178, 3 August 2009. http://www.garanteprivacy.it/garante/doc.jsp?ID=1672821

818. Garante per la Protezione dei Dati Personali, Guidelines on Online Examination Records, *Official Journal*, No. 288, 11 December 2009. http://www.garanteprivacy.it/garante/doc.jsp?ID=1683328

2010

819. Garante per la Protezione dei Dati Personali, Decision on Video Surveillance, 8 April 2010. http://www.garanteprivacy.it/garante/doc.jsp?ID=1734653 **[part of short analysis]**

2011

820. Garante per la Protezione dei Dati Personali, *Annual Report for the Year 2010* – Summary, 2011. http://www.garanteprivacy.it/garante/doc.jsp?ID=1898400

821. Garante per la Protezione dei Dati Personali, Requirements Applying to the Processing of Personal Data for Marketing Purposes as Performed by Relying on Operator-Assisted Telephone Calls, Following the Creation of the Public Opt-Out Register 19 January 2011, *Official Journal*, No. 24, 31 January 2011. http://www.garanteprivacy.it/garante/doc.jsp?ID=1791330

822. Garante per la Protezione dei Dati Personali, Data Sharing and Tracking of Transactions in the Banking Sector, *Official Journal*, No. 127, 3 June 2011. http://www.garanteprivacy.it/garante/doc.jsp?ID=1868766 **[part of short analysis]**

823. Garante per la Protezione dei Dati Personali, "Speech by the President of the Italian Data Protection Authority On the occasion of submitting the DPA's Annual report For the Year 2010", Rome, 23 June 2011.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1869083

824. Garante per la Protezione dei Dati Personali, *Authorisation no. 1/2011 Concerning Processing of Sensitive Data in the Employment Context*, 24 June 2011. http://www.garanteprivacy.it/garante/doc.jsp?ID=1906467

2012

825. Garante per la Protezione dei Dati Personali, *Codice in materia di protezione dei dati personali B. Disciplinare tecnico in materia di misure minime di sicurezza* [Personal Data Protection Code. Attachment B. Technical guide on minimum security measure – unofficial translation], articolo 33 e 36 del codice, 2012. http://www.garanteprivacy.it/garante/doc.jsp?ID=1557184

826. Garante per la Protezione dei Dati Personali, "Guidelines on processing personal data for dissemination and publication on exclusively health-related web sites", *Official Journal*, No. 42, 20 February 2012.
http://www.garanteprivacy.it/garante/doc.jsp?ID=1879894

1.8 GERMANY SECURITY AND PRIVACY POLICY DOCUMENTS

1.8.1 Bundestag (Federal Government/Parliament)

2006

827. Bundestag, Plenarprotokoll Deutscher Bundestag, Stenografischer bericht Sitzung am 1 Juni 2006 [Report of plenary session of the Bundestag (interesting part about Bundesbeauftragten für den Datenschutz) - unofficial translation], Bundestag, 1 June 2006. http://dip21.bundestag.de/dip21/btp/16/16037.pdf

828. Bundestag, Plenarprotokoll Deutscher Bundestag, Stenografischer bericht Sitzung am 5 September 2006 [Report of plenary session of the Bundestag (with interesting discussion about reform of judicial laws as response to terrorist threats) - unofficial translation], Bundestag, 5 September 2006.
http://dip21.bundestag.de/dip21/btp/16/16045.pdf

829. Bundestag, Plenarprotokoll Deutscher Bundestag, Stenografischer bericht Sitzung am 7 September 2006 [Report of plenary session of the Bundestag (same day as the publication of the notification about anti-terrorism measures, therefore a lot is discussed about this topic) - unofficial translation], Bundestag, 7 September 2006. http://dip21.bundestag.de/dip21/btp/16/16047.pdf

830. Bundestag, Plenarprotokoll Deutscher Bundestag, Stenografischer bericht Sitzung am 21 September 2006 [Report of plenary session of the Bundestag (discussion about 'Antiterrorism data' on page 5009) - unofficial translation], Bundestag, 21 September 2006. http://dip21.bundestag.de/dip21/btp/16/16051.pdf

831. Bundestag, Plenarprotokoll Deutscher Bundesta, Stenografischer bericht Sitzung am 26 Oktober 2006 [Report of plenary session of the Bundestag (discussion about RFID and risks for security and privacy on page 5954) - unofficial translation], Bundestag, 20 October 2006. http://dip21.bundestag.de/dip21/btp/16/16060.pdf

832. Bundestag, Plenarprotokoll Deutscher Bundestag, Stenografischer bericht Sitzung am 26 Oktober 2006. [Report of plenary session of the Bundestag (discussion about anti-

terrorism data and the development towards still more security on page 6660) - unofficial translation], Bundestag, 26 October 2006.
http://dip21.bundestag.de/dip21/btp/16/16060.pdf

2007

833. Bundestag, Plenarprotokoll Deutscher Bundestag, Stenografischer bericht Sitzung am 3 March 2007. [Report of plenary session of the Bundestag (discussions about privacy and terrorism on page 9371) - unofficial translation], Bundestag, 3 March 2007. http://dip21.bundestag.de/dip21/btp/16/16092.pdf

2008

834. Bundestag, zu der Unterrichtung durch die Bundesregierung -16/7070 Nr. 1.23-EU-Jahresbericht 2007 zur Menschenrechtslage [Reaction of the Bundestag on EU annual report for human rights - unofficial translation], 11 February 2008. http://dip21.bundestag.de/dip21/btd/16/080/1608031.pdf

835. Bundestag, Standortbestimmung Datenschutz [Response of the federal government to questions of members of Parliament about data protection - unofficial translation], 27 March 2008.
http://dip21.bundestag.de/dip21/btd/16/086/1608668.pdf

836. Bundestag, Plenarprotokoll der 184. Sitzung vom 17.10.2008 [Report of plenary session of Bundestag (concerning data protection and telecommunications) - unofficial translation], 17 October 2008.
http://dip21.bundestag.de/dip21/btp/16/16184.pdf

2009

837. Bundestag, zu der Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit-16/4950-Tätigkeitsbericht 2005 und 2006 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit- 21. Tätigkeitsbericht [Recommendations and activities of federal commissioner for data protection and freedom of information on data protection 2005 and 2006 - unofficial translation], 16 March 2009.
http://dip21.bundestag.de/dip21/btd/16/122/1612271.pdf

838. Bundestag, Entwurf eines Gesetzes zu dem Abkommen vom 1. Oktober 2008 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität [Cooperation between Germany and US in fighting serious crime - unofficial translation], 24 May 2009. http://dip21.bundestag.de/dip21/btd/16/131/1613123.pdf

839. Bundestag, Plenarprotokoll der 224. Sitzung vom 28.05.2009 [Report of plenary session of Bundestag (discussions included about cooperation between Germany and US to fight serious crime) - unofficial translation], 28 May 2009. http://dip21.bundestag.de/dip21/btp/16/16224.pdf

2010

840. Bundestag, Plenarprotokoll der 14. Sitzung vom 19.01.2010 [Report of plenary session of the Bundestag (discussion about body scanners) - unofficial translation], 19 January 2010. http://dip21.bundestag.de/dip21/btp/17/17014.pdf **[part of short analysis]**

841. Bundestag, Probebetrieb von Körperscannern am Flughafen Hamburg [Requests for information by members of Parliament about trial for body scanners at Hamburg airport - unofficial translation], 26 October 2010. http://dip21.bundestag.de/dip21/btd/17/035/1703569.pdf

2011

842. Bundestag, Entwurf eines Gesetzes zur Verbesserung des Schutzes personenbezogener Daten der Beschäftigten in der Privatwirtschaft und bei öffentlichen Stellen [Draft bill for the improvement of the protection of personal data of employees in private enterprises and in public places - unofficial translation], 21 February 2011. http://dip21.bundestag.de/dip21/btd/17/048/1704853.pdf

843. Bundestag, Weitere Datenschutzskandale vermeiden - Gesetzentwurf zum effektiven Schutz von Beschäftigtendaten vorlegen [Draft bill for data protection – to avoid further scandals that have to do with lacking data protection - unofficial translation], 26 September 2011. http://dip21.bundestag.de/dip21/btd/17/071/1707176.pdf

1.8.2 Bundesregierung (Cabinet)

2005

844. Bundesregierung, Der vorgelegte Entwurf der Kommission der Europäischen Gemeinschaften für einen Rahmenbeschluss zur Einführung EU-weit einheitlicher Speicherungspflichten für Telekommunikationsverkehrsdaten und die Haltung der Bundesregierung zu diesem Entwurf [Reaction of federal government to EC bill on storage of telecommunication traffic - unofficial translation], Bundestag, 6 December 2005. http://dip21.bundestag.de/dip21/btd/16/001/1600142.pdf

2007

845. Bundesregierung, Entwurf eines Gesetzes zu dem Abkommen vom 25. Juni 2003 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Auslieferung, zu dem Abkommen vom 25. Juni 2003 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe, zu dem Vertrag vom 14. Oktober 2003 zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen, zu dem Zweiten Zusatzvertrag vom 18. April 2006 zum Auslieferungsvertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika sowie zu dem Zusatzvertrag vom 18. April 2006 zum Vertrag zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen [Draft bill from the German federal government about extradition treaty with the US - unofficial trans-

lation], Bundestag, 22 February 2007. http://dip21.bundestag.de/dip21/btd/16/043/1604377.pdf

846. Bundesregierung, Entwurf eines Gesetzes zu dem Abkommen vom 26. Juli 2007 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records - PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen 2007) [Draft bill concerning the handling of PNR and transfers of information between airline companies and the United States Department of Homeland Security, agreements between EU and USA - unofficial translation], 21 October 2007.
http://dip21.bundestag.de/dip21/btd/16/067/1606750.pdf

847. Bundesregierung, Entwurf eines Gesetzes zu dem Übereinkommen des Europarates vom 23. November 2001 über Computerkriminalität [Draft bill concerning Council of Europe agreement about cybercrime - unofficial translation], Bundestag, 15 November 2007. http://dip21.bundestag.de/dip21/btd/16/072/1607218.pdf

2009

848. Bundesregierung, Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften [Draft bill for data protection audits and changes to data protection prescriptions - unofficial translation], 17 February 2009. http://dip21.bundestag.de/dip21/btd/16/120/1612011.pdf

2010

849. Bundesregierung, Vorratsdatenspeicherung und Sicherheitslücken [Answers of the Bundestag to members of Parliament about the storing of telecommunications and internet data for six months in favor of fighting terrorism and crime and security gaps - unofficial translation], 22 April 2010.
http://dip21.bundestag.de/dip21/btd/17/014/1701482.pdf **[part of short analysis]**

850. Bundesregierung, Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes [Draft bill for regulations for protection of data of employees - unofficial translation], 14 December 2010.
http://dip21.bundestag.de/dip21/btd/17/042/1704230.pdf

2011

851. Bundesregierung, Entwurf eines Gesetzes zur Fortentwicklung des Meldewesens (MeldFortG) [Draft bill about development of reporting business - unofficial translation], 15 November 2011.
http://dip21.bundestag.de/dip21/btd/17/077/1707746.pdf

2012

852. Bundesregierung, *Rahmenprogramm der Bundesregierung "Forschung für die zivile Sicherheit* (2012 bis 2017)" [*Report of framework programme "Research for civil se-*

curity" - unofficial translation], 25 January 2012. http://dip21.bundestag.de/dip21/btd/17/085/1708500.pdf

853. Bundesregierung, Gesichtsscanner in Fußballstadien und Datenabgleich mit der Verbunddatei "Gewalttäter Sport" [Answers of government to questions of members of Parliament about face recognition in football stations - unofficial translation], 15 March 2012. http://dip21.bundestag.de/dip21/btd/17/090/1709003.pdf

1.8.3 Parlementarische Kontrollgremium (Parliamentary Control Commission)

2006

854. Parlamentarische Kontrollgremium (PKGr), *Bericht gemäß § 14 Abs. 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5 und 8 dieses Gesetzes (Berichtszeitraum 1. Juli 2004 bis 31. Dezember 2005), Bericht gemäß § 14 Abs. 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmelde-geheimnisses (Artikel 10-Gesetz – G10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5 und 8 dieses Gesetzes [Notification about anti-terrorism measures and consequences]*, 7 September 2006. http://dip21.bundestag.de/dip21/btd/16/025/1602551.pdf **[part of short analysis]**

2007

855. Parlamentarische Kontrollgremium (PKGr), Bericht gemäß § 8a Abs. 6 Satz 2, § 9 Abs. 4 Satz 7 des Bundesverfassungsschutzgesetzes über die Durchführung sowie Art, Umfang und Anordnungsgründe der Maßnahmen nach § 8a Abs. 2 des Bundesverfassungsschutzgesetzes, § 2a des Gesetzes über den Bundesnachrichtendienst sowie §§ 4a und 5 des Gesetzes über den Militärischen Abschirmdienst im Berichtszeitraum 1. Januar bis 31. Dezember 2006 Bericht zu den Maßnahmen nach dem Terrorismusbekämpfungsgesetz [Anti-terrorism measures in different policy areas. Supplement to earlier bill - unofficial translation], 4 July 2007. http://dip21.bundestag.de/dip21/btd/16/059/1605982.pdf

856. Parlamentarische Kontrollgremium (PKGr), Bericht gemäß § 14 Abs. 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5 und 8 dieses Gesetzes (Berichtszeitraum 1. Januar 2006 bis 31. Dezember 2006) [Draft bill concerning limitations to letter and telephone secrecies - unofficial translation], 24 October 2007. http://dip21.bundestag.de/dip21/btd/16/068/1606880.pdf

857. Parlamentarische Kontrollgremium (PKGr), Bericht über die Kontrolltätigkeit gemäß § 6 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Berichtszeitraum: Oktober 2005 bis Dezember 2007) [Main points of control commission concerning among others: fighting international terrorism - unofficial translation], 11 December 2007. http://dip21.bundestag.de/dip21/btd/16/075/1607540.pdf

2009

858. Parlamentarische Kontrollgremium (PKGr), Bericht gemäß § 8a Absatz 6 Satz 2 und § 9 Absatz 4 Satz 7 des Bundesverfassungsschutzgesetzes (BVerfSchG) über die Durchführung sowie Art, Umfang und Anordnungsgründe der Maßnahmen nach § 8a Absatz 2 und § 9 Absatz 4 BVerfSchG, den §§ 2a und 3 des Gesetzes über den Bundesnachrichtendienst (BNDG) sowie den §§ 4a und 5 des Gesetzes über den Militärischen Abschirmdienst (MADG) im Berichtszeitraum 1. Januar bis 31. Dezember 2007 (Bericht zu den Maßnahmen nach dem Terrorismusbekämpfungsergänzungsgesetz) [Report about anti-terrorism measures - unofficial translation], 4 January 2009. http://dip21.bundestag.de/dip21/btd/16/115/1611560.pdf

1.8.4 Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Agency for Electricity, Gas, Telecommunications, Mail and railways)

2007

859. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Tätigkeitsberichte 2006/2007 der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen gemäß § 121 Abs. 1 Telekommunikationsgesetz und § 47 Abs. 1 des Postgesetzes und Sondergutachten der Monopolkommission gemäß § 121 Abs. 2 des Telekommunikationsgesetzes und gemäß § 44 Abs. 1 des Postgesetzes i.V.m. § 81 Abs. 3 des Telekommunikationsgesetzes a.F. [Report of Federal agency for electricity, gas, telecommunications, mail and railways about their activities. Data protection in telecommunications is being discussed - unofficial translation], 16 December 2007. http://dip21.bundestag.de/dip21/btd/16/077/1607700.pdf

1.8.5 Delegation der Bundesrepublik Deutschland in der Parlementarischen Versammlung des Europarates (Delegation of Germany in the Parliamentary gathering of the European Council)

2008

860. Delegation der Bundesrepublik Deutschland in der Parlementarischen Versammlung des Europarates, Tagung der Parlamentarischen Versammlung des Europarates vom 21. bis 25. Januar 2008 in Straßburg [Description of the parliamentary meeting of the Council of Europe in Strassbourgh. Main points: black list of Security Council, video surveillance, data protection - unofficial translation], 23 October 2008. http://dip21.bundestag.de/dip21/btd/16/107/1610709.pdf

1.8.6 Auschusses für Umwelt, Naturschutz und Reaktorsicherheit (Commission for Environment, Protection of nature and Safety of reactors)

2009

861. Auschusses für Umwelt, Naturschutz und Reaktorsicherheit, zu dem Gesetzentwurf der Bundesregierung-16/11609-Entwurf eines Zehnten Gesetzes zur Änderung des

Atomgesetzes [Recommendations of representatives on the topic of adjustments to atom bill - unofficial translation], 27 January 2009. http://dip21.bundestag.de/dip21/btd/16/117/1611782.pdf

1.8.7 Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (Commission for Education, Research and Technology assessment)

2010

862. Ausschusses für Bildung, *Forschung und Technikfolgenabschätzung, Technikfolgenabschätzung (TA) Zukunftsreport - Ubiquitäres Computing* [*Report about ubiquitous computing by the commission for education, research and technology assessment* - unofficial translation], 5 January 2010. http://dip21.bundestag.de/dip21/btd/17/004/1700405.pdf

1.8.8 Wissenschaftliche Dienste Bundestag (Parliamentary Scientific Institute)

2010

863. Wissenschaftliche Dienste Bundestag, *Körperscanner* [*Report of scientific institute/service of the Bundestag about body scanners* - unofficial translation], 25 March 2010. http://www.bundestag.de/dokumente/analysen/2010/koerperscanner.pdf

1.8.9 Enquete-Kommission „Internet und digitale Gesellschaft“ Datenschutz (Working party “Internet and Digital Society”)

2012

864. Enquete-Kommission "Internet und digitale Gesellschaft" Datenschutz, Persönlichkeitsrechte, *Fünfter Zwischenbericht der Enquete-Kommission "Internet und digitale Gesellschaft" Datenschutz, Persönlichkeitsrechte* [*Report of committee of inquiry 'Internet and digital society' about data protection and personality rights* - unofficial translation], Bundestag, 14 March 2012. http://dip21.bundestag.de/dip21/btd/17/089/1708999.pdf **[part of short analysis]**

1.8.10 Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Federal Agency for Data Protection and Freedom of Information)

2004

865. Schaar, Peter, Überwachung des Bürgers durch Staat und Wirtschaft - Welche Perspektiven hat der Datenschutz? Rede des Bundesbeauftragten für den Datenschutz Peter Schaar auf der 28. DAFTA am 18. November 2004 in Köln [Speech of the Federal Commissioner of the German data protection authority about the perspectives of data protection - unofficial translation], Bundesbeauftragten für den Datenschutz, 18 November 2004. http://www.bfdi.bund.de/SharedDocs/Publikationen/PM39-04UeberwachungDesBuergersDurchStaatUndWirtschaft-WelchePerspektivenHatDerDatenschutz.html

2005

866. Bundesbeauftragte für den Datenschutz Übergabe des 20, Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz (2003/2004) an den Präsidenten des Deutschen Bundestages [Description of activities of the Federal Commissioner for data protection - unofficial translation], 19 April 2005. http://www.bfdi.bund.de/SharedDocs/Publikationen/PM14-05Uebergabedes20.Taetigkeitsberichts-LinkZumTaetigkeitsbericht.html

867. Schaar, Peter, Rede des Bundesbeauftragten für den Datenschutz, Peter Schaar, bei der "Europäischen Konferenz der Beauftragten für Informationsfreiheit" am 25.11.2005 in Berlin: Das Recht auf Informationszugang als Angelegenheit auf europäischer Ebene [Speech of the Federal Commissioner of the German Data Protection Authority about the right of access to information on European territory - unofficial translation], Bundesbeauftragten für den Datenschutz, 25 November 2005. http://www.bfdi.bund.de/SharedDocs/Publikationen/RedeBeauftragteFuerInformationsfreiheit.html

2006

868. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, Der vermessene Mensch, Tagungsband zum Symposium Biometrie und Datenschutz* [Report of symposium from the Data Protection Authority about biometry and data protection - unofficial translation], 27 June 2006.
http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/TagungsbandVermessenerMensch.html

2007

869. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Unterrichtung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Tätigkeitsbericht 2005 und 2006 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 21. Tätigkeitsbericht – 23 April 2007 [Description of activities of the Federal Commissioner for Data Protection and Freedom of Information - unofficial translation], 23 April 2007.
http://dip21.bundestag.de/dip21/btd/16/049/1604950.pdf

2008

870. Schaar, Peter, The invasion of privacy by the state, Rede des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, über die Rolle des Datenschutzes in einer modernen Informationsgesellschaft [Speech by Federal Data Protection Commissioner about the role of data protection in the modern information society - unofficial translation], 9 May 2008.
http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2008/09052008-dt-britischeJuristengesellschaft-Cheltenham.html

871. Schaar, Peter, Die Grenzen des Rechtsstaates – furcht vor dem Gläsernen Bürger, Vortrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Rahmen der Veranstaltungsreihe des Bildungswerks Dresden der Konrad-Adenauer-

Stiftung [Speech by Federal Data Protection Commissioner about the limits of the constitutional state - unofficial translation], 11 June 2008. http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2008/GrenzenDesRechtsstaates-FurchtVorGlaesernemBuerger.html

872. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum geplanten BKA-Gesetz zur Abwehr von Gefahren des internationalen Terrorismus [Position of the Data Protection Authority concerning the planned bill for keeping off dangers of International Terrorism - unofficial translation], 15 September 2008. http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/StellungnahmeBKAGesetz.html

2009

873. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Aktuelle Entwicklungen im europäischen und internationalem Datenschutz unter besonderer Berücksichtigung des transatlantischen Dialogs, rede von Peter Schaar [Speech by the Federal Commissioner of the German Data Protection Authority about recent developments in European and International data protection - unofficial translation], 30 January 2009.
http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/30012009_RedeSchaarEuDSTagWien.html

874. Schaar, Peter, Wie nachrichtendienstliche Erkenntnisse und polizeiliche Daten zukünftig verschmelzen werden – neue Herausforderungen für die Aufsichtsbehörden? Vortrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen der Conference of DPA's of Federal and Plurinational States [How intelligence data and police data will merge in the future - new challenges for supervision? Speech by Federal Data Protection Commissioner at Conference of DPA's of federal and plurinational states - unofficial translation], Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 19 March 2009.
http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2009/PlurinationaleKonferenzMaerz.html **[part of short analysis]**

875. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - 22. Tätigkeitsbericht [Recommendations and activities of Federal Commissioner for Data Protection and Freedom of Information on data protection 2007 and 2008 - unofficial translation], 20 April 2009. http://dip21.bundestag.de/dip21/btd/16/126/1612600.pdf

2010

876. Schaar, Peter, Diskretionszone für Körperscanner gewährleisten! [Message from Federal Data Protection Commissioner about Guaranteeing discrete zone for body scanners - unofficial translation], 24 September 2010.
http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2010/41_DiskretionszoneKoerperscanner.html

2011

877. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Bundesdatenschutzgesetz, Text und Erläuterung [Federal Data Protection Law, full explanation - unofficial translation], 15 January 2011. http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1_Januar_2011.html

878. Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2009 und 2010 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - 23. Tätigkeitsbericht [Recommendations and activities of Federal commissioner for data protection and freedom of information on data protection 2009 and 2010 - unofficial translation], 14 April 2011. http://dip21.bundestag.de/dip21/btd/17/052/1705200.pdf

1.8.11 Datenschutz Hamburg

2011

879. Datenschutz Hamburg (HmbBfDI), *MEINE DATEN KRIEGT IHR NICHT*! [You don't get my data! - unofficial translation], 2011. http://www.mahsh.de/cms/upload/downloads/Medienkompetenz/MeineDatenKriegtIhrNicht_web_2011.pdf

1.9 ROMANIA SECURITY AND PRIVACY POLICY DOCUMENTS

1.9.1 Parlmentul Romaniei (Parliament)

2012

880. Parlmentul Romaniei, Camera Deputatilor, *Raportul comun suplimentar asupra propunerii legislative privind retinerea datelor generale sau prelucrate de furnizorii de retele publice e comunicatii electronice si de furnizorii de servicii de comunicatii electronice destinate publicului, 22.05. 2012* [*Report and debate about the transposition of the data retention directive*], Bucharest, 22 May 2012. http://www.cdep.ro/comisii/juridica/pdf/2012/rp010.pdf **[part of the short analysis]**

1.9.2 Government/Presidency

2006

881. Romanian government, Stenograma audierii publice din ziua de 27 iunie 2006 «Libertate individuală versus securitate naţională. Echilibrul între transparenţă şi secretizare» [Public debate organized by the Romanian Government on the subject: "Individual freedom vs. national security – balancing transparency and secrecy"], 27 June 2006. http://www.cdep.ro/pls/dic/site.page?den=ap200606_8 **[part of short analysis]**

2007

882. Presedintele Romaniei, Strategia de securitate nationala a Romaniei, [Romanian national security strategy], Bucurest, 2007. http://www.presidency.ro/static/ordine/SSNR/SSNR.pdf **[part of short analysis]**

1.9.3 Romanian Information Agency

2008

883. Maior, George Cristian, Societate, Democratie, Intelligence, proceedings of a round table, [Romanian Secret Service – round table society, democracy, intelligence], Bucharest, 8 October 2008. http://www.sri.ro/upload/intellspecial.pdf **[part of short analysis]**

1.9.4 Romanian National Ombudsman

2002

884. The Romanian National Ombudsman, *Annual Report* [*Setting up the function of the Data Protection Authority*], 2002. http://www.avp.ro/rapoarte-anuale/raport-2002-avocatul-poporului.pdf

2004

885. The Romanian National Ombudsman, *Annual Report* [*Proposal for a dedicated Data Protection Authority; registration of public authorities as data processors*], 2004. http://www.avp.ro/rapoarte-anuale/raport-2004-avocatul-poporului.pdf

2005

886. The Romanian National Ombudsman, *Annual Report* [*End of activity as DPA*], 2005. http://www.avp.ro/rapoarte-anuale/raport-2005-avocatul-poporului.pdf

1.10 USA SECURITY AND PRIVACY POLICY DOCUMENTS

1.10.1 Congressional Research Service

2000

887. Stevens, Gina Marie, *Electronic Communications Privacy Act of 2000 (H.R. 5018): Summary in Brief*, Congressional Research Service, 3 October 2000.

888. Stevens, Gina Marie and Melinda DeAtley, *Summary of the Proposed Rule for the Privacy of Individually Identifiable Health Information*, Congressional Research Service, 22 March 22 2000.

2001

889. Doyle, Charles, *Terrorism Legislation: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Congressional Research Service, 26 October 2001. **[part of short analysis]**

2002

890. Relyea, Harold C., *The Privacy Act: Emerging Issues and Related Legislation*, Congressional Research Service, 27 February 2002.

891. Smith, Marcia S., Jeffrey W. Seifert, Glenn J. McLoughlin and John Dimitri Moteff, *Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*, Congressional Research Service, 4 March 2002.

892. Doyle, Charles, *The USA PATRIOT Act: A Legal Analysis*, Congressional Research Service, 15 April 2002.

893. Doyle, Charles, *The USA PATRIOT Act: A Sketch*, Congressional Research Service, 18 April 2002.

894. Stevens, Gina Marie, *Privacy Protection for Online Information*, Congressional Research Service, 21 May 2002.

2003

895. Moteff, John D., and Gina Marie Stevens, *Critical Infrastructure Information Disclosure and Homeland Security*, Congressional Research Service, 29 January 2003.

896. Belasco, Amy, *Total Information Awareness Programs: Funding, Composition, and Oversight Issues*, Congressional Research Service, 21 March 2003. **[part of short analysis]**

897. Stevens, Gina Marie*, A Brief Summary of the HIPAA Medical Privacy Rule*, Congressional Research Service, 30 April 2003.

2004

898. Krouse, William J., *The Multi-State Anti-Terrorism Information Exchange (MATRIX) Pilot Project*, Congressional Research Service, 18 August 2004.

899. Stevens, Gina Marie, and Harold C. Relyea, *Privacy: Key Recommendations of the 9/11 Commission*, Congressional Research Service, 19 August 2004.

2005

900. Weiss, Martin A., *The EU-U.S. "Safe Harbor" Agreement on Personal Data Privacy*, Congressional Research Service, 25 January 2005.

901. Smith, Marcia S., *Wireless Privacy and Spam: Issues for Congress*, Congressional Research Service, 26 January 2005.

902. Murphy, M. Maureen, *Privacy Protection for Customer Financial Information*, Congressional Research Service, 18 April 2005.

903. Smith, Marcia S., *Internet Privacy: Overview and Pending Legislation*, Congressional Research Service, 16 May 2005.

904. Reese, Shawn, *State and Local Homeland Security: Unresolved Issues for the 109th Congress*, Congressional Research Service, 9 June 2005.

905. Doyle, Charles, *USA PATRIOT Act Sunset: A Sketch*, Congressional Research Service, 29 June 2005.

906. Figliola, Patricia Moloney, *Digital Surveillance: The Communications Assistance for Law Enforcement Act*, Congressional Research Service, 3 August 2005.

2006

907. James, Nathan, *DNA Testing for Law Enforcement: Legislative Issues for Congress*, Congressional Research Service, 19 January 2007.

908. Seghetti, Lisa M., and Stephen R. Viña, *U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*, Congressional Research Service, 26 January 2006.

909. Stevens, Gina Marie, *Data Security: Federal Legislative Approaches*, Congressional Research Service, 9 February 2006.

910. Stevens, Gina Marie, and Tara Alexandra Rainson, *Data Security: Protecting the Privacy of Phone Records*, Congressional Research Service, 17 May 2006.

911. Feikert, Clare, *Anti-Terrorism Authority Under the Laws of the United Kingdom and the United States*, Congressional Research Service, 7 September 2006.

912. Stevens, Gina Marie, and Todd B. Tatelman, *Protection of Security-Related Information*, Congressional Research Service, 27 September 2006.

913. Yeh, Brian T., and Charles Doyle, *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis*, Congressional Research Service, 21 December 2006.

2007

914. Doyle, Charles, *National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments*, Congressional Research Service, 20 March 2007.

915. Relyea, Harold C., *Privacy Protection: Mandating New Arrangements to Implement and Assess Federal Privacy Policy and Practice*, Congressional Research Service, 23 August 2007.

916. Bazan, Elizabeth B., *P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act*, Congressional Research Service, 23 August 2007.

2008

917. Seifert, Jeffrey W., *Data Mining and Homeland Security: An Overview*, Congressional Research Service, 27 August 2008.

918. Stevens, Gina and Charles Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, Congressional Research Service, 2 September 2008.

2009

919. Stevens, Gina Marie, and Charles Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, Congressional Research Service, 3 December 2009.

2010

920. Ruane, Kathleen Ann, *Privacy Law and Online Advertising*, Congressional Research Service, 20 January 2010.

921. Stevens, Gina, *Federal Information Security and Data Breach Notification Laws*, Congressional Research Service, 28 January 2010.

922. Rollins, John and Liana Sun Wyler, *International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress*, Congressional Research Service, 18 March 2010.

923. Henning, Anna C., Elizabeth B. Bazan Charles Doyle and Edward C. Liu, *Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization*, Congressional Research Service, 2 March 2010.

2011

924. Doyle, Charles, *Privacy: An Overview of the Electronic Communications Privacy Act*, Congressional Research Service, 30 March 2011.

925. Stevens, Gina, *Privacy Protections for Personal Information Online*, Congressional Research Service, 6 April 2011.

926. Thompson, Richard M., *Governmental Tracking of Cell Phones and Vehicles: The Confluence of Privacy, Technology, and Law*, Congressional Research Service, 1 December 2011.

2012

927. Murrill, Brandon J., Edward C. Liu and Richard M. Thompson, *Smart Meter Data: Privacy and Cybersecurity*, Congressional Research Service, 3 February 2012.

1.10.2 Office of the President of the United States

2001

928. Office of the President of the United States, Organization and Operation of the Homeland Security Council, Homeland Security Presidential Directive 1, 29 October 2001. http://www.fas.org/irp/offdocs/nspd/hspd-1.htm

929. Office of the President of the United States, Combating Terrorism Through Immigration Policies Homeland Security Presidential Directive 2, 29 October 2001. http://www.fas.org/irp/offdocs/nspd/hspd-2.htm

2002

930. Office of the President of the United States, Homeland Security Advisory System, Homeland Security Presidential Directive 3, 11 March 2002. http://www.fas.org/irp/offdocs/nspd/hspd-3.htm

931. Office of the President of the United States, National Strategy to Combat Weapons of Mass Destruction (unclassified version), Homeland Security Presidential Directive 4, 11 December 2002. http://www.fas.org/irp/offdocs/nspd/nspd-17.html

2003

932. Office of the President of the United States, Management of Domestic Incidents, Homeland Security Presidential Directive 5, February 28, 2003. http://www.fas.org/irp/offdocs/nspd/hspd-5.html

933. Office of the President of the United States, Integration and Use of Screening Information to Protect Against Terrorism, Homeland Security Presidential Directive 6, 16 September 2003. http://www.fas.org/irp/offdocs/nspd/hspd-6.html

2004

934. Office of the President of the United States, Biodefense for the 21st Century, Homeland Security Presidential Directive 10, 28 April 2004. http://www.fas.org/irp/offdocs/nspd/hspd-10.html

935. Office of the President of the United States, Comprehensive Terrorist-Related Screening Procedures Homeland Security Presidential Directive 11, 27 August 2004. http://www.fas.org/irp/offdocs/nspd/hspd-11.html

2007

936. Office of the President of the United States, The National Strategy for Aviation Security, Comprehensive Terrorist-Related Screening Procedures, National Security Presidential Directive 47, 26 March 2007.

2009

937. Office of the President of the United States, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 2009. http://www.whitehouse.gov/issues/homeland-security

2010

938. Office of the President of the United States, Surface Transportation Security Assessment, March 2010. http://www.whitehouse.gov/issues/homeland-security

939. Office of the President of the United States, National Security Strategy, May 2010. http://www.whitehouse.gov/issues/homeland-security

2011

940. Office of the President of the United States, National Preparedness, Presidential Policy Directive 8, 30 March 2011.

941. Office of the President of the United States, National Strategy for Counterterrorism, June 2011. http://www.whitehouse.gov/issues/homeland-security

2012

942. Department of Justice and Office of Director of National Intelligence, Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of Director of National Intelligence, Feb 2012.

1.10.3 Department of Homeland Security

2004

943. 9/11 Commission, *The 9/11 Commission Report*, 22 July 2004. http://govinfo.library.unt.edu/911/report/index.htm **[part of short analysis]**

2005

944. Privacy Office, *A Report Concerning Passenger Name Record Information Derived from flights between the U.S. and the European Union*, U.S. Department of Homeland Security, 19 September 2005.
http://www.dhs.gov/files/publications/editorial_0514.shtm#4

2006

945. Privacy Office, *Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required Under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458*, U.S. Department of Homeland Security, Washington DC, 27 April 2006. http://www.dhs.gov/files/publications/editorial_0514.shtm#4

946. Office of the Secretary of the Department of Homeland Security, Regulations Implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act), *Federal Register*, Vol. 71, No. 110, 8 June 2006, pp. 33147-33168.

947. Privacy Office, *Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations*, U.S. Department of Homeland Security, Washington DC, December 2006. http://www.dhs.gov/files/publications/editorial_0514.shtm#4

2007

948. Department of Homeland Security, *CCTV: Developing Privacy Best Practices: Report on the DHS Privacy Office Public Workshop 18 December 2007*, December 2007.

2008

949. Privacy Office, *A Report Concerning Passenger Name Record Information Derived from flights between the U.S. and the European Union*, U.S. Department of Homeland Security, 18 December 2008. http://www.dhs.gov/files/publications/editorial_0514.shtm#4

2010

950. Department of Homeland Security, Testimony of DHS Secretary Janet Napolitano before the Senate Committee on Homeland Security and Governmental Affairs for a hearing entitled "Securing America's Future: The Cybersecurity Act of 2012", 16 February 2012. http://www.dhs.gov/ynews/testimony/20120216-3a-s1-cyber-hsgac.shtm

951. Department of Homeland Security, *Computer Network Security & Privacy Protection*, 19 February 2010. http://www.dhs.gov/files/publications/editorial_0514.shtm#4

952. Department of Homeland Security, DHS Response to the European Commission's Report on the Joint Review of the U.S. - EU Passenger Name Record Agreement, 31 March 2010. http://www.dhs.gov/files/publications/editorial_0514.shtm#4

953. Department of Homeland Security, *Bottom-Up Review Report*, July 2010. http://www.us-cert.gov/related-resources/

2012

954. US Customs and Border Protection, *Border Control Strategic Plan 2012-2016*, May 2012.

1.10.4 Federal Trade Commission

2000

955. US Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, FTC, Washington, DC, May 2000.

2003

956. US Federal Trade Commission, *Staff Workshop Report: Technologies for Protecting Personal Information*, FTC, Washington, DC, 2003.

2005

957. US Federal Trade Commission, The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud: A Legislative Recommendation to Congress, FTC, Washington, DC, June 2005.

958. US Federal Trade Commission, *RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission*, FTC, Washington, DC March 2005.

959. US Federal Trade Commission, *Spyware Workshop: Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff*, FTC, Washington, DC March 2005.

960. US Federal Trade Commission, *Subject Line Labeling As a Weapon Against Spam: A CAN-SPAM Act Report to Congress*, June 2005.

2007

961. US Federal Trade Commission, *Spam Summit: The Next Generation of Threats and Solutions: A Staff Report by the Federal Trade Commission's Division of Marketing Practices*, FTC, Washington, DC, November 2007.

962. US Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Federal Trade Commission Report to Congress*, FTC, Washington, DC, February 2007.

2008

963. US Federal Trade Commission, *Security In Numbers: Social Security Numbers and Identity Theft: A Federal Trade Commission Report Providing Recommendations On Social Security Number Use In the Private Sector*, FTC, Washington, DC, December 2008.

2012

964. US Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FTC, Washington, DC, March 2012.

1.10.5 Federal Communications Commission

2003

965. Federal Communications Commission, *Homeland Security: Industry leaders adopt recommendations to ensure the security of media facilities during emergencies*, FCC Press Release, 9 December 2003.

2004

966. Federal Communications Commission, *Media Security and Reliability Council, Communications Infrastructure Security, Access, and Restoration Working Group Final Report*, February 25, 2004.

967. Powell, Michael K., Written statement on Implementing the 9-11 Commission's Recommendation to Expeditiously Provide Spectrum to Public Safety Organizations Before the Committee on Commerce, Science and Transportation United States Senate, 8 September 8 2004.

968. Federal Communications Commission, *Advisory Committee on Diversity for Communications in the Digital Age Adopts Recommendations*, FCC Press Release, 13 December 2004.

2006

969. Kevin J. Martin, Written statement on "Phone Records For Sale: Why Aren't Phone Records Safe From Pretexting?" Before the Committee on Energy and Commerce U.S. House of Representatives, 1 February 2006.

970. Monteith, Kris Anne, Written statement on "Protecting Consumers' Phone Records" before the Subcommittee on Consumer Affairs, Product Safety, and Insurance Committee on Commerce, Science and Transportation United States Senate, 8 February 2006.

2010

971. Federal Communications Commission, FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap, DA 10-1354, 9 August 2010.

2012

972. Federal Communications Commission, *Report and order in the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 15 February 2012.

973. Genachowski, Julius, *Prepared Remarks on Cybersecurity*, Bipartisan Policy Center, Washington DC, 22 February 2012.

974. Federal Communications Commission, FCC Advisory Committee Adopts Recommendations to Minimise Three Major Cyber Threats, Including an Anti-bot Code of Conduct, IP Rout Hijacking Industry Framework and Secure DNS Best Practices, FCC Press Release, 22 March 2012.

975. Federal Communications Commission, *Location-based Services: An overview of opportunities and other considerations*, Wireless Telecommunications Bureau, May 2012.

976. Federal Communications Commission, Comments Sought on Privacy and Security of Information Stored on Mobile Communications Devices, DA 12-818, 25 May 2012.

1.10.6 Department of Commerce, National Telecommunications and Information Agency

2010

977. US Department of Commerce, National Telecommunications and Information Agency (NTIA), Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Internet Policy Task Force Green Paper), Washington DC, 16 December 2010.

2011

978. US Department of Commerce, National Telecommunications and Information Agency (NTIA), Internet Policy Task Force, *Keynote Address by Cameron F. Kerry, General Counsel, U.S. Department of Commerce*, Washington DC, 6 December 2011.

979. US Department of Commerce, National Telecommunications and Information Agency (NTIA), Internet Policy Task Force, Testimony of Assistant Secretary Strickling on Internet Privacy: The Views of the FTC, the FCC, and NTIA, Washington DC, 14 July 2011.

980. US Department of Commerce, National Telecommunications and Information Agency (NTIA), Internet Policy Task Force, Cybersecurity, Innovation and the Internet Economy Green Paper, Washington DC, 8 June 2011.

981. US Department of Commerce, National Telecommunications and Information Agency (NTIA), Internet Policy Task Force, Protecting Consumers & Promoting Innovation Online: A Call for Baseline Privacy Legislation, Washington DC, 16 March 2011.

982. US Department of Commerce, National Telecommunications and Information Agency (NTIA), Internet Policy Task Force, Testimony of Assistant Secretary Strickling Regarding the State of Online Consumer Privacy, Washington DC, 16 March 2011.

2012

983. US Department of Commerce, National Telecommunications and Information Agency (NTIA), Internet Policy Task Force,Testimony of Assistant Secretary Strickling on "Privacy and Innovation: Does the President's Proposal Tip the Scale?", Washington DC, 29 March 2012.

2 SHORT ANALYSIS OF POLICY DOCUMENTS

2.1 INTERNATIONAL ORGANISATIONS

31. 31st International Conference of Data Protection and Privacy Commissioners, Joint Proposal on International Standards for the Protection of Privacy with Regard to the Processing of Personal Data, Madrid, 5 November 2009. http://www.privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf 36 Pages.

What domain (health, transport, policing, etc.) does it address?

- Personal data – protection, processing, privacy, transparency
  - In the public and private sectors
- Security - technical measures

Surveillance is not mentioned in this document.

Target audience of the document

European Union Member States, Corporations who deal with personal data processing, the public at large

Stated purpose of the document

The stated purpose of this document is:

1. To define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data; and
2. The facilitation of the international flows of personal data needed in a globalised world. (p. 7)

It is stated to be necessary because of the borderless nature of the Internet.

Context of the document

The document follows on from the 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg, where it was unanimously decided there was an urgent need for protecting privacy in a borderless world. They therefore aimed to reach a Joint Proposal for setting International Standards on Privacy and Personal Data Protection.

The context is to bring to light the borderless flow of personal data that occurs digitally, due to increasing internet penetration. The authors note it to be essential that there is an international effort to maintain personal privacy both in the public and private sectors.

Other documents referred to:

- Universal Declaration of Human Rights
- International Covenant on Civil and Political Rights

Key points in the document

The authors state that there should be fair processing of personal data as well as limit the use of the data to what the original purpose for which the data was collected. Additionally, they assert that there should be a limit imposed on the amount of time data can be retained.

Moreover, the authors state that consent should be given by subjects, so there should be

transparency with regards to how personal data is processed and used. Transparency can be increased through the use of clear and plain language (especially when minors are involved).

The authors state that data processors should ensure that personal data is accurate, either through collecting directly from the source, or informing the person where the data was gathered from. Furthermore, the authors note that individuals should have access to these data and should be able to request deletion. They also stress that individuals should be notified if there has been a security breach concerning their personal data.

According to the authors, only through fulfilling the above requirements can personal data be seen as legitimate for processing. Also, they state that there should be additional conditions for the processing of sensitive personal data. [3]

Finally, the authors note that exercising the rights outlined in the document should not entail undue cost or delay to the data subject.[4] The authors end with recommendations for measures which individual states could undertake for the protection of individual personal privacy. These recommendations include the introduction of codes of conduct, delegated supervisory authorities, privacy impact assessments and cooperation and coordination between these authorities.

Assessment of the importance or significance of the document

(Evaluation on the basis of Google search hits, English language results)
This document was referred to (and many similar ideas were put forth) in the European Parliamentary Assembly resolution 1847 (2011).

A Google search indicates that this document has made a large impact, returning over 12,700 results when searching for the title of the document. This does not include the number of hits when searching for "Madrid resolution", because it is difficult to separate the irrelevant ones. Some of the search results were responses to the Joint Proposal, including responses from the US Federal Trade Commission, the US Department of Homeland Security and other governmental websites. This document has been referred to as a benchmark for international privacy standards.

Google Scholar searches provide over 2000 results and indicate that the document has been mentioned in books and journals, in topics ranging from 'Tech Law' and IT Privacy to Privacy Impact Assessment and Privacy by Design.

Overall, this document can be considered as having a significant impact in the public and private sectors.

[3] Sensitive data refers to information containing "[...] racial or ethnic origin, political opinions, or religious or philosophical beliefs as well as those data relating to health or sex life." (p. 16)
[4] The data subject is the individual from which the data originates

2.2 EUROPEAN POLICY DOCUMENTS

40. Committee of Ministers, Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, CM(2005)56 final, 13 May 2005. https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2005)56&Sector=secCM&Language=lanEnglish&Ver=final&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 Online, approx. 10 pages.

What domain (health, transport, policing, etc.) does it address?
Human rights, information society

Target audience of the document
The document is a declaration from the Council of Europe's committee of ministers, representing the Member States submitted to the Tunis phase of the World Summit on the Information Society.

Stated purpose of the document
The document is a declaration that in line with existing declarations from the council, the impacts of ICT, desirability of the information society, the role of ICT in the democratic process, and the potential advances in the exercise of human rights, members states need to review and where necessary adjust human rights instruments, adopt policies compliant with ECHR and case law, especially when adopting measures that may curtail the exercise of human rights in the information society.

Context of the document
The World Summit on the Information Society (WSIS) was two United Nations-sponsored conferences about information, communication and the information society. The first was in 2003 in Geneva and the second in 2005 in Tunis. The chief stated aim was to bridge the global digital divide between rich and countries by increasing Internet access in the developing world. This document was the declaration from the Council of Europe to that second phase.

The document makes reference to a large number of other documents:

- Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005)
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
- European Convention on Transfrontier Television (ETS No. 132)
  Protocol Amending the European Convention on Transfrontier Television (ETS No. 171)
- Convention on Information and Legal Co-operation concerning "Information Society Services" (ETS No. 180)
- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181)
- European Convention for the protection of the Audiovisual Heritage (ETS No. 183)
- Protocol to European Convention for the protection of the Audiovisual Heritage, on the protection of Television Productions (ETS No. 184)
- Convention on Cybercrime (ETS No. 185)
- Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS

No. 189)
- Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations
- Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies
- Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunications, with particular reference to telephone service
- Resolution ResAP (2001) 3 "Towards full citizenship for persons with disabilities through inclusive new technologies"
- Recommendation Rec(2001)7 of the Committee of Ministers to member states on measures to protect copyright and neighbouring rights and combat piracy, especially in the digital environment
- Recommendation Rec(2002)2 of the Committee of Ministers to member states on access to official documents
- Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting
- Recommendation Rec(2004)15 of the Committee of Ministers to member states on electronic governance ("e-governance")
- Declaration of the Committee of Ministers on a European policy for New Information Technologies, adopted on 7 May 1999
- Declaration of the Committee of Ministers on Cultural Diversity, adopted on 7 December 2000
- Declaration of the Committee of Ministers on freedom of communication on the Internet, adopted on 28 May 2003
- Political Message from the Committee of Ministers to the World Summit on the Information Society (Geneva, 10-12 December 2003) of 19 June 2003

Key points in the document

The document engages with the rights to freedom of expression, information and communication, the right to respect for private life and correspondence, The right to education and the importance of encouraging access to the new information technologies and their use by all without discrimination, The prohibition of slavery and forced labour, and the prohibition of trafficking in human beings, The right to a fair trial and to no punishment without law, The protection of property, The right to free elections, and Freedom of assembly. Across each of these areas the broad conclusion is that ICT can provide substantial benefits in these areas, but also potential challenges. So whilst ICT can facilitate communication across nations, they can also be used to reduce freedom of expression through state censorship. Member states are encouraged to promote interoperable communications standards, frameworks for self- and co-regulation of private sector actors, enhance methods for reducing ICT assisted slavery, promote codes of conduct for media and information provides in relation to judicial processes, provide the legal frameworks necessary for the defence of private intellectual property and the prevention of cybercrime, examine the use of ICT in promoting democracy and guarantee freedom of ICT-assisted assembly, and that monitoring and surveillance of digital assembly does not take place.

The document also engages with a multi-stakeholder approach to developing the information society that brings together council of Europe member states, civil society, the private sector, and the council of Europe. The latter is primarily involved in the promotion of the convention on cybercrime, and the convention on the protection of individuals in relation to the automat-

ic processing of personal data.
Assessment of the importance or significance of the document The declaration is not foundational for further laws, but provides an indication of ambition and intention. It has been presented at an international forum.

49. Parliamentary Assembly, Resolution 1843: The protection of privacy and personal data on the Internet and online media, 2011. http://assembly.coe.int/ASP/Doc/ATListingDetails_E.asp?ATID=11377 4 pages.

What domain (health, transport, policing, etc.) does it address?

- Trans-border data flows – public and private sector
- Security - unlawful use of private data, punishment,
- Privacy of personal data – how to maintain this right

Surveillance is not mentioned.

Target audience of the document

European Parliament, Secretary General of the Council of Europe. Also:

- The Parliaments of Armenia, the Russian Federation, San Marino and Turkey.
- Observer delegations from Canada, Israel and Mexico.
- States co-operating with the Council of Europe, in particular the Council of Europe's other observer states Japan, the United States and the Holy See
- European Commission for Democracy through Law
- The United Nations, particularly the:
    - United Nations Internet Governance Forum
    - International Telecommunication Union
    - United Nations Educational, Scientific and Cultural Organization

Stated purpose of the document

The document states that such a resolution is necessary because "digitalisation of information has caused unprecedented possibilities for the identification of individuals through their data" (p. 1). Its purpose is to encourage a global compliance with the obligations outlined in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

It follows on (and is a response to) the report from the Committee on Culture, Science and Education, on The protection of privacy and personal data on the Internet and online media (2011, 29 July).

Context of the document

The purpose of the document is to take a global view on personal privacy and assert the position of the European Parliament, since digital data flows essentially have no boundaries.

Other documents referred to:

- European Convention on Human Rights
- Protection of Children against Sexual Exploitation and Sexual Abuse
- European Parliamentary Assembly Communications:
    - Recommendation 509 (1968) - human rights and modern scientific and technological developments
    - Resolution No. 3 - data protection and privacy in the 3rd millennium
    - Resolution 428 (1970) - declaration on mass communication media and human rights
    - Madrid 2009 and Jerusalem 2010 resolutions
- Convention for the Protection of Individuals (Convention No. 108)
- Charter of Fundamental Rights of the European Union

- International Covenant on Civil and Political Rights
- Convention on Cybercrime
- Convention on Human Rights and Biomedicine
    - Protocol concerning Genetic Testing for Health Purposes
- Council of Europe Convention on Access to Official Documents
- Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism
- Convention on Mutual Administrative Assistance in Tax Matters

Key points in the document

The document outlines a common approach for nations around the world for how to deal with the emergences of new technologies and how they may infringe on the right to privacy, as well as the protection of personal data.

The key point made by the authors is that any international initiative for ensuring protection of private data should be based on Convention No. 108 (and its additional protocol). They view this as the best method for ensuring the right to privacy and data protection. A note is also made that EU member states should only agree to transfer personal data to other states or organisations that are a Party to Convention No. 108.

The main point of the authors is to emphasise the right of everyone to the protection of personal data, especially health data. The authors therefore seek to have effective remedy against those who breach ones right to protection and privacy of personal data, such as the act being punishable by law. Also, public and private entities should be able to be held accountable in case of infringement.

Some recommendations made by the authors include:

- Cookies or other unauthorised automated devices are noted to be a violation of privacy
- Higher protection should be given to data and other information that form the core area of private life, from images to biometric and genetic data.
- Public and private entities should collect the minimum amount of personal data needed
- Everyone must be able to control the use of others of their personal data, thus consent must be given (in advance) and there must be the ability to withdraw consent

Assessment of the importance or significance of the document

This document provided the footing for a recommendation from the Parliamentary Assembly to the Committee of Ministers. The recommendation calls for an international plan of action for the promotion of common legal standards to guarantee the protection of privacy and personal data when it comes to the use of ICTs.

(Evaluation on the basis of Google search hits, English language results)

However a Google search only returns 5 results, all of which are mirrors to the resolution. Therefore, outside of the European Parliament, this document did not have an impact.

69. European Parliament, Resolution on the Commission communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European policy approach (COM(2001) 298 – C5-0657/2001 – 2001/2280(COS)), 22 October 2002. 8 pages

What domain (health, transport, policing, etc.) does it address?
Information and network security

Target audience of the document
The Commission and the Council would be the primary audience, as this document is a response from the European Parliament to a communication from the Commission.

Stated purpose of the document
The document is a response to communication from the European Commission on network and information security

Context of the document
The context of the document is the increasing social and economic importance of electronic communications networks, requiring an adequate legal and policy framework at the EU level to guarantee the protection of network and information security in order to allow the smooth operation of the internal market. Network security requires all actors to be aware of their security role. Computer Emergency Response Teams (CERTs) operate in different ways across Europe therefore creating unnecessary complication and an absence of cooperation.

The document is primarily a response to:
Commission Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European policy approach (COM(2001) 298 - C5-0657/2001)

It also mentions:
European Parliament, Recommendation of 6 September 2001 on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, OJ C 72 E, 21.3.2002

Council of Europe Convention on Cybercrime, signed in Budapest on 23 November 2001, proposal of 19 April 2002 for a Council Framework Decision on attacks against information systems OJ C 203 E, 27.8.2002

Commission communication entitled ‘e-Europe 2005: An information society for all’ (COM(2002) 263), OJ C 72 E, 21.3.2002

Key points in the document
The current level of information and network security is seen as inadequate, users are often unable to protect themselves against threats (both malicious and unintentional), network attacks may be targeted against critical infrastructure, solely voluntary responses only by those affected would be inadequate. Secure access to public administrative services of EU actors is a desirable goal. There are an increasing number of international cyber security initiatives but the document agrees with the need for a specifically European approach, including the need

to formulate common definitions and standards. It is important to include relevant sectors in the formulation of network security policy.

The document calls upon the commission to supply information on current problems in developing policy in this area, and states that a European strategy should be drawn up. This should encompass standards, develop encryption and certification standards, ensure that action is taken to combat crime, raise awareness among citizens and steps up scientific research in areas of current weakness. The document supports the setting up on a network security task force, with clear objectives and potential early warning system. The document state that the primary basis for EU legislation in this area is Title XV of the treaty, relating to trans-European networks, harmonisation and the internal market (Article 95).

Assessment of the importance or significance of the document

The document dates from 2002 and it appears that network and information security strategy at the European level, including research programmes have developed in this direction. As of February 2013, the EU now has a Cyber Security Strategy as called for in this document:

European Commission, Joint Communication to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace(JOIN(2013) 1 final), 7 February 2013. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

79. European Parliament, Recommendation to the Council and to the European Council on the future of the area of freedom, security and justice as well as on the measures required to enhance the legitimacy and effectiveness thereof (2004/2175(INI)), 14 October 2004.
http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2004/10-14/P6_TA-PROV%282004%2910-14_EN.pdf 7 Pages.

What domain (health, transport, policing, etc.) does it address?
Privacy
- Data protection

Security
- from terrorist attack, immigration policy

Surveillance is not mentioned.

Target audience of the document
European Parliament, The European Council, the Commission, the governments and parliaments of the Member States.

Stated purpose of the document
The document exists to form recommendations from the European Parliament to the Council and European Council in the future of the *area of freedom, security and justice* (AFSJ).

It states that changes are necessary due to the lack of legitimacy and effectiveness of the AFSJ. This document follows on from Article 2 of the EU Treaty, as well as other communications to the European Parliament regarding the AFSJ.

Context of the document
The document is a response to the increasing threat of international terrorism that has come to light since 9/11, especially when the EU was struck in the Madrid attacks of 11 March, 2004. The authors claim that "terrorism is the main problem affecting the harmony and security of the people of Europe" (p.8).

The document precedes the signing of the draft of a Constitutional treaty announced to take place less than two weeks following the release of this document. It also relates to the future of the AFSJ, which was to be discussed the following month.

Other Documents Referred to
- Rule 114(3) and Rule 94 of its Rules of Procedure
- Report of the Committee on Civil Liberties, Justice and Home Affairs (A6-0010/2004)
- Proposal for a recommendation to the Council and to the European Council (B6-0006/2004)
- EU Treaty
- Treaty of Nice
- Draft Constitutional Treaty (29 October 2004)
- International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (1990)
- Geneva Convention

- Hague Conference on Private International Law
- Article 2 of Framework Decision 2002/584/JHA

Key points in the document

The document is written with a literal sense of alarm over the lack of action of the Union, with regards to data protection, or combating the threat of terrorism and its challenges posed to citizens' freedoms. The sense of urgency stems i.e. from the notice received by the authors that "On 5 November 2004, the European Council intends to lay down the priorities for the area of freedom, security and justice (AFSJ) for the next few years" (p. 7)

The authors also state that the document has come about due to the addition of 10 new member states to the European Union, therefore there is a focus on the issue of immigration policy, specifically the fight against illegal immigration.

To enhance the legitimacy of the AFSJ, the authors recommend that all Union institutions have strict compliance with regards to freedom, democracy and the rule of law. The document also recommends a common level of fundamental rights protection for all EU citizens. They also recommend increased transparency to legislative debates, as well as consultation of European Parliament on any international agreement on judicial cooperation in criminal and police matters.

The authors also make recommendations to promote fundamental rights and freedoms through policies, as well as a systematic evaluation of the current fundamental rights policies. For this, they also recommend the adoption of joint data protection standards, as well as the formation of a joint data protection authority.

A further recommendation made is to train judges, lawyers and police officers in European law, and also to increase information flow between the judicial, administration and research areas. For this data flow to occur, the authors suggest a computerised network that allows "permanent mutual accessibility to national administrations responsible for security checks (e.g. reformatting of SIS II), for judicial cooperation (e.g. mutual accessibility of national police records) or for the movement of persons, including third-country nationals" (p. 11).

As far as security is concerned, the authors recommend research into security requirements, especially to "prevent catastrophes caused either by natural disasters or by terrorist attacks" (p. 11).

Assessment of the importance or significance of the document
(Evaluation on the basis of Google search hits, English language results)

A Google search of "2004/2175(INI)" returns 20 results (with less than half of them in English). Some are transcripts of the document, others refer to the document within a context of Politics and Society. A Google Scholar search with the same input returns 5 results, 3 of which are English journal articles referencing the document. The articles are about the European security agenda.

A Google search of "Recommendation to the Council and to the European Council on the future of the area of freedom, security and justice" returns 7 results, most which link to sites dealing with European Law.

A Google search without quotation marks around the search terms returned over 1.1 million results. However, not all of these were referring to this specific document. Many of the links were about the European Councils programme 'Strengthening Freedom, Security and Justice'. However, the programme makes no mention of this recommendation.

93. European Parliament, Legislative resolution on the proposal for a Council decision establishing the Specific Programme "Prevention of and Fight against Crime' for the period 2007-2013, General Programme 'Security and Safeguarding Liberties" (COM(2005)0124 – C6-0242/2005 – 2005/0035(CNS)), 14 December 2006. 7 pages

What domain (health, transport, policing, etc.) does it address?
Crime prevention, organised crime.

Target audience of the document
The Council of the European Union

Stated purpose of the document
The document is the European Parliament's response to the Commission proposal (COM(2005)0124) for a Council decision Establishing the specific Programme "Prevention of and Fight against Crime" for the period 2007-2013, as part of the General Programme "Security and Safeguarding Liberties". The document approves the proposal with a number of amendments, and calls on the Commission to alter its proposal accordingly, and keep the Parliament informed of any further changes to the proposal.

Context of the document
The document was produced by the European Parliament under the consultation procedure, in response to a proposal originating with the Commission, to be decided upon by the Council.

The document is a response to European Commission, Establishing a framework programme on "Security and Safeguarding Liberties" for the period 2007-2013, Communication from the Commission to the Council and the European Parliament, COM(2005) 124 final, Brussels, 6.4.2005. It makes extensive reference to that text, quoting it as it amends it.

Key points in the document
The document amends the Commission's proposal in the following ways:

- Identifies Union's objective of providing citizens with a high level of safety within an area of freedom, security and justice, as a priority objective.
- Replaces a particular focus upon trans-border crime with a focus upon organised crime.
- Adds efforts to make best use of existing agencies, through capability building, and that the programme should actively make provision for the review of its modalities.
- Changes language that suggests that organised and trans-border crime can be **best** fought at a Union level, with language that suggests it **requires** action at the Union level.
- Removes some limitations on the expenditure of the programme associated with the generic definition of envisaged actions.
- Altered language of crime prevention to include preventing criminals from enjoying the proceeds of crime.
- Added regional and local law enforcement bodies to the national and Union bodies whose co-operation, co-ordination and mutual understanding should be promoted – through enhancing interoperability, increasing number of Joint Investigation Teams, counter-terrorism training, and awareness exercises.
- Added requirement of strict compliance with current and future provisions in data

protection and retention to promotion of best practices in crime prevention and development of crime fighting tools. Also added development of independent benchmarking tool.
- Added setting up of compensation fund for protection and compensation of crime victims and witnesses.
- Added promotion, within suitable projects, of citizen involvement and active participation of civil society in improving overall security.
- Added establishment under Europol and Eurojust co-operation agreements of legal assistance unit to determine legal basis for extending police/security service operations in compliance with law.
- Added restrictions on public-private partnership involvement in the programme, including strict control from point of view of respect for fundamental rights, including personal data protection.
- Added detail to financial support, access to funding, and proposal procedures of the programme.
- Added social impact to geographic impact of activities.
- Simplified detail with reference to Articles 3 & 7 of Council Decision 1999/468/EC.
- Added requirement that commission ensure that actions provided for under this decision are transparent, and subject to ex ante evaluation and ex post evaluation.
- Added consultation with beneficiaries of programme to its evaluation.
- Added reporting requirements.
- Added equal treatment clause for organisations funded/not already funded by EU under this programme.
- Added acknowledgement, dissemination and publication requirement for recipients of funding under this programme, in particular relating to crime statistics.

Assessment of the importance or significance of the document

The document is taken into regard by:

Council of the European Union, Council Decision of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks' (2007/124/EC, Euratom), OJ L 58, 24 February 2007, pp. 1-6.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007D0124:EN:NOT

The Council Decision, now being law, is arguably more important for future policy activity than this resolution from the Parliament; however, this document does potentially demonstrate some divergence between the Parliament and the Commission.

99. European Parliament, Resolution of 21 June 2007 on an area of freedom, security and justice: Strategy on the external dimension, Action Plan implementing the Hague programme (2006/2111(INI)), 21 June 2007. 10 pages.

What domain (health, transport, policing, etc.) does it address?
External dimension of the area of freedom, security and justice (EU)

Target audience of the document
European Council and European Commission.

Stated purpose of the document
The development of the internal area of freedom, security and justice (AFSC) was giving raised a host of concerns about the relationship between external and internal elements in terms of the rule of law, democratic values, respect for human rights and sound institutions; the balance between security and justice; the coherence and efficiency of internal EU institutional procedures; and the use of various policy instruments in this area. The European Parliament (EP) therefore made a large number of recommendations for the consideration of the Council and Commission, under several broad headings: improving democratic accountability in the external dimension of the AFSJ; the main objectives of the Strategy for the External Dimension of Justice and Home Affairs: Global Freedom, Security and Justice, adopted on 1 December 2005 ('the Strategy'); strengthening security and human rights; providing Union citizens with a high level of security against terrorism and organised crime; strengthening police and judicial cooperation and borders management; and strengthening international solidarity as regards migration, readmission and asylum policies.

Context of the document
The context is implied in the above description, especially the EP's perception of hindrances to the implementation of the Strategy's objectives.

Other documents mentioned: Treaty on European Union (TEU); Treaty establishing the European Community (TEC); Presidency Conclusions and objectives defined by successive European Councils since 1999 in the field of the external dimension of the AFSJ, including the Council of 14 and15 December 2006; proposal from the Commission on a Council framework decision on certain procedural rights in criminal proceedings throughout the European Union (COM(2004)0328); proposal from the Commission on a Council framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005)0475); Communication from the Commission on a Strategy on the External Dimension of the area of freedom, security and justice (COM(2005)0491); the Commission's progress report on the implementation of that strategy (SEC(2006)1498); the Council's Strategy for the External Dimension of Justice and Home Affairs: Global Freedom, Security and Justice, adopted on 1 December 2005; the Council's report on the implementation of that Strategy for the year 2006, endorsed at the 2768th JHA Council of 4 and 5 December 2006; JHA external relations Multi-Presidency Work Programme (5003/1/7) adopted on 23 January 2007; the Council's Action-Oriented Paper on improving cooperation on organised crime, corruption, illegal immigration and counter-terrorism between the EU and the Western Balkans (9360/06); the Action-Oriented Paper on increasing EU support for combating drug production in and trafficking from Afghanistan, including transit routes (9305/06) (both adopted by the JHA Council on 1 and 2 June 2006); the Action-Oriented Paper on Implementing with Russia the Common Space of freedom, se-

curity and justice (15534/06), adopted on 11 November 2006; European Parliament's previous annual debates on AFSJ and resolutions focused on the external dimension thereof (terrorism, CIA, data protection, migration, trafficking, fighting drugs, money laundering); European Parliament's recommendation of 14 October 2004 to the Council and to the European Council on the future of the area of freedom, security and justice as well as the measures required to enhance the legitimacy and effectiveness thereof (OJ C 166 E, 7.7.2005); the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinion of the Committee on Foreign Affairs (A6-0223/2007).

Key points in the document

Under the headings given above, the document makes more than 56 specific points, including recommendations, endorsements, urgings, reminders, expressions of concern, etc. The items on data protection and related topics may be of particular interest: see para. 24, which refers to the need for a single data protection policy embracing the first and former third pillars.

Assessment of the importance or significance of the document

This was probably an important document, setting forward the EP's policies and priorities in this field at a time when the Hague Programme was being implemented, especially regarding its external dimension. Other documents in our series that deal with the Hague Programme are from the House of Lords; European Commission, and European Council.

144. European Parliament, Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)), 6 July 2011. 8 Pages.

What domain (health, transport, policing, etc.) does it address?

- Personal data in general (collection, processing, storage, security and forwarding)
- Transparency of data collection, processing, storage, security and forwarding

Surveillance is only mentioned in relation to a fundamental right to be protected from it.

Target audience of the document

The European Council and the European Commission

Stated purpose of the document

This document is a resolution to 'A comprehensive approach on personal data protection in the European Union'.

It states it is necessary as the EU is in need of; *"[…]a comprehensive, coherent, modern, high-level framework able to protect effectively individuals' fundamental rights, in particular privacy, with regard to any processing of personal data of individuals within and beyond the EU in all circumstances.*" (p. 2)

It follows on from the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions titled 'A comprehensive approach on personal data protection in the European Union'.

Context of the document

The document was written due to challenges facing data protection, especially with increasing global data transfer and increased online activity. It also refers to the 'war on terror', which has generated increased security concerns.

The document also notes that there should be exemption from data protection rules when used for journalistic, artistic or literary purposes. The authors note that these exceptions should be developed in order to protect freedom of the press. These precautions could have stemmed from the News of the World phone hacking event (2009, July).

Documents referred to:

- Treaty on the Functioning of the European Union (Article 16)
- Charter of Fundamental Rights of the European Union (Articles 7, 8)
- European Convention for the Protection of Human Rights and Fundamental Freedoms (Articles 8, 13)
- Data Protection Directive 95/46/EC of the European Parliament (1995, 24 October) and additional protocol thereto of 8 November 2001 regarding supervisory authorities and transborder data flows
- Council Framework Decision 2008/977/JHA (2008, 27 November)
- Regulation (EC) No 45/2001 of the European Parliament (2000, 18 December)
- Directive 2002/58/EC of the European Parliament (2002, 12 July)
- Council of Europe Convention 108 (1981, 28 January)
- Committee of Ministers Recommendation No. R (87) 15 and Recommendation CM/Rec. (2010)13

- United Nations General Assembly (1990). Guidelines for the regulation of computerised personal data files
- European Commission communication (2010). A comprehensive approach on personal data protection in the European Union, and Council conclusions
- European Data Protection Supervisor communication to the EC (2011, 14 January). A comprehensive approach on personal data protection in the European Union
- Article 29 Data Protection Working Party; opinion 168 'The Future of Privacy', Opinion 8/10
- Stockholm Programme ; Rule 48
- Article 39 TEU
- The report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Industry, Research and Energy, the Committee (2011) on the Internal Market and Consumer Protection, the Committee on Culture and Education and the Committee on Legal Affairs
- Lisbon Treaty
- Regulation (EC) No 45/2001
- e-Privacy Directive
- Privacy and Data Protection Impact Assessment Framework for Radio Frequency Identification
- Safe Harbour Principles

Key points in the document

The document discusses the protection of personal data within the European Union, as well as third party countries. The authors focus on the need to clarify the way in which an individual's digital data is collected, stored, processed and used (both online and offline). Thus, it calls for not only increased transparency but also for the use of simpler terms for the end user.

Data protection, privacy and security are all three fundamental rights and the document asserts that citizens should not have to choose between being free and being safe. The document calls for an evaluation of current data protection rules, to ensure that there is still 1) a high level of protection, 2) a balance between privacy, freedom of speech and access to information and 3) no hindrance to everyday processing of personal data. The authors show support for 'privacy by design' and privacy enhancing technologies.

The authors place an emphasis on the need for special protections for children, young persons and the elderly. Awareness-raising programs are also encouraged. It calls for media literacy to be part of formal education, with the view of teaching minors how to act responsibly online.

The document indicates that increased transparency and understanding will breed trust for new technologies, and thus increase adoption and use. Therefore, it is stated that there should be clear consent provided for the collection and use of private data. Additionally, the authors note that those concerned should be notified when their data has been breached.

Assessment of the importance or significance of the document

An important document expressing the importance attached by the European Parliament to the topics of privacy and data protection and the original EC document.

(Evaluation on the basis of Google search hits, English language results)

A Google search for the exact title mainly provides mirrored links to the document. Some websites have written about the resolution, mainly legal websites. [5] It seems to have stayed out of the mainstream media.

A Google search of 'resolution' + "a comprehensive approach on personal data protection in the European Union" returns over 14,000 results. The first few links are directly to the article, and the following ones are documents which relate to it. One is the opinion of the Data Protection Supervisor with regards to this document. It was also noted to be an antecedent to legislative proposal on the processing of personal data[6].

[5] http://www.mondaq.com/x/143778/Data+Protection+Privacy/European+Parliament+Adopts+Resolution+on+Reform+of+Data+Protection+Directive
http://ipandit.practicallaw.com/3-506-8371?source=relatedcontent
http://legalmemory.blogspot.nl/2011/07/european-parliament-resolution.html
[6] http://www.europarl.europa.eu/oeil/popups/summary.do?id=1188884&t=e&l=en

146. Council of the European Union, *A Secure Europe in a Better World, European Security Strategy*, Brussels, 12 December 2003. 14 pages.

What domain (health, transport, policing, etc.) does it address?
International relations, global security

Target audience of the document
No specified audience in the document, but could be understood to be European citizens, policy makers, and external audiences. This document is in a readable, accessible form so the intended audience could be broad.

Stated purpose of the document
The document is the first European Security Strategy. The document sets out the key threats facing the EU, the EU's strategic objectives, and intention for an international order based on effective multilateralism, as well as the policy implications for Europe. The document implies that Europe should be making a more active contribution to global and regional security equal to its potential.

Context of the document
The document was drawn up by the EU High Representative for Common Foreign and Security Policy (Javier Solano) and adopted by the Council. It represents a clarification of Europe's International security policy. The document describes the context of Europe's security environment.

The document does not explicitly refer to any other texts.

Key points in the document
First, the document gives an account of Europe's peaceful and relatively secure context, with the European Union at the centre of this. The EU is identified as an inevitable global actor due to size, population, economy and available policy instruments. The document then sets out global challenges (internal and external security linked, globalisation, armed conflict, underdevelopment, competition for natural resources and energy dependence) and key threats (terrorism, weapons of mass destruction, regional conflicts, state failure and organised crime). It describes the EU's strategic security objectives: addressing the previously mentioned threats, building security in the EU's neighbourhood and promoting an international order based on effective multilateralism. The document argues that the EU needs to be more active in pursuit of its strategic objectives, increase its military, diplomatic, civilian post-crisis capability, be more coherent in terms of different foreign policy instruments and external activities of Member States, and work more closely with a broad range of international partners.

Assessment of the importance or significance of the document
The document is important and foundational as a statement of EU international security policy. It has however been superseded by later security strategies (Council of the European Union, *The Stockholm Programme – an open and secure Europe Serving and Protecting Citizens*, Brussels, 4th May 2010). Very relevant for the period 2003-2010.

164. Council of the European Union, The Stockholm Programme - An open and secure Europe serving and protecting citizens, 5731/10, Brussels, 3 March 2010. http://ue.eu.int/policies/fight-against-terrorism/documents/related-documents?lang=en. 135 pages.

What domain (health, transport, policing, etc.) does it address? Freedom, Security and Justice across a wide range of domains
Target audience of the document Many of the sections of the document are explicit invitations from the Council to the Commission to engage in particular activity. The Commission should therefore be considered the primary audience.
Stated purpose of the document The European Council reaffirms the priority it attaches to the development of an area of freedom, security and justice, responding to a central concern of the peoples of the States brought together in the Union. Document makes the argument that there are still challenges remaining, and it is time for a new agenda to build on previous efforts and enhance coherence in freedom, security and justice. This programme was adopted for 2010-2014.
Context of the document The context of the document follows on from the Tampere and Hague Programmes. Its introduction mentions the removal of internal border controls, more coherent management of external borders, significant steps in the creation of European asylum system, European agencies reaching operational maturity and enhanced civil cooperation, but acknowledges that there are still challenges to be addressed. The document mentions a large range of documents. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Lisbon 12.12.2007, OJ C306 17 December 2007. Article 11 of the treaty on European Union Article 68, 70, 84, 222 of the treaty of the functioning of the European Union Council of the European Union, European Pact on Immigration and Asylum, Brussels, 24.9.2008. http://register.consilium.europa.eu/pdf/en/08/st13/st13440.en08.pdf Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No.11 and No.14, Rome, 4 November 1950. The European Parliament, the Council and the Commission, Charter of Fundamental Rights of the European Union (2000/C 364/01), Nice, 18 December 2000. http://www.europarl.europa.eu/charter/pdf/text_en.pdf Council of the European Union, Framework Decision 2008/913/JHA of 28.11.2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ *L 328 , 6 December 2008.*

Hague Conference on Private International Law, Convention on the International Protection of Adults, Hague, 13 January 2000.

Council of the European Union, Directive 2004/80/EC of 29.4.2004 relating to compensation to crime victims, OJ L 261/15, 6 August 2004.

Council of the European Union, Framework Decision 2001/220/JHA of 15.3.2001 on the standing of victims in criminal proceedings, OJ L 82/1, 22 March 2001.

The Council of the European Union, Resolution of the Council on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, 2009/c 295/01), Brussels, 30 November 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:295:0001:0003:en:PDF

Council of Europe, Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data, Strassbourg, 28 January 1981. http://conventions.coe.int/treaty/en/treaties/html/108.htm

Council of the European Union, Conclusions on an Information Management Strategy for EU internal security, Brussels, 30 November 2009.

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 210/12, 6 August 2008.

Council of the European Union, Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA (Prüm framework). OJ L 210/12 6 August 2008.

Council of the European Union, Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89, 29 December 2006.

European Parliament and the Council of the European Union, Decision 1351/2008/EC, Establishing a multiannual community programme on protecting children using the Internet and other communication technologies, Brussels, 16 December 2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D1351:EN:NOT

Council of Europe, Convention on Cybercrime, CETS 185, Budapest, 23 November 2001.

Council of the European Union, Counter-Terrorism strategy, Brussels, 30 November 2005. http://register.consilium.eu.int/pdf/en/05/st14/st14469-re04.en05.pdf

Key points in the document

Sections (reflecting political priorities set out in the introduction) include, “towards a citizen’s Europe in the area of Freedom, Security and Justice”, “promoting citizen’s rights: a Europe of rights”, “Making people’s lives easier: a Europe of law and justice”, “a Europe that protects”, “access to Europe in a globalised world”, “a Europe of responsibility, solidarity and partnership in migration and asylum matters”, “Europe in a globalised world – the external dimension of freedom, security and justice”.

Promoting citizenship and fundamental rights: European citizenship should become fundamental reality, with a single area of rights and freedoms, beyond national boundaries. This makes specific mention of protecting personal data based upon the idea of a Union based upon common values and respect for fundamental rights and based European Convention for the protection of human rights and fundamental freedoms. This section also includes comments on the right to freedom of movement (including further enlargement of the Schengen area), respect for diversity and protection of the vulnerable, children's rights, victims of crime and terrorism, rights of individuals in criminal proceedings, protecting citizen's rights in the information society, participation in democratic life, and entitlement to protection in non-Member States.

The subsection on protecting citizen's rights in the information society makes reference to the rights to privacy and protection of personal data set out in the Charter of Fundamental Rights. The document argues that the Union must create a comprehensive strategy to protect data within the Union, promote application of relevant instruments on data protection, regulate the circumstances within which interference with these rights is justified and apply data protection principles in the private sphere. It identifies an increased exchange of personal data, and technological development that both challenge and provide new opportunities for the protection of personal data. Basic principles include purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality respect for the rights of the individual, control by national independent supervisory authorities and access to effective judicial redress. The document suggests that the EU should be a driver of international data protection standards, and these should be included in bilateral and multilateral agreements. The Council invites the Commission to evaluate existing data protection instruments, and where necessary produce further legislation, propose recommendations for data sharing principles with the US, consider data protection agreements with third countries for law enforcement purposes, improve compliance with data protection principles, examine the introduction of a European certification for "privacy aware" technologies, and conduct information campaigns.

A Europe of law and justice – consolidation of currently fragmented access to justice, recognition of legal decisions across Member States, training and cooperation. This section discusses the concept of mutual recognition introduced in Tampere 1999. The goal is for European legal systems to be able to work together effectively, in line with national legal traditions, and for citizens to be able to assert their rights anywhere in the Union. The document then looks at furthering the concept of mutual recognition in criminal and civil law, strengthening mutual trust (through training, developing networks, evaluation, improving tools implementation, and detention) and developing a core of common minimum rules. The document suggests that the benefit to citizens of a European judicial area come from providing easier access to justice and supporting economic activity

A Europe that protects: an internal security strategy should be developed that engages with organised crime, terrorism and other threats. Increase cooperation and coordination. The European Council is convinced that the enhancement of actions at European level, combined with better coordination with actions at regional and national level, are essential to protection from trans-national threats. In discussing the desired internal security strategy, the document discusses the European information exchange model and the information management strategy for internal security, which includes a strong data protection regime, and the need to share security relevant information whilst still protecting fundamental rights. This section also discusses network and information security, mobility related data sharing, sharing of criminal

records, travelling violent offenders, databases of third nationals with convictions, law enforcement databases, and passenger name records. This is all stated in terms of compatibility with protecting citizen's rights. The section also examines police cooperation, more effective crime prevention, crime data collection, protection against serious and organised crime, human trafficking, sexual exploitation of children and child pornography, cyber crime, economic crime and corruption, drugs, terrorism and disaster management. The document states the Union should establish the legal framework applicable to cyberspace within the Union, including evidence collection in cross-border investigations. There is also discussion of information sharing in relation to financial crimes and suspicious transactions. With regard to terrorism, the document states that respect for the rule of law, fundamental rights and freedoms is one of the bases for the EU's counter terrorism work.

Access to Europe in a globalised world – discusses integrated border management and visa policies to allow desirable access (business, tourists, students, scientists, etc.) but also guarantee security for citizens. This section includes discussion of the role of Frontex, capability building in third nations, the European Border Surveillance System (Eurosur), border checks, Schengen Information systems (SISII) and Visa Information System, and shared visa policy.

A Europe of responsibility, solidarity and partnership in migration and asylum matters. A key policy objective, with intention of establishing a common asylum system by 2012. Increasing pressure from illegal immigration. Makes particular reference to the member states at the southern borders.

Europe in a globalised world – the external dimension. Need for increase integration of external dimension of freedom, security and justice into general policies of the Union. External dimension of this programme is seen as critical.

Across all areas, the policy tools are seen as including: mutual trust, implementation of existing instruments, legislation, increased coherence (between EU institutions and agencies, and greater council oversight of agencies such as Europol, Eurojust, Frontex), evaluation, training, communication, dialogue with civil society, and financing.

Assessment of the importance or significance of the document

Highly important. This programme defines strategic guidelines for legislative and operational planning within the area of freedom, security and justice in accordance with Article 68 TFEU. It also makes a large number of invitations to the Commission to undertake particular legislative and policy activities, that will themselves produce significant outcomes. One of these is the call upon the Council and Commission to produce an internal security strategy

The European Council invited the Commission to submit a mid-term review before June 2012 of the implementation of the Stockholm Programme.

The document has significant sections on the balance between privacy (couched in terms of fundamental rights and data protection) and information-based security practices.

187. European Commission, Establishing a framework programme on "Security and Safeguarding Liberties" for the period 2007-2013, Communication to the Council and the European Parliament, COM(2005) 124 final, Brussels, 4 April 2005. 40 Pages.

What domain (health, transport, policing, etc.) does it address?
Law enforcement, security (prevention and fight against crime and terrorism), civil liberties (freedom), consequence management (of terrorist activities). Privacy is mentioned once, in the context of being a thematic area of security research. This document does not cover surveillance.

Target audience of the document
The European Council and the European Parliament

Stated purpose of the document
This document is a proposal to establish a framework programme on "Security and Safeguarding Liberties". It aims to tie together the existing frameworks regarding freedom, security and justice in a balanced manner. It exists for the following stated reasons:

1. to simplify and rationalise the framework both in financial, legal and management terms
2. to streamline budget structure
3. to increase coherence and consistency among programmes
4. to avoid duplication of efforts

The framework builds on two legal instruments: 1) Articles 30 and 34(2)(c) of the Treaty on European Union, covering the prevention and fight against crime, and 2) Article 308 of the Treaty establishing the European Community, covering the prevention, preparedness and consequence management of terrorist attacks.

Context of the document
The document refer explicitly to the terrorist attacks of 9/11 and underscore the importance of prevention and preparedness with regards to terrorist activities. Also the virtue words 'justice, liberty and freedom' are commonly used, noted to be the vary values that would be threatened in the event of a terrorist attack.

Other documents referred to:

- 7th Framework Programme on Research & Technological Development
- European Security Strategy of 12 December 2003
- Article 29 of the Treaty on European Union
- Vienna action plan
- The Hague Programme
- Title VI of the Treaty on European Union (Articles 29-42)
- Treaty establishing the European Community (Article 3(1)(u)).
- Article 308 of the Treaty establishing the European Community
- Commission Communications on:
    - Terrorism of 20 October 2004
    - Exchange of information and cooperation on terrorist offences
    - Enhancing police and customs cooperation in the EU
    - Enhancing access to information by law enforcement agencies
    - Building our common Future - Policy challenges and Budgetary means of the Enlarged Union 2007-2013

- Financial Perspectives 2007 – 2013
- Frameworks:
  - Fundamental Rights and Justice
  - Solidarity and Management of Migration Flows
- Declaration on solidarity against terrorism of 25 March 2004
- Community Civil Protection Mechanism
- European Programme for the Protection of Critical Infrastructure
- Rapid Response and Preparedness Instrument
- Article 308 of the Treaty establishing the European Community
- Article 54(2)(a) of the Financial Regulation
- European Drugs strategy in December 2004
- Council Decision 2002/630/JHA of 22 July 2002
- Regulation (EC, Euratom) No 2988/95
- Regulation (Euratom, EC) No 2185/96
- Regulation (EC) No 1073/1999

Key points in the document

The document states that freedoms and liberty cannot be guaranteed if one is not sufficiently protected from criminal acts. It is stated that citizens expect threats to health and safety will be countered at a European level, therefore prevention and combating crime (in particular terrorism) needs to be addressed on a European level. According to the authors, the Union can act as a catalyst for reinforcement and extension of legislation in this area, especially when given financial support. Moreover, it is stated that combining all activities related to law enforcement and crime prevention will lead to increased cost effectiveness and increased transparency.

It is stated that the programme aims to safeguard the EU as an area of Freedom, Security and Justice. Freedom, security and justice are noted as the three key objectives of the framework. They will be addressed through different legal bases, and the document states the framework is designed to be complimentary to existing community programmes. It proposes two different programmes:
1.Prevention, Preparedness and Consequence Management of Terrorism programme
2.Prevention of and Fight against Crime[7] programme.

The main justifications given for the programme are:
1. Financial intervention can ensure a fair sharing of responsibilities between member states, as well as reinforce solidarity between these states
2. More emphasis on promoting and developing partnerships between public and private organisations in the fields of; crime prevention, statistics and criminology, protection of victims and witnesses.
3. A more coordinated approach across member states towards prevention, preparedness, crisis and consequence management (re: terrorist threats), through using common approaches, including legislation.

Financial resources foreseen for the programme were 745 million euro for the period of 2007-2013. Within this, 142.4 million euro were foreseen for the specific programme for the programme Prevention, Preparedness and Consequence Management of Terrorism.

[7] Organised or otherwise, in particular terrorism, trafficking in persons and offences against children, illicit drug trafficking and illicit arms trafficking, corruption and fraud (p. 21)

Assessment of the importance or significance of the document
A very important EU policy document outlining the EU security strategy for the period 2007-2013.

(Evaluation on the basis of Google search hits, English language results)

A Google search indicates that this document has made some impact, as it returned over 35,000 results. Many of the top links were mirrors to the document itself (in English or translated into other European languages). It also appears to be referenced in other financial programmes by the EU including asylum and migration, and security research and innovation.

Google Scholar searches indicate that the document has been referred to in a few (around 20) different journals and book chapters. They are in relation to biometrics, security policy, social values, police cooperation within EU member states, terrorism, human trafficking and human rights.

188. European Commission, The Hague Programme: Ten priorities for the next five years The Partnership for European renewal in the field of Freedom, Security and Justice, Communication to the Council and the European Parliament, COM(2005) 184 final, Brussels, 10 May 2005. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0184:EN:HTML 19 pages.

What domain (health, transport, policing, etc.) does it address?
Freedom, security and justice (EU)

Target audience of the document
European Council and European Parliament

Stated purpose of the document
The Hague Programme marked the end of a cycle and the beginning of a new one. In order to carry out the Hague Programme, the European Council invited the Commission to present an Action Plan to the Council in which the aims and priorities of the Programme are to be translated into concrete actions, including a timetable for the adoption and implementation of all actions.

Context of the document
The European Council of 4-5 November 2004 endorsed the Hague Multiannual Programme for strengthening the area of freedom, security and justice, succeeding the Tampere Programme (1999) that was evaluated by the Commission in 2004 [COM(2004) 401, 2.6.2004]. This evaluation and the Recommendation adopted by the European Parliament on 14 October 2004 [P6_TA(2004)0022, 14.10.2004] have been taken into account in the Hague Programme, which set out the framework and main objectives for the next five years. It sought to respond to the expectations of citizens and dealt with all aspects of policies relating to the area of freedom, security and justice. It addressed both general orientations (fundamental rights, implementation and evaluation) and specific orientations, focusing on (1) strengthening freedom, (2) strengthening security, (3) strengthening justice, and (4) external relations.

This Action Plan needs to be read in conjunction with other Plans and Strategy papers regarding specific policy issues in the area of freedom, security and justice. These are identified as the EU Action Plan on Drugs of 14 February 2005 [COM(2005) 45, 14.2.2005], following the new European Strategy on Drugs 2005-2012; the Communication on Perspectives for the development of mutual recognition of decisions in criminal matters and of mutual confidence; and the Communication "Developing a Strategic Concept on Tackling Organised Crime". The Commission presented on 6 April 2005 three Framework Programmes on (1) Solidarity and Management of Migration Flows, (2) Security and Safeguarding Liberties and (3) Fundamental Rights and Justice [COM(2005) 122, 123 and 124, 6.4.2005]. The three proposals are fully in line with the strategic priorities set by the Hague Programme. The Strategic Objectives 2005-2009 [COM(2005) 12, 26.1.2005] referred specifically to the development of a partnership in view of the strengthening of an area of Freedom, Security and Justice. The Hague Programme called for a mid-term review of the Action Plan by 1 November 2006. The Commission will therefore present a report on the progress made and on the possible adjustments needed to the Programme.

Key points in the document

This Action Plan identifies, from among the orientations of the Programme, ten specific priorities upon which the Commission believes efforts for the next five years should be concentrated. It then lists a very large number of the concrete measures and actions to be taken over the next five years, with target dates for each. This list closely adheres to the structure of the Hague Programme. Within the objectives of (a) strengthening freedom (b) strengthening security (c) strengthening justice, the main ten priorities identified by the Commission was summarised as follows:

Fundamental rights and citizenship: creating fully-fledged policies; ensure the full development of policies monitoring and promoting respect for fundamental rights for all people and of policies enhancing citizenship.

The fight against terrorism: working toward a global response; focus on different aspects of prevention, preparedness and response in order to further enhance, and where necessary complement, Member States capabilities to fight terrorism, in relevant areas such as recruitment, financing, risk analysis, protection of critical infrastructures and consequence management.

A common asylum area: establish an effective harmonised procedure in accordance with the Union' values and humanitarian tradition; work towards the establishment of a common asylum area taking into account the humanitarian tradition and respect of international obligations of the Union and the effectiveness of a harmonised procedure.

Migration management: defining a balanced approach; Define a balanced approach to migration management by developing a common immigration policy which addresses legal migration at Union level, while further strengthening the fight against illegal migration, smuggling and trafficking in human beings, in particular women and children.

Integration: maximising the positive impact of migration on our society and economy; Develop supportive measures to help Member States and deliver better policies on integration so as to maximise the positive impact of migration on our society and economy and to prevent isolation and social exclusion of immigrant communities. This will contribute to understanding and dialogue between religions and cultures, based on the fundamental values of the Union.

Internal borders, external borders and visas: developing an integrated management of external borders for a safer Union; Further develop an integrated management of external borders and a common visa policy, while ensuring the free movement of persons (people-to-people).

Privacy and security in sharing information: striking the right balance; Strike the right balance between privacy and security in the sharing of information among law enforcement and judicial authorities, by supporting and encouraging a constructive dialogue between all parties concerned to identify balanced solutions, while fully respecting fundamental rights of privacy and data protection, as well as the principle of availability of information as laid down in the Hague Programme.

Organised crime: developing a strategic concept; Develop and implement a strategic concept on tackling organised crime at EU level. Make full use of and further develop Europol and Eurojust.

Civil and criminal justice: guaranteeing an effective European area of justice for all Guaran-

tee an European area of justice by ensuring an effective access to justice for all and the enforcement of judgments. Approximation will be pursued, in particular through the adoption of rules ensuring a high degree of protection of persons, with a view to building mutual trust and strengthening mutual recognition, which remains the cornerstone of judicial cooperation. Improve the EU substantive contract law.

Freedom, Security and Justice: sharing responsibility and solidarity; Give practical meaning to notions of shared responsibility and solidarity between Member States by providing adequate financial resources that can meet the objectives of Freedom, Security and Justice in the most efficient way.

Assessment of the importance or significance of the document

Very important. It outlined a very large programme of work for development in this field. It became a central focus. Other documents in our series that deal with the Hague Programme are from the House of Lords; European Parliament, and European Council.

204. European Commission, Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 171 final, Brussels, 20 April 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF 69 Pages.

What domain (health, transport, policing, etc.) does it address?

Privacy

- Ensuring the protection of fundamental rights

Security

- Crime and terrorism, cross-border criminality, victims of crime, cyber-crime and network security

Surveillance

- Boarder surveillance (who is responsible for implementation and reporting)

Target audience of the document

The European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, FRONTEX, EASO,

Stated purpose of the document

The authors state that The European Union should respond to expectations and concerns of its citizens, to ensure the protection of fundamental rights and provide an area of freedom, security and justice.

The document exists to formulate a timetable to implement the Stockholm Programme. It is necessary so that all involved parties know their responsibilities in the implementation.

It directly relates to the Stockholm Programme, and its focus is to translate these political objectives into concrete proposals, for adoption between 2010 and 2014.

Context of the document

The document was written at a time when the authors saw Europe beginning to be affected by the global financial / economic crisis and in the context of constant social and technological change.

Other documents referred to:

- Council document 17024/09
- EU Charter of Fundamental Rights
- the Lisbon Treaty
- Europe 2020 Strategy
- EU Civil Protection Mechanism

Key points in the document

The authors believe that security, justice and fundamental rights should not be treated in isolation, and instead should go together in formulating a coherent approach to meet the challenges of a rapidly changing social and technological environment that puts risks on freedoms, justice and security. The authors state that European citizenship needs to become a

tangible reality, that has added value over national citizenship.

There is special attention towards policies responding to violence against women and children. They also make special note of safeguarding children's rights. Free movement is something which the authors state needs to be rigorously enforced through removing existing barriers when moving from one Member State to another.

To soften the damage caused by the financial crisis, the authors state that reducing administrative burdens and transaction costs will help businesses recover. For instance, the authors note that cross-border debt should be able to be recovered just as easily as domestic debt through legislation.

The authors also touch on criminal law, where they state that "criminals should not be able to avoid prosecution and prison by crossing borders and exploiting differences between national legal systems" (p. 5). The authors recognise the growing cross-border criminality.

Therefore, the document states that increased information sharing from police, border authorities, criminal justice agencies and the like, on cross-border cases will help mitigate this. According to the authors, this would also require an overview on the existing data collection and processing systems, with an assessment of their efficiency, effectiveness and their respect to the right to privacy.

Immigration is also addressed by the authors, where it is said that a coherent migration and asylum policy across member states is necessary.

Assessment of the importance or significance of the document
Important EU document outlining priorities translating the broad strategic lines in the areas of freedom, security and justice.

(Evaluation on the basis of Google search hits, English language results)

A Google search of "Action Plan Implementing the Stockholm Programme" returned over 46,700 hits. The first 20 hits were all websites which linked to the document, but also made a brief news post about what the document contained. Some websites were official governmental sites (such as the European Union website and the UK parliament website), and some were independent blogs. Interestingly, it is also required reading for those studying Migration Law at McGill university.

A search of the same key words in Google Scholar indicated that the document was referenced in at least 100 different journal articles and books. Many of the references were in articles and books about migration and foreign policy. Others were about practicing European Law. A few were about data protection and privacy, in the context of a new European framework.

When searching for "Action Plan Implementing the Stockholm Programme" + response, I found that there was a response from the Committee of Regions[8] and UK Parliaments Department of Justice and Home Affairs[9]. It was referred to in a motion for a European Parlia-

[8]http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B7-2012-150&language=EN http://eur-

[9] http://www.publications.parliament.uk/pa/ld201011/ldselect/ldeucom/90/9003.htm

ment resolution on judicial training (2012, March 9).[10] The document was also recommended for debate by the UK House of Lords.[11]

[10] lex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,nl&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=559876:cs&page=

[11] http://www.publications.parliament.uk/pa/ld201012/ldselect/ldeucom/149/14904.htm

232. European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, Brussels, 25 Jan 2012. 118 pages.

What domain (health, transport, policing, etc.) does it address?
Data protection

Target audience of the document
The document is directed at the European Parliament and the Council. However, if the proposal is accepted, much of this document will become text of a Regulation, and the audience will be Europe-wide.

Stated purpose of the document
This document is a proposal from the EU Commission for a regulation by the European Parliament and the Council. This explanatory memorandum presents in further detail the proposed new legal framework for the protection of personal data in the EU as set out in Communication COM (2012) 9 final, specifically legislative proposal for general data protection regulation. The document argues that rapid technological changes mean that the previous centrepiece of EU data protection legislation (Directive 95/46/EC, complemented by Framework Decision 2008/977/JHA) has been challenged. Whilst its principles are seen as sound, it has not prevented legal uncertainty, fragmented implementation of data protection across the EU, and public perception of risks associated with online activity. This document therefore sets out for the case for personal data protection reform. Stated objectives are to ensure consistent enforcement of data protection rules, and to rationalise the current governance system to assist with this.

Context of the document
Personal data protection is seen as a key element of the Digital Agenda for Europe and the Europe 2020 strategy. This appears to be strongly driven by the Commission. The Action Plan implementing the Stockholm Programme stressed the need to ensure that the fundamental right to personal data protection is consistently applied in the context of all EU policies. Additionally, in the Communication on "A comprehensive approach on personal data protection in the European Union", the Commission concluded that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection. The proposal also results from two years worth of public and stakeholder consultation on the legal framework for the fundamental right to the protection of personal data and the comprehensive approach to personal data protection. A Regulation would be more consistent than a Directive. The Lisbon Treaty also contained a special provision on the protection of personal data in article 8 of the Charter of Fundamental Rights.

The document refers to a range of other documents, many of which are EU legal instruments.

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 of such data, OJ L 281, 23 November 1995. The document makes frequent reference to this Directive, as the proposed resolution, whilst based upon the Directive, would significantly alter it.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of per-

sonal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30 December 2008

Article 16(1) of Treaty on the Functioning of the European Union (TFEU), as introduced by the Lisbon Treaty,

Article 16(2) TFEU, the Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data.

European Commission, Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions – A digital agenda for Europe, COM(2010) 245 final. Brussels, 26 August 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

European Commission, Communication from the Commission, Europe 2020: a strategy for smart, sustainable and inclusive growth, COM(2010) 2020 final, Brussels, 3 March 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

European Council, The Stockholm Programme — An open and secure Europe serving and protecting citizens, OJ C 115, 4 May 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF

Resolution of the European Parliament on the on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme adopted 25 November 2009 (P7_TA(2009)0090).

European Commission, Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions – Delivering an area of freedom, security and justice for Europe's citizens Action Plan Implementing the Stockholm Programme, COM(2010) 171 final, Brussels, 20 April 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0171:EN:HTML

European Commission, Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection within the European Union. COM(2010) 609 final, Brussels, 4 November 2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

Special Eurobarometer (EB) 359, Data Protection and Electronic Identity in the EU(2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002,

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Reg-

ulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Text with EEA relevance; OJ L 337, 18 December 2009.

Key points in the document

The document first sets out the existing legal instruments relating to personal data protection in the EU, and the need for reform, followed by an account of the consultation process leading to this document, including the impact assessment process and the resultant changes. The third section sets out the legal basis for the proposal, fundamental rights issues, and then a detailed explanation of the proposal, article by article, describing the intentions of each section. Following a small section on budgetary implications the majority of the document is the text of the proposed Regulation, followed by a legislative financial statement.

A strong logic through this text is the need from economic stakeholders to have consistency increased and uncertainty reduced in relation to personal data protection across the EU. The document places a stronger emphasis on data minimisation, valid explicit consent and the encouragement of "Privacy by Design" and data protection by default. The proposed regulation introduces a number of changes to personal data protection in the EU. These include: More supervision and enforcement (including protections of the independence of national Data Protection Authorities, stronger enforcement and fining powers, mechanisms for cross border collaboration of DPAs and a European Data Protection Board built upon the Article 29 working party), measures to enhance individuals' control of their personal data (strengthening rights, clarifying the concept of consent, introducing a strong right to object to profiling, greater transparency, rights to data portability, procedures for exercising those rights, and the deletion of unnecessary data (the "right to be forgotten")). There is also focus upon the responsibilities of "responsible organisations" with obligations to good data management practices (including security), the principle of accountability, the burden of proof for legality, proportionality etc, data protection impact assessments, and the introduction of security breach notification. There is also an international dimension in which data protection rights are asserted against third country entities delivering services in the EU, or monitoring the behaviour of Europeans.

Assessment of the importance or significance of the document

Highly significant. Its impact is wide-ranging, and would bring in significant changes to the DP framework in Europe. A Regulation, if passed, becomes immediately enforceable as law in all Member States, and does not require transposing into national law. This would be applicable to both public and private sectors. Under discussion by Council and Parliament, anticipated by 2014.

This document should be considered alongside the proposal for a Directive for data protection in law enforcement:

European Commission, Proposal for a Directive of the European Parliament and of 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 offenses or the execution of criminal penalties, and the free movement of such data, COM(2012) 010 final, 25 January 2012.

292. European Network and Information Security Agency (ENISA), *Cyber security: Future challenges and opportunities*, 2 December 2011. http://www.enisa.europa.eu/publications/position-papers/cyber-security-future-challenges-and-opportunities 27 pages.

What domain (health, transport, policing, etc.) does it address?
Cyber security, Critical infrastructure protection

Target audience of the document
Public and private sectors, EU institutions and bodies, Member States, "multiple stakeholders", including down to individual citizens.

Stated purpose of the document
This document is part of working towards a holistic, collaborative, international and aligned approach to cyber crime and cyber security across sector and national boundaries. It provides an overview of ENISA's role and activity in cyber security.

Context of the document
Increased dependence on ICT makes critical infrastructure protection not just about security but also about competitiveness and prosperity. Networks are globally connected. There is a need for consistency across geographical borders, international coordination is required. The Lisbon treaty is seen as an opportunity to improve dialogue between communities in network and information security.

The document mentions the following other documents:

European Commission, A Digital agenda for Europe Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions. COM(2010) 245 final, Brussels, 19 May 2010.

European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Communication from the Commission to the European Parliament and The Council, COM(2010) 673 final, Brussels, 22 November 2010.

European Network and Information Security (ENISA), *Cloud Computing: Benefits, risk and recommendations for information security*, 20 November 2009.

European Network and Information Security (ENISA), *Botnets: Measurement, Detection, Disinfection and Defence*, 07 March 2011. www.enisa.europa.eu/activities/resilience-and-CIIP/networks-and-services-resilience/botnets/botnets-measurement-detection-disinfection-aand-defence

European Network and Information Security (ENISA), *EISAS – European Inforamtion Sharing and Alert System for citizens and SME's: A Roadmap for further development and* deployment, 16 February 2011. www.enisa.europa.eu/activities/cert/other-work/eisas_roadmap/

European Commission, A strategy for smart, sustainable and inclusive growth, Communication from the Commission, COM(2010) 2020 final, Brussels, 3 March 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

European Commission, Critical Infrastructure Protection 'Achievements and next steps: towards global cyber security', Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions, COM(2011) 163 final, Brussels, 31 March 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:HTML

Europol, *EU Organised Crime Threat Assessment (OCTA) 2011,* The Hague, 4 May 2011. https://www.europol.europa.eu/content/press/europol-organised-crime-threat-assessment-2011-429

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services

Council of the European Union, EU-U.S. Summit 20 November 2010, Lisbon – Joint Statement, MEMO/10/597, Brussels, 20 November 2010. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597

European Parliament and the Council of the European Union, Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency. 10 March 2004. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

Key points in the document

The introduction provides context for the document which focuses upon dependency upon ICT, in an increasingly globally interconnected society. Despite the positive benefits of this, there are also a range of threats. The document provides an overview of four malicious threats (stuxnet, attacks on EU Emission's trading scheme, 2011 attacks against RSA, Sony Playstation Network, and Diginotar). It provides category definitions for cybercrime, cyber espionage. The document provides an account of current inconsistent approaches to cyber security in different Member States and argues for a coherent pan-European approach. It describes ENISA's role as providing a neutral European platform, establishing and maintaining networks, promoting dialogue, providing expertise and advice, risk assessment and management. The document then provides more detailed information on ENISA activity in the areas of trend and threat analysis, awareness of risks and challenges, early warning and response, critical information infrastructure protection, supporting the international CERT community, policy implementation, action against cybercrime, international cooperation, information exchange and building communities. It also remarks upon ENISA's future and the intention to agree a new more flexible and responsive mandate for the agency. The document concludes by identifying a number of areas where current EU approaches to cyber security could be extended (cross-border collection of data relating to cyber security, improved dialogue between information security communities, a proactive approach to building new cross-border communities, modernisation and further development of ENISA).

Assessment of the importance or significance of the document

ENISA assists the European Commission in the technical preparatory work for updating and developing community legislation on network and information security. The publication is not a legal action by ENISA. The document is an overview of ENISA's cyber security role and activity against the context of how the agency sees the cyber security threat and risk envi-

ronment.

315. Article 29 Data Protection Working Party, Opinion 10/2001 on the need for a balanced approach in the fight against terrorism, WP 53, Brussels, 14 December 2001. 4 pages

What domain (health, transport, policing, etc.) does it address?
Counter-terrorism

Target audience of the document
European decision-making bodies

Stated purpose of the document
A reminder that counter-terrorism legislation and measures of surveillance must be consistent with human rights, freedoms, and data protection requirements.

Context of the document
Directly in response to 9/11 and the temptation to cast aside liberties, rights, etc. in the name of combating terrorism.

It refers to several documents: The Data Protection Directive 95/46/EC and Directive 97/66/EC; the Council of Europe Cybercrime Convention of 31 November 2001; the conclusions of the EU Justice and Home Affairs summit of 20 September 2001, the "roadmap" of the European Union following the attacks in the United States (13880/1) of 15 November 2001; other Article 29 documents (the Working document "Processing of Personal Data on the Internet" of 23 February 1999, Recommendations 1/99 on "Invisible and Automatic Processing of Personal Data on the Internet performed by software and hardware" and 2/99 on the "Respect of privacy in the context of interception of telecommunications" and 3/99 on the "Preservation of traffic data by Internet Service Providers for law enforcement purposes", the Working document "Privacy on the Internet – An integrated EU Approach to On-line Data Protection" of 21 November 2000, Opinions 2/2000 concerning "The general review of the telecommunications legal framework" and 7/2000 "On the European Commission proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 – COM(2000)385", Opinion 4/2001 on "the Council of Europe's Draft Convention on Cyber-crime" and Opinion 9/2001 on the Commission communication "Creating a safer Information Society by improving the security of information infrastructures and combating computer-related crime"); and the Charter of Fundamental Rights of the European Union.

Key points in the document
It briefly reviews the measures taken or proposed for increasing surveillance and data processing to combat terrorism. While it is necessary to fight terrorism, respect must be had for legalities and for fundamental rights (including privacy) and freedoms in a democratic society. Intrusive measures include biometrics, telephone tapping, telecommunications data retention, data-sharing, real-time surveillance. Proportionality and long-term consequences of these developments must be taken into account. It 'underlines the need to establish a comprehensive debate on the initiatives to fight terrorism analysing all their consequences on the fundamental rights and freedoms of persons and in particular refusing the amalgam between fight against real terrorism and the fight against criminality in general, as well as limiting the procedural measures which are invasive to privacy to those really necessary.' It warns against seeing data protection as a barrier to the fight against terrorism: measures to combat terrorism must not reduce the standards of rights protection.

Assessment of the importance or significance of the document

It is a significant response by the Working Party to tendencies that were rapidly developing after 9/11 but which had earlier antecedents.

355. Article 29 Data Protection Working Party, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, 1 December 2009. 28 pages.

What domain (health, transport, policing, etc.) does it address? Legal and regulatory affairs.
Target audience of the document European Commission and the general DP/privacy policy community.
Stated purpose of the document Response to EC consultation on the future effectiveness of Directive 95/46.
Context of the document Highly significant contribution because it comes from the Article 29 WP and the Working Party on Police and Justice (WPPJ).
Key points in the document It assesses the need for possible changes concerning the 95/46 Directive and other instruments, in the light of new technologies, globalisation, law enforcement, surveillance, etc. Sees the need for clarification of rules and principles, innovation of new principles, strengthening the effectiveness of the law, and formation of a comprehensive framework post-Lisbon Treaty. More specifically, it gives a brief overview of the history and context of data protection in the EU, and proposes the introduction of one comprehensive legal framework while recognising the need for specific rules (*leges speciales*), provided that they fit within the notion of a comprehensive framework and comply with the main principles so that the main safeguards and principles of data protection apply to data processing in all sectors. Considering that data protection is a fundamental right, it calls upon the Commission to take initiatives towards the further development of international global standards regarding the protection of personal data, and it highlight other legal instruments that are useful internationally. It reasserts the value of sound and technologically neutral principles and concepts as exemplified in the existing Directive. Because there are new risks to privacy stemming for technological developments, it invokes the need for a binding principle of 'Privacy by Design', PETS and privacy default settings, and for embedding data protection and privacy principles into specific technological contexts. It goes on to argue that the main challenges to data protection require a stronger role for the different actors, including a stronger position for the data subject in the data protection framework, suggesting ways of empowering the data subject. This would require improvement of redress mechanisms, including class actions. In addition, the new framework should provide alternative solutions in order to enhance transparency and the introduction of a general privacy breach notification, and should specify the requirements of 'consent'. It argues that harmonisation needs to be improved, as the empowerment of the data subject is currently being undermined by the lack of harmonisation amongst the national laws implementing Directive 95/46/EC. The role of data subjects on the internet is an area of should be further clarified. It aims at strengthening the responsibility of the data controllers by embedding data protection in organizations, so that it becomes part of shared values and practices, and responsibilities for it should be expressly assigned; this will help DPAs as well. It presses for the introduction of an accountability principle, and for streamlined notification by data controllers to DPAs. It envisages stronger and clearer roles for national DPAs, as well

as greater uniformity of standards and powers, as well as their independence and ability to make policy inputs. The co-operation of the DPAs should be improved, and the working methods of the WP29 should be further improved. An MoU between WP29 and the Commission would improve their relations. Finally, the document discusses the data protection challenges in the field of police and law enforcement, in the context of the Lisbon Treaty. The Framework Decision 2008/977/JHA on the protection of personal data in the framework of police and judicial co-operation in criminal matters can be seen as a first step towards a general framework in the former third pillar. The dramatic increase of the storage and exchange of personal data in this sector, and in the context of new threats resulting from terrorism and organised crime, and stimulated by the technological developments, pose immense challenges for data protection and should be addressed in the future legal framework. The WP29 discusses the conditions for law and policy making on data protection in this area.

Assessment of the importance or significance of the document

This document was very influential. It focused and contributed to subsequent debate leading towards the 2012 'package' of data protection legislative change (new Regulation and Directive). It became very widely known and discussed. The measures adopted in the new framework should be compared to the measures advocated in this document.

363. Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, WP 192, Brussels, 22 March 2012. 9 pages

What domain (health, transport, policing, etc.) does it address?
Online and mobile services

Target audience of the document
The document is explicitly addressed to European and national legislative authorities, data controllers and the users of online or mobile facial recognition technologies.

Stated purpose of the document
The stated purpose of this document is to consider the legal framework and provide appropriate recommendations applicable to facial recognition technology when used in the context of online and mobile services. This is necessary because there has been a rapid increase in the availability and accuracy of facial recognition technology.

Context of the document
The document is in response to developments in facial recognition technology and particularly its application in online services (including social networks) and on mobile devices. The documents states that this requires specific attention from WP29 as the use of the technology in this manner raises a range of data protection concerns.

The document makes reference to several other documents throughout the text. These are primarily other Article 29 working group opinions and:
European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

The document builds upon (but does not repeat):
Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, Brussels, 27th April 2012.

Also referenced are:
Article 29 Working Party, Opinion 5/2009 on online social networking, WP163, Brussels, 12th June 2009;

Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP136, Brussels, 20th June 2007;

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP169, Brussels, 16th February 2010;

Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP18, Brussels, 13th July 2011.

Article 29 Working Party, Working document on biometrics, WP80, Brussels, 1st August 2003.

Key points in the document
After stating its context, stated purpose and audience in the introduction, the document pro-

vides some definitions of digital image and facial recognition, including the component processes of facial recognition (image acquisition, face detection, normalisation, feature extraction, enrolment and comparison). It provides examples of facial recognition as a means of identification, a means of authentication/verification, and as a means of categorisation. The document then discusses the legal framework. This is based upon the Data Protection Directive (95/46/EC) and considers digital images as personal data, digital images as special categories of personal data, the processing of personal data in the context of a facial recognition system, data controllers, legitimate ground. Finally it addresses five specific risks (unlawful processing for the purposes of facial recognition; security breaches during transit; face detection, normalization and feature extraction; security breaches during data storage; and subject access) and makes specific recommendations in relation to those risks.

Key arguments include face recognition is considered as data processing, digital images of the face should be considered as biometrics (and sensitive biometrics if they can be used to infer sensitive categories such as ethnicity, religion or health), that some processing of facial images may be required to ascertain if an individual has given their consent for further processing, that information that facial recognition is in use should be directly given to users, and that data controllers must engage in a range of measures to ensure that data is processed securely and data protection rights are protected.

Assessment of the importance or significance of the document

The Article 29 working party has an advisory status and acts independently. It was set up under the directive 95/46/EC and is composed of representatives of the data protection supervisory authorities of EU member states, representatives of the authorities established for EU institutions and bodies, and a representative of the Commission. This document is significant in the particular case of facial recognition technology, but also demonstrates an application of EU law on data processing and data protection to a specific set of technologies.

364. Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, WP 191, Brussels, 23 March 2012. 32 pages.

What domain (health, transport, policing, etc.) does it address? Privacy and data protection across all domains.
Target audience of the document The Commission.
Stated purpose of the document Despite its generally positive stance toward the proposed Regulation, the Working Party feels that parts of the proposal for a Regulation need clarification and improvement. With regard to the Directive for data protection in the area of police and justice, the Working Party is disappointed by the Commission's level of ambition and underlines the need for stronger provisions. The Working Party highlights areas of concern and makes suggestions for improvement. The Working Party may produce further opinions on the proposals in the future.
Context of the document The Opinion provides the Art 29 WP's views on the EC's proposed Data Protection Regulation and Directive for data protection in the area of police and justice released on 25 Jan.
Key points in the document Following an introduction and general remarks, the Opinion is in two main parts. The first part covers the Working Party's views on the proposed Regulation and the second part on the proposed Directive for data protection in the area of police and justice. Space does not permit an easy summary of all of the key points made in the Art. 29 WP's Opinion. However, the points in the table of contents give a good indication of its breadth. Among the points regarding the proposed Regulation, the Art 29 WP addresses the following: Positive aspects Role of the Commission Role of European Data Protection Authorities in policy-making Thresholds for SMEs Implications on budget and resources General provisions The principle of public access to information Further incompatible use Exceptions introduced for public authorities Minors Right to be forgotten Direct marketing Profiling Representative Accountability Data breach notification With regard to the role and functioning of DPAs Jurisdiction and competence of DPAs (one-stop shop) Mutual assistance Consistency "One-stop shop" for data subjects

EDPB institutional structure
International transfers
Disclosures not authorised by EU law
Right to liability and compensation
Fines
Judicial remedies
Churches and religious associations

Re the Directive, the Working Group covers the following:
Choice of instrument
Consistency
Scope of application
Data processing principles
Data subject rights
Data controller obligations
International transfers
Powers of DPAs and co-operation
What is missing

Assessment of the importance or significance of the document
The Art. 29 Working Party's views are of central importance as it represents those of the DPAs. One can assume the EC would take on board many if not all of the Art. 29 WP's suggestions for amendments. The Opinion is important for other stakeholders too, especially industry, as it is a clear indication of the support for the draft data protection framework as well as an indication of what needs to be fixed.

368. European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final), Brussels, 26 September 2005. 12 pages

What domain (health, transport, policing, etc.) does it address?
Data retention in law-enforcement and counter-terrorism.

Target audience of the document
Probably the European Commission and European Parliament, but the Council, the Article 29 WP, and other bodies would be part of the audience as well.

Stated purpose of the document
Response to the proposal for a data retention directive, giving the EDPS view on the impact on privacy and data protection.

Context of the document
EDPS says that the proposal 'must be seen as a reaction to the initiative by the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom for a Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism ('the draft Framework Decision'), that was rejected by the European Parliament (in the consultation procedure).' He was not consulted on the draft Framework Decision and is not giving an opinion on it yet, but in this document he is giving his views on the proposal's substance.

Other substantive documents mentioned include the EU DP Directive 95/46/EC and Telecomms Directive 2002/58/EC; the European Convention on Human Rights; the EU Treaty; the Charter on Fundamental Rights; Article 29 Data Protection Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)], WP 99, Brussels, 9 November 2004 [our number 306]; 'Liberty and security, striking the right balance', Paper by the UK Presidency of the European Union of 7 September 2005.

Key points in the document
While recognising the importance of fighting terrorism and other serious crime, and improving law enforcement, this does not imply a need for new instruments as foreseen the proposal. It is essential to the EDPS that the proposal respects fundamental rights. The necessity and the proportionality of the obligation to retain data — in its full extent — have to be demonstrated. More safeguards are needed. There is no evidence of the necessity for retention for a year; on this and other points, the Art 29 WP opinion 99 of 2004 [our number 306] should be the departure point for appraisal of the proposal. Proportionality must be demonstrated. 'The EDPS takes the view that retention of traffic and location data alone is in itself not an adequate or effective response [to the threat of terrorism]. Additional measures are needed, so as to ensure that the authorities have a targeted and quick access to the data needed in a specific

case. The retention of data is only adequate and effective in so far as effective search engines exist.' To be proportionate, the proposal should limit the retention periods; limit the number of data to be stored; and contain adequate safety and data security measures. The EDPS points out the need of an effective control on the access and further use, preferably by judicial authorities in the Member States. The EDPS questions the legal basis of the proposal as well. He goes on to make specific observations on details of the proposal before stating that the proposal's idea of having an evaluation of the proposed Directive within three years is welcome.
Assessment of the importance or significance of the document Data retention became one of the most controversial privacy and data protection issues of the post-9/11 world. The EDPS' document was a significant contribution to policy discussion and a defence of fundamental rights. There were other documents on this issue, from a number of other organisations in the EU and Member States. Subsequently, the EU legislated Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13 Apr 2006. In 2011, the EDPS gave an opinion on the evaluation report on the Directive and the Council of the EU consulted on the reform of the Directive at the end of 2011.

394. European Data Protection Supervisor (EDPS), Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels, 18 March 2010. 21 pages.

What domain (health, transport, policing, etc.) does it address?

- Data security (RFID, social networks and browser apps)
- Privacy by design

Surveillance is mentioned only a side note in relation to the privacy recommendations.

Target audience of the document

The European Commission

Stated purpose of the document

It is a statement of opinion on promoting trust in the information society. It exists to provide recommendations for the European Commission for a new European Digital Agenda. It is necessary because ICT raise new concerns that are not covered in the existing framework. The document builds on earlier opinions of the EDPS.

Context of the document

The document builds on previous ICT data protection policies and opinions by the EDPS. It relates to building online health and government service policies (e.g., eHealth, eTransport, eGovernment). Security concerns are raised by the author about the sensitive nature of the data necessary to use online health; about tracking through use of RFID; about government policies in general. This is why trust is noted as very important for the emergence and successful development of ICTs.

Other documents referred to:

- Treaty on the Functioning of the European Union (Article 16)
- Charter of Fundamental Rights of the European Union (Articles 7 & 8)
- Directive 95/46/EC of the European Parliament (1995, 24 October)
- Directive 2002/58/EC of the European Parliament (2002, 12 July, amended by Directive 2009/136/EC, 2009 November 25)
- Regulation (EC) No 45/2001 (2000, 18 December), Article 41
- Article 29 Working Party, Opinion 168 "Future of Privacy"
- EDPS Opinions: 25 July, 2007 on the implementation of the Data Protection Directive; 20 December, 2007 on the RFID; the two opinions on the ePrivacy Directive (2008, 10 April & 2009, 9 January)
- Europe's Digital Competitiveness Report
- Post i2010 Strategy - Toward an open, green and competitive knowledge society
- European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), Article 8
- The Data Protection Directive (Article 17)
- The ePrivacy directive (Articles 14.3, 5.3)
- The Stockholm Programme
- Safer Social Networking Principles for the EU
- 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Key points in the document

The salient idea was that of 'privacy by design' (PbD). Recommendations for specific ICT areas (RFID, social networks and browser applications) are discussed. These recommendations are suggested to be clarified in legislation, as well as used as a guiding principle when implementing policies, activities and initiatives in ICT sectors.

The author of the document formulates a clear concern about the increased collection and analysis of personal data, as well as the technological capabilities to track and hack individuals. It is a concern that has been realised from the proliferation of ICTs – with increased possibilities comes increased risk.

PbD can be applied to RFID, social networks and browsers. It is recommended that PbD provisions could be already included in existing legal instruments. In the non-legislative sense, the document recommends that PbD should be a guiding principle in Europe's Digital Agenda, as well as in other EU initiatives. Moreover, legislation to hold service providers accountable for complying with PbD is recommended.

The main issue with RFID and social networks was the possibility for data to be tracked unbeknownst to the user (through the RFID or cookies for social networks), which was reflected in the recommendation for increased self-regulation and further education on personal responsibility as a data controller.

Assessment of the importance or significance of the document

(Evaluation on the basis of Google search hits, English language results)

From a Google Scholar search, this document seems to have made a small impact. It has been used in a handful of research journals and has been linked to by a few public websites. However it is unclear if policies have been drafted with this document as a basis.

A Google search of "Opinion on Promoting Trust in the Information Society" returns 5,230 results, but 25 of these results are directly related to this document. This is known because the results of this search do exceed 3 pages. It is therefore unclear how Google gets the figure of 5,230. The majority of the top results are not mirror links to the document but are summaries of the document, or 'news posts' about the document being released. The websites which mention this document include:

- The Electronic Privacy Information Center
- The European Digital Rights
- The Practical Law Company

The document was also referenced in a Submission from the Office of the Privacy Commissioner of Canada to the Digital Economy Consultation[12] titled: Privacy, Trust and Innovation – Building Canada's Digital Advantage (2010). Therefore, it has made an impact in European Parliament and international governments. In the public eye it has mainly caught the attention of law experts.

[12] http://www.priv.gc.ca/information/pub/sub_de_201007_e.asp

413. European Data Protection Supervisor (EDPS), Opinion on the data protection reform package, Brussels, 7 March 2012. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf 75 pages.

What domain (health, transport, policing, etc.) does it address?
European data protection reform

Target audience of the document
The document is primarily directed towards the European Commission, which requested the EDPS Opinion on the data protection reform package. It will also be of interest to other national data protection authorities and lawmakers.

Stated purpose of the document
The document is the European Data Protection Supervisor's opinion on the data protection regulation reform package put forward by the Commission. It is therefore a nuanced reading of the elements of that package, in relation to strengths and weaknesses. The document also makes a series of recommendations to improve the proposed reforms.

Context of the document
The EDPS was asked by the European Commission to deliver his Opinion on the package of data protection reforms that included:

- A proposed Regulation (on the protection of individuals with regard to the processing of personal data and on the free movement of such data) intended to replace Directive 95/46/EC and amend Directive 2002/58/EC,
- A proposed Directive (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) intended to replace Framework Decision 2008/977/JHA,
- A Communication entitled "Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century" COM(2012) 9 final.

This document is that opinion.

In addition to the documents in the data protection reform package, this document refers to a number of other related documents.

The Treaty on the Functioning of the European Union (in particular Article 16):
"The Lisbon Treaty inserted a new, single legal basis for rules on data protection in Article 16 of the TFEU. This single legal basis constitutes the legal impetus for reconsidering the existing EU rules on data protection."

The Charter of Fundamental Rights of the European Union (in particular Article 7 and 8

European Parliament and the Council, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995.

European Parliament and the Council of the European Union, Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Com-

munity institutions and bodies and on the free movement of such data. OJ L8/1, 12 January 2001.

European Data Protection Supervisor (EDPS), Opinion on the Communication 'A comprehensive approach on personal data in the European Union' of 14 January 2011, OJ L181, 22 June 2011.

Article 29 Working Party, The Future of Privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP168), 1 December 2009.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ L121, 15 May 2009.

Council of the European Union, Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L138, 4 June 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:138:0014:0032:EN:PDF

Council of the European Union, Council Decision 2008/615/JHA on the stepping up of cross-border cooperation,particularly in combating terrorism and cross-border crime, 23 June 2008 OJ L210, 6 August 2008.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF
The Prüm-Decision

Key points in the document

The document provides initial remarks on the reform package, the need for reform of the EU legal framework on data protection (technological change, legal certainty harmonisation, police and judicial co-operation and increased global data transfer) and the package's main weakness, before providing specific comments on the proposed regulation and the proposed directive.

For the EDPS, the main weakness of the reform package is that it does not remedy the current lack of comprehensiveness of the EU data protection framework. Data protection rules for EU institutions, bodies and agencies have been left unchanged, as have police and judicial cooperation in criminal matters. No timeframe has been provided for further reform of these areas. The Directive is a self-standing legal instrument, not a sectoral addition to the Regulation. It therefore contains different versions of definitions, principles, rights and obligations for the law enforcement sector. Relations between the two instruments are not clear enough.

The document then comments upon the Regulation and Directive in chapter-by-chapter detail. For the Regulation this entails an introduction; horizontal issues; general provisions; principles; rights of data subjects; controllers and processors; transfers to third countries; competences and powers of supervisory authorities; co-operation and consistency; remedies, liability and sanctions; and specific data processing situations. For the Directive, this entails an introduction; horizontal issues; general provisions; principles; rights of data subjects; competences and powers of supervisory authorities, transfer to third countries; and oversight mechanisms.

The document raises concerns about the relationship between the regulation and national law as several sections build upon national law allow national law to give effect to its provisions, specify or develop rules, and depart from the regulation under certain circumstances. There are also concerns about the broad concept of "public interest" and variable meanings of "national security". In summary, the EDPS welcomes the Regulation in strengthening the rights of individuals (especially in transparency and the right to object) and the powers of national data protection authorities, and not requiring transposition into national law. The EDPS is disappointed by the Directive for data protection in the law enforcement area, which is said to provide inadequate and inferior protection to the Regulation. The package as whole does not remedy lack of comprehensiveness of EU data protection rules. The opinion concludes with a series of concrete recommendations for the Directive, regulation and the reform process as a whole.
Assessment of the importance or significance of the document The EDPS is an independent supervisory authority protecting personal data and privacy and promoting good practice in EU institutions and bodies. It monitors the EU's processing of personal data, advises on policies and legislation that affects privacy, and cooperates with other data protection authorities. This opinion is part of that second role of policy advice. It is therefore important to the extent to which the Commission and other EU law making bodies take it into account.

2.3 UK POLICY DOCUMENTS

456. House of Commons Home Affairs Select Committee, A Surveillance Society?, Fifth Report of Session 2009-10, HC 58-I, The Stationery Office, London, 8 June 2008. 119 pages

What domain (health, transport, policing, etc.) does it address?
Personal information, public and private sector, surveillance

Target audience of the document
This document is geared towards policy-makers and other decision-makers. It is also relevant to academics and researchers in the field of surveillance and policy.

Stated purpose of the document
The document is the final report of the House of Commons, Home Affairs Committee inquiry into the growth of public and private databases and forms of surveillance directly relevant to the work of the Home Office.

"A perception of the growth of surveillance—in particular the collection, storage and use of personal information—as an increasingly important part of the Government's policy in tackling crime, managing borders and delivering public services, lay behind our decision to undertake this inquiry. We examined Home Office responsibilities—such as identity cards, the National DNA Database and CCTV—in this context."

Context of the document
Increased potential for surveillance of citizens in public space and public communication has caused increased concern, including about the danger of becoming a "surveillance society" if trust is not maintained. Commercial sector developments and advances in information technology.

In March 2007 the Home Affairs Committee launched a wide-ranging inquiry into the growth of public and private databases and those forms of surveillance directly relevant to the work of the Home Office. The document makes specific mention of the benefits and risk of increasing surveillance. It places the inquiry in the context of the HMRC child benefit data loss of October 2007, and the alleged recording of a Member of Parliament's privileged conversations at HMP Woodhill in 2005/6. At the time of writing, the National Identity Register had a basis in law and was being set up. It had not yet been cancelled, and several parts of the recommendations for the Home Office refer to the NIR (as well as ContactPoint and the NHS Care Records Service).

The document refers to the following other documents:

Surveillance Studies Network, *A Report on the Surveillance Society for the Information Commissioner*. September 2006

Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, London, March 2007. http://www.raeng.org.uk/news/publications/list/reports/dilemmas_of_privacy_and_surveillance_report.pdf

Office for National Statistics, *Focus on the Digital Age (2007 edition)*, 15 March 2007. http://www.ons.gov.uk/ons/rel/social-trends-rd/focus-on-the-digital-age/2007-edition/index.html

Cabinet Office, *Transformational Government: Enabled by Technology*, Cm 6683, November 2005. http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/141734/transgov-strategy.pdf

Tri Media by ICM Research, *Personal Information Survey*, Information Commissioner's Office, Year?.

HM Government, *Information sharing vision statement*, September 2006. http://webarchive.nationalarchives.gov.uk/+/http://www.dca.gov.uk/foi/sharing/information-sharing.pdf

Sir David Varney, *Service Transformation: a Better Service for Citizens and Businesses, a Better Deal for Taxpayers.* HM Treasury, December 2006. http://www.official-documents.gov.uk/document/other/011840489X/011840489X.pdf

Prime Minister's Strategy Unit, Cabinet Office, Building on Progress: Public Services, March 2007. http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/cabinetoffice/strategy/assets/building.pdf

Gill and Spriggs, *Assessing the impact of CCTV*, London, Home Office Research, Developments and Statistics Directorate, 2005.

Academy of Medical Sciences, *Personal data for public good: using health information in medical research*, January 2006. http://www.acmedsci.ac.uk/p48prid5.html

Home Affairs Committee, *Fourth Report of Session 2003–04, Identity Cards,* HC 130, 20 July 2004.
http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/13002.htm

Key points in the document

The document advocates government data minimisation, proper consideration of risks of excessive surveillance, provides ground rules for government and agencies to preserve trust. Government should make use of technical means to protect personal information and should conduct risk assessments before new information technology projects. The document recommends that the Home Office exercise restraint in collecting personal information and address the question of whether or not surveillance activities are proportionate to responses to varying threats. There is an explicit discussion about balancing protecting the public and individual liberty.

The document rejects the assertion that the UK is a surveillance society in that all information collection is centralised in the service of the state. However, surveillance capacity has increased to the point that the UK could be characterised as a surveillance society if trust in government's data collection and sharing intentions is not preserved.

The report welcomes the Information Commissioner's efforts to increase awareness of the increase in surveillance potential, and recommended an annual report be put before Parliament, be responded to by the government and discussed in Parliament.

The document outlines significant technological developments in surveillance (databases, profiling, data-mining, predictive technology, search engines and social networks), the motives behind business adoption of these (personalisation, digitally-supported decision making, and government procurement, competitive advantage) and of government initiatives (transformational government, common infrastructures, promoting trust). It identifies a common driver in raised expectations, and also engages with public demands for surveillance.

The document identifies a trend towards personalisation of services which requires the collecting of more information, in both the private and public services. Companies want to take up technological advances and citizens have raised expectations. Elimination of technical barriers to information sharing has significant social implications. It argues the government should be more open about its intentions in collecting personal information and curb the development of new databases.

The document engages with the concept of balancing benefits of surveillance against cumulative risks to individuals and to society. The inquiry asked contributors to reflect on their processes for balancing these risks. Arguments against benefits included achieving similar goals through less information intensive processes and the opportunity costs of surveillance measures. Risks examined include practical effects of misuse or mistakes; a black market in personal information; data loss and identity fraud; incorrect information and false matches; cumulative effects and disproportionate burdens upon the disadvantaged; impacts on privacy and individual liberty; and shifts in citizen-state relations of trust.

The document examines the strength of existing safeguards, including regulation, data protection principles, public sector responsibilities, technological safeguards (privacy enhancing technologies and digital identity management). The document welcomes technological methods, and advises government to track developments in these, but does not believe they are a panacea, and may introduce "privacy divides". The document makes the argument that where there is no choice to share information, the collecting organisation is particularly responsible for securing that information. The document also examines the case for new safeguards. The document recommends the assessment of the adequacy of the Data Protection Act, and encourages the use of Privacy Impact Assessments (to the extent that they are not bureaucratic exercises, and are carried out as part of preliminary risk assessment), as well as proposing a set of guidelines for future personal information databases.

The document argues that decision to collect information about people's activities should be taken only after an appropriate balance is struck between the potential harm, including intrusion of privacy, and intended benefit of the project. The use of personal data by the Home Office is particularly significant both in terms of clear benefits, but also potentially more dangerous risks. The document contains a fairly substantial section on the use and assessment of a range of technologies and practices, including; CCTV surveillance, the National Identity Card Scheme, the National DNA database, the relation between surveillance and terrorism, information sharing and data matching, transport databases, profiling, the Regulation of Investigatory Powers Act 2000 (RIPA).

Assessment of the importance or significance of the document
The Home Affairs Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Home Office and its associated public bodies. This report received fairly significant media coverage.

507. House of Lords Constitution Committee, Surveillance: Citizens and the State, Second Report of Session 2008-09, HL Paper 18, The Stationery Office, London, 6 February 2009. 130 pages

What domain (health, transport, policing, etc.) does it address?
The document is addressed to high level constitutional politics, but has applicability across other domains, including policing, borders, finance, health, transport etc.

Target audience of the document
The report makes recommendations to the Information Commissioner, the Office of the Surveillance Commissioner, the Intelligence Services Commissioner, and the National Identity Scheme Commissioners, to Government, to Parliament and a recommendation to all public and private sector organisations.

Stated purpose of the document
The Constitution Committee is appointed by the House of Lords in each session to examine the constitutional implications of all public bills coming before the House; and to keep under review the operation of the constitution. The Constitutional Committee decided that the constitutional impacts of developments in surveillance had not been sufficiently scrutinised. The document is the record of the Committee's inquiry into surveillance. It attempted to answer the following questions:

- Have increased surveillance and data collection by the state fundamentally altered the way it relates to its citizens?
- What forms of surveillance and data collection might be considered constitutionally proper or improper?
- Is there a line that should not be crossed? How could it be identified?
- What effect do public and private sector surveillance and data collection have on a citizen's liberty and privacy?
- How have surveillance and data collection altered the nature of citizenship in the 21st century, especially in terms of citizens' relationship with the state?
- Is the Data Protection Act 1998 sufficient to protect citizens? Is there a need for additional constitutional protection for citizens in relation to surveillance and the collection of data?

The document states that the committee followed a "constitutional approach", trying to find the constitutional principles that govern the use of surveillance in the UK.

Context of the document
In context of Information Commissioner's 2004 warning about "sleepwalking into a surveillance society", expansion of the DNA database, and other databases of personal information, and steady increase in CCTV, the 2006 Surveillance Studies Network report and Royal Academy of Engineering.

The document refers to a wider range of other documents:

The Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, March 2007.

Surveillance Studies Network, *A Report on the Surveillance Society: Full Report, for the Information Commissioner*, September 2006

Gareth Crossman, Liberty, *Overlooked: Surveillance and Personal Privacy in Modern Britain*, October 2007. http://www.liberty-human-rights.org.uk/policy/reports/overlooked-privacy-report-december-2007.pdf

Home Office and ACPO, *National CCTV Strategy*, October 2007

House of Commons Justice Committee, Protection of Private Data 1st Report (2007–08): Protection of Private Data (HC 154). January 2008.

Richard Thomas and Mark Walport, *Data Sharing Review Report (Thomas-Walport Review)*, 11 July 2008.
http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf

European Commission for Democracy Through Law (Venice commission), Opinion in video surveillance in public places by public authorities and the protection of human rights, March 2007. http://www.venice.coe.int/2007/CDL-AD(2007)014-e.asp

Home Office information charter, Current version available at:
http://www.homeoffice.gov.uk/about-us/corporate-publications-strategy/information-charter/

Council for Science and Technology, *Better use of Personal Information,* November 2005.
http://webarchive.nationalarchives.gov.uk/+/http://www2.cst.gov.uk/cst/reports/files/personal-information/report.pdf

Coleman, N., *Protecting government information: independent review of government information assurance*, June 2008.

HM Government, *Information Sharing vision statement*, September 2006.

Cabinet Office, *Data handling procedures in government: Interim progress report*, December 2007. http://www.cabinetoffice.gov.uk/sites/default/files/resources/data_handling-interim_0.pdf

Key points in the document
The introduction gives background, key events during the constitutional inquiry, and details on the constitutional approach. Privacy and restrain in use of surveillance is part of individual freedom. Individual freedom is a precondition of the constitutional framework. "Mass surveillance

has the potential to erode privacy. As privacy is an essential pre-requisite to the exercise of individual freedom, its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country". The inquiry is less concerned with private sector surveillance but notes that activity there is widespread and often leading developments.

Chapter two gives an overview of surveillance and data collection. This includes key definitions of two broad types of surveillance (mass surveillance and targeted surveillance), personal data, data sharing, matching, mining and profiling, privacy, and data protection, as well as the characteristics of contemporary surveillance, including the role of technology, the impetus behind surveillance, large scale and routine practices, the availability of technology, the global flow of personal data, and public and private sector uses. Increasing data sharing over time increases the difficulty of tracing personal data processing and maintaining accountability and responsibility. This has implications for the current regulatory regime. The document recommends that before introducing any new surveillance measure the Government should publish its likely effect on public trust and compliance. Potentially in conjunction with the Information Commissioner or independent review body.

Chapter three looks at the advantages (for law enforcement, public safety, and service provisions) and disadvantages of surveillance and the use of personal data. The disadvantages include the threat to privacy and the social relationship, the reduction of trust in the state, discrimination and impacts upon personal security. Trust in the state is an essential prerequisite for compliance with the law, undermining trust can cause resistance and lead to creation of an antagonistic relationship between individual and state. Evidence received on the advantages of data collecting and sharing received from central government via the Ministry of Justice was policy aspirations with little comment on outcomes.

Chapters four and five examine legal regulation and safeguards, and regulators respectively, including the sources of regulation and how effective they are at controlling surveillance activity. Chapter six engages with privacy protection in government and the limits of legal regulation. The document argues that Government should not confine itself to questions of legal authorisation and compliance when seeking to improve surveillance, as law alone cannot prevent abuse of surveillance powers, and that measures may be legal but also unsuitable or damaging to public trust.

Chapter seven looks at the role of Parliament in relation to primary and secondary legislation and Parliamentary scrutiny. Constitutional requirement that ministers are accountable to Parliament suggests that surveillance or data collection activities undertaken under ministerial authority should be open to Parliamentary scrutiny. The report argues that privacy and the application of executive and legislative restraint to the use of surveillance and data collection powers are necessary conditions for the exercise of individual freedom and liberty. Privacy and executive restraint should be taken into account at all times by all parts of government. The document recommends that statutes involving data processing and surveillance should be subject to post-legislative scrutiny. The document highlights the importance of necessity and proportionality, and expresses concern about the overuse of secondary legislation.

Chapter eight is on the role of the citizen, including the exercise of autonomous consent, public opinion, beliefs and attitudes, and citizen engagement in policy decisions affecting privacy. It argues that growing expectations that individuals are responsible for their own data creates a new and increasingly onerous set of personal obligations. The report also suggests that research

in this area is not particularly reliable and often partisan. Chapter nine provides the committee's 43 recommendations, including specific recommendations on the National DNA Database, CCTV, and for legislation and regulation.
Assessment of the importance or significance of the document Highly significant for privacy and surveillance within the UK context given the authorship.

523. Joint Committee on Human Rights, *Legislative Scrutiny: Protection of Freedoms Bill*, Eighteenth Report of Session 2010-12, HL Paper 195/ HC 1490, The Stationery Office Limited, London, 07 October 2011. 148 pages.

What domain (health, transport, policing, etc.) does it address?
The right to private life, specifically in relation to the use of:

- Biometrics & DNA for crime prevention (in particular issues re social stigma, retention & processing)
    - With regards to children – the storage of biometric data for crime prevention, parental consent
- Surveillance - CCTV (compliance with the Data Protection Act 1998) – mainly in/by the private sector
- Powers of entry into a persons residence

Security (the use of biometric data and DNA in crime prevention and fighting)

Target audience of the document
British Parliament, British public

Stated purpose of the document
This report by a joint Committee on Human Rights scrutinised the Protection of Freedoms Bill, and exists to bring light to concerns about certain measures in the bill. Specifically, it focuses on measures which may not be compliant with the UK's human rights obligations, or sections which risk infringement of individual rights.

This report directly relates to the Protection of Freedoms Bill.
It makes specific references to the National DNA Database.

Context of the document
The Protection of Freedoms Bill (UK) and the National DNA database.
The document was written to evaluate the balance (or lack thereof) between security and personal privacy for measures proposed in the Bill.

Other documents referred to:

- Public Order Act 1986
- Protection of Freedoms Bill (2011, 11 February)
- European Convention on Human Rights
- Crime and Security Act 2010
- UN Convention on the Rights of the Child (Articles 40, 16, 3)
- UK Home Office, *The Human Rights Memorandum*
- Terrorism Act 2000
- Immigration Act 1971
- Immigration and Asylum Act 1999
- Counter-Terrorism Act 2008
- International Criminal Court Act 2001
- Terrorism Prevention and Investigation Measures Bill
- Precedents:
    - Gillan and Quinton v UK (2010)
    - Marper v UK (2008)

- Gillick v West Norfolk and Wisbech Area Health Authority (1986)
- Police and Criminal Evidence Act 1984
- Data Protection Act 1998
- Home Office, Code of Practice relating to Surveillance Cameras, March 2011.
- Tribunals, Courts and Enforcement Act 2007
- Armed Forces Bill
- Serious Organised Crime and Police Act 2005
- Police Act 1997
- Freedom of Information Act 2000
- Public Order Act 1986
- The "Scottish Model" (for retention of DNA)[13]

Key points in the document

The authors overall recognise that the Protection of Freedoms Bill "*enhances legal protections for human rights and civil liberties*" (p. 7), but take issue with a few specific aspects. These are mainly:

Retention and processing of biometric materials. One of the main concerns of the authors is that there seems to be broad conditions that allow police to authorise the retention of biometric information indefinitely, for the purposes of national security. The authors argue that there is no significant justification provided for the necessity of police to have this power. They also posit that there should be provision for review when biometric data is automatically retained, to safeguard against arbitrary and disproportionate retention.

The anonymisation of DNA profiles is also mentioned as a concern. The authors interpret the Bill to allow for the indefinite retention of DNA profiles, which will be anonymised after a period of time. However, they note that the UK Government admitted there was difficulty with complete anonymisation. The authors conclude that there is a risk to the right to a private life, if DNA profiles are unable to become truly anonymous after a period of time.

The authors also note that there should be accurate statistical information provided about the operation of the National DNA database, especially when a match assists in the identification of an offender. The reason given is so that the committee could then assess if the privacy relinquished for the National DNA database was proportionate to the amount of crime it succeeded in preventing and/or convicting.

With regards to children, the authors state that the bill should be clearer when the need for parental consent is forfeited, as the current definition is too broad; *"[...]it is otherwise not reasonably practicable to obtain the consent of the parent."*(p. 40).

CCTV. The authors are positive about the introduction of a 'Code of Practice relating to Surveillance Cameras', but they believe that limiting the application of the code to the public sector will restrict the impact of the code. As such, they recommend that the code should "*include information on the use of CCTV technology in schools, residential care homes and healthcare settings, where risks to private lives of pupils, residents and patients may be heightened"* (p. 45).

Powers of entry (residential). The key issue of the authors is the clause which basically al-

[13] http://www.scotland.gov.uk/Publications/2009/02/24104443/5

lows the extension of powers of entry by Ministers, when they "consider enforcement action is appropriate" (p. 47).

As a background to the Protection of Freedoms Bill, the Home Office published a list of around 1,200 statutory powers that were associated with powers of entry.[14] The consequences outlined include the possibility to allow the use of force, as well as the opportunity to create new powers of entry or remove existing restrictions. It is therefore noted that in its existing form, the Bill has potential to allow the invasion of personal privacy.

Assessment of the importance or significance of the document
The recommendations were debated in parliament and on May 1, 2012 the Protection of Freedoms Act came into force.[15] Overall this document is significant and has been used in the foundations of the Protection of Freedoms Act.

(Evaluation on the basis of Google search hits, English language results)
A Google search indicates that this document has been published on many different websites, with over 35,000 results being returned. Most of the results were mirrors to the document, or links to online stores (all over the world, not just in the UK) to buy the document. A few blogs discussing the document also came up.

A Google Scholar search returns nothing except one link to the document in the Google Books store. This indicates that the document was not published in any journals or referenced in other books.

This document was referred to in a report by the Select Committee on the Constitution of the House of Lords, where it is agreed upon that clause 41 would not prevent the creation by ministers of more extensive powers of entry.

[14] This ranged from the Terrorism Act (2000) to the Hypnotism Act (1952). A full list can be found here: http://www.homeoffice.gov.uk/publications/about-us/legislation/powers-entry/
[15] http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

546. Ministry of Defence, *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security*, The Stationary Office, London, February 2012. 63 pages.

What domain (health, transport, policing, etc.) does it address?
Defence and security technology procurement and industry

Target audience of the document
The official audience for this White Paper is the UK Parliament, but is also directed at the UK Defence and security industry and responds to issues raised during the preceding consultation process. The document is high level policy until the next review in 2015 and therefore relevant for MOD staff involved in procurement.

Stated purpose of the document
The White Paper replaces the previous Defence Industrial Strategy (2005). It is a response to a need to transform the Ministry of Defence and UK armed forces, take account of defence and security overlaps, the defence over-commitment of the previous government, and instigate a new approach to buying and supporting defence and security equipment. This includes providing industry with transparency regarding future MOD plans.

Context of the document
The document identifies its context as a dangerous and uncertain world with continued threats from Al Qaida and groups in Northern Ireland and with constrained government budgets. At the same time, law enforcement is seen as being better equipped than ever, the UK being the world's second largest defence exporter, and the fifth in Security. The UK domestic market for security products is states as £1.8 billion p.a.

The document details the Ministry of Defence's technology and equipment procurement strategy and should be contextualised against the background of the Strategic Defence Review and the most recent National Security Strategy.

The document refers to the following other documents:
HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (Cm 7952) October 2010.

HM Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security* Review (Cm 7948), October 2010.

British Army, *Transforming the British Army: Modernising to face an unpredictable future,* July 2012. www.army.mod.uk/documents/general/Army2020_brochure.pdf

Lord Levene of Portsoken, *Defence Reform: An independent report into the structure and management of the Ministry of Defence*, June 2011. http://www.mod.uk/NR/rdonlyres/B4BA14C0-0F2E-4B92-BCC7-8ABFCFE7E000/0/defence_reform_report_struct_mgt_mod_27june2011.pdf

Lord Currie of Marlybone, *Review of Single Source Pricing Regulations: An independent report into the single source pricing regulations used by the Ministry of Defence*, October 2011. http://www.mod.uk/NR/rdonlyres/894BD700-CE90-43AD-AD52-

A94E681AC86B/0/review_single_source_pricing_regs.pdf

Secretary of State for Defence, Defence Industrial Strategy: Defence White Paper, December 2005.
http://www.mod.uk/nr/rdonlyres/f530ed6c-f80c-4f24-8438-0b587cc4bf4d/0/def_industrial_strategy_wp_cm6697.pdf

Secretary of State for the Home Department, *CONTEST: The United Kingdom's Strategy for Countering Terrorism* (Cm 8123), July 2011. http://www.homeoffice.gov.uk/publications/counter-terrorism/counter-terrorism-strategy/strategy-contest?view=Binary

Cabinet Office*, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, November 2011. www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

It also refers to two forthcoming documents, Bernard Gray's Material Strategy and the MOD 10 year equipment plan.

Key points in the document

The key point of the document is that the Ministry of Defence aims to move to a model of technology and service procurement based upon open competition in a potentially global market. But still protecting a UK technological advantage and guaranteeing high quality outcomes. The government intends to support industry to allow them to compete in that marketplace, whilst attempting to purchase "off the shelf" technology as often as possible. The document notes the significant impact of defence and security procurement upon industry and the economy and identifies a vital government role in supporting this (including Ministerial support for exports, increased potential for SME involvement, and creating the conditions for greater private sector investment). The document states that the MOD wants to ensure the UK continues to be a unique environment for defence and security industry. It argues that the best way to counter the easy availability of high technology weapons to potential adversaries is to invest in defence technology and science. The document also mentions the importance of "being an intelligent customer" and maintaining credibility with allies.

"We will ensure that our Armed Forces and the wider national security community continue to get the equipment and support they require at an affordable cost and at value-for-money to the taxpayer. This will encourage a vibrant UK-based industry that is able to compete against the best in the world to meet not only the UK's needs, but is also able to win a significant share of the world market."

"The sole objective of defence and security procurement, financed through the defence and security budgets, is: To provide our Armed Forces and national security agencies with the best capabilities we can afford, to enable them to protect the UK's security and to advance the UK's interests, both now and in the long term; and in doing so, to obtain the best possible value-for-money." (page 10)

Assessment of the importance or significance of the document

The document will be significant for security and defence technology development and marketing in the UK, and for UK-based defence and security companies operating abroad. It leaves a large amount of room for market considerations as well as particular requirements

capture processes to determine the exact details of defence and security technology procurement.

There is no mention of privacy within this document. There are discussions of the potential trade-offs and balances between best value for money and open, transparent, competitive procurement processes and the requirements of national security (operational advantage and freedom of action).

560. Surveillance Studies Network, *A Report on the Surveillance Society For the Information Commissioner*, Information Commissioner's Office, September 2006. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf 102 pages.

What domain (health, transport, policing, etc.) does it address?
This document covers several domains:

- The context of the surveillance society
  - Consequences on society (social sorting, autonomy, choice & consent).
- Surveillance technologies (telecommunications, video, database, biometrics)
  - Location tracking & tagging, (GPS/RFID/CCTV/UK National IDs)
  - Operation and implementation of these technologies (medical records, border control, crime fighting)

Target audience of the document
The UK Information Commissioner, the public at large.

Stated purpose of the document
This document exists to inform about the social consequences of increased surveillance. It includes a section designed to stimulate public discussion and debate. It also calls for new privacy regulation for current and emerging surveillance technologies. It does not follow on from other policies or official documents.

Context of the document
This document was requested in response to the increased surveillance and identification systems introduced since 9/11 and as part of the subsequent 'war on terror'. It also relates to the proposed *National ID* policy. It does not build on existing legislation but rather evaluates the current technological and legal capabilities for surveillance.

Other documents referred to:

- Beck, U. (1992). The Risk Society, Newbury Park, CA: Sage
- Barbaro, A. & Zeller, T. (2006, August 9). 'A face is exposed for AOL searcher no. 4417749', New York Times.
- Orwell, G. (1949). 1984. UK: Secker and Warburg
- Marx, G.T. (1985). 'The surveillance society: the threat of 1984-style techniques'. The Futurist.
- Gandy, O. (1989). 'The surveillance society: information technology and bureaucratic social control', Journal of Communication.
- Kafka, F. (1914). The Trial.
- Fair Information Principles
- Drugs Act (2005)
- Cross Regional Information Sharing Project
- National ANPR Strategy
- US Patriot Act
- BBC News. (2002, December 20). Phone firms 'flooded' by crime checks.
- PETS Scheme (2000, February 28)
- Weiner, M. (1991) 'The computer for the 21st century', Scientific American
- Huber, P.W. & Mills, M.P. (2002). 'How technology will defeat terrorism', City Journal 12(1)

- The Nominal Index
- New Labour's modernisation agenda
- The Social Security Administration (Fraud) Act 1997
- National Fraud Initiative
- Home Office consultation paper
- Suspicious Activity Reports
- Cabinet Office (2006) Ministerial Committee on Data Sharing (MISC 31)
- The Climbié Inquiry
- National Identity Register
- Project Semaphore
- US Strategic Border Initiative
- Home Detention Curfew Scheme
- Office of the Information Commissioner (2002). Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998. Wilmslow: Office of the Information Commissioner.
- House of Commons Science and Technology Committee (2006) Sixth Report, HC 1032, London: The Stationary Office.
- Identity Cards Act 2006
- UK Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Information sharing index
- Chief Secretary to the Treasury (2003) Every Child Matters (Cm 5860), London: The Stationary Office.
- Children Act 2004
- Intelligence Services Act 1994
- Longitudinal Labour Force File (Canada)
- Cabinet Office Performance and Innovation Unit (PIU) (2002) Privacy and Data-Sharing: The Way Forward for Public Services. London: Cabinet Office.
- European Data Protection Directive 95/46/EC
- Telecommunications Directive (97/66/EC)
- European Convention on Human Rights
- OECD (1981) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD.
- Council of Europe (1981) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Strasbourg: Council of Europe.
- The 'Safe Harbor' Agreement
- Greenleaf, G. (2005) 'APEC's Privacy Framework: a new low standard'. Privacy Law & Policy Reporter 11: 121-4.
- Article 29 Working Party
- Stewart, B. (1996) 'Privacy impact assessments'. Privacy Law & Policy Reporter 3 (4): 61-4.
- Raab, C. (2006) 'The safe online consumer: Addressing issues and problems', Paper presented at the 56th Annual Conference of the International Communication Association, Dresden, 19-23 June

Non-textual references

- Big Brother (TV show)

- Minority Report (2002, Film)
- The Net (1995, Film)
- The Conversation (1974, Film)
- Enemy of the State (1998, Film)

Key points in the document

The document covers consequences of increased surveillance in these areas: medical records, crime and terrorism prevention and border control. The authors state that the security and safety of individuals has been the paramount reason for having many surveillance systems put in place, especially relating to the 'war on terror'. It also addresses the lack of mainstream knowledge about how personal databases are used; triggered by "dataveillence".[16] Surveillance implies mistrust and the overarching consequence is a limitation on freedoms.

The authors are not convinced that the current regulations for surveillance are capable of restricting the amount of surveillance on individuals. Privacy protection measures are seen as the first line of defense in surveillance regulation, but this document only touches upon that, with more focus on the social outcomes. Lack of choice is a main point of discussion, as the general consensus is 'you only care if you have something to hide', and 'better safe than sorry'.

Social sorting (distinctions of race, class, gender, geography, citizenship, credit ratings and so forth), a direct result of surveillance, can have unjust effects on life chances. Additionally, digitised bureaucracy and increasing reliance on digital analysis of data is thought to lead to dehumanisation and increasing false negatives, which also impacts life chances.

The authors seem to have written this document with the intention to warn about the rarely discussed social issues of a surveillance society. They are not taking the stance that surveillance in itself is a negative thing, but acknowledge that it has the potential to be. Global data sharing between private and public organisations seems to be the biggest concern of the authors, as this can lead to false negatives[17] and profiling.

The recommendations in the document are presented with increasing time-pressure to implement surveillance regulation, due to the difficulty of removing a practice that is already in place. Current international guidelines and laws are evaluated, with emphasis on the necessity to update them. Self-regulation for individuals and organisations appears to be the most favoured solution, through methods like Privacy Impact Assessment.

The persistence and increasing sophistication of surveillance technologies, blurring boundaries between the private and public sectors, as well as government policies promoting information sharing as a solution to social problems, has led to the authors' prediction of privacy-free societies in the future.

Assessment of the importance or significance of the document

The document had great and broad social impact and has paved the way for further research, public debate and parliamentary debate into surveillance and its impact on society, politics, the economy, media and legislation.

[16] "Dataveillance" monitors people's activities or communications (especially transactions, exchanges, statuses, accounts) in automated ways, using information technologies. (p. 4)

[17] False negatives refer to a result that appears negative when it should not.

(Evaluation on the basis of Google search hits, English language results)

A Google search shows that this document is widely disseminated through University websites and other learning institutions. It has also been reported on by major news outlets, such as the BBC and The Guardian. Google Scholar search results display that this document has also been referred to in a number of journals for a variety of topics, from 'Facebook as a political weapon', to 'A Synthetic theory of law and technology'.

Following a link from a news website, I found that the report was presented at the 28th International Data Protection and Privacy Commissioners' Conference (London, 2006), which was hosted by the Information Commissioner's Office.

A search of the British Parliament website shows that some issues raised in this report have been examined further by the following UK bodies:

- Lord Justice Leveson's Inquiry into the Culture, Practice and Ethics of the press; the House of Commons Culture, Media and Sport Committee's inquiries into Phone Hacking and Media Plurality;
- The Parliamentary Joint Committee on Privacy and Injunctions' inquiry into privacy, anonymised injunctions and super-injunctions;
- The Parliamentary Joint Committee's report on the Draft Defamation Bill
- The report by Dame Elizabeth Filkin on the relationship between the Metropolitan Police Service and the media (January 2012).

2.4 NETHERLANDS POLICY DOCUMENTS

594. Eerste Kamer, Evaluatie Wet bescherming persoonsgegevens; Verslag van een expertmeeting inzake de rol van de overheid bij digitale dataverwerking [Evaluation of the Data Protection Law – notes of the expert meeting organized by the Upper Chamber of Parliament with chair Article 29, EDPS, etc.], The Hague, 22 March 2011.

What domain (health, transport, policing, etc.) does it address? Personal data protection and data processing in the (semi) public sectors
Target audience of the document The Dutch Senate/The Upper Chamber of Parliament [Eerste Kamer]
Stated purpose of the document To evaluate the Dutch Data Protection Law. The document minutes the meeting of members of the Senate with five experts (including the EDPS and the chairman of the Article 29 Working Party) about the role of and the related problems for the Dutch (semi)public sector in processing, exchanging and protecting personal data of and about Dutch citizens. Besides evaluating the Dutch Data Protection Law, the discussion also touched on current data protection challenges as well as future developments.
Context of the document In the years preceding the meeting, the Dutch Data Protection Law had often been the subject of debate, sometimes in relation to the many developments in the area of security. That was also reflected in the topics addressed during the meeting recorded in this report. More concretely, the meeting examined the implications of the report by the Committee Brouwer-Korf "Gewoon doen: beschermen van veiligheid en persoonlijke levensfeer" [Just do it: Protecting security and individual privacy] for privacy and data protection. The main 'documents' mentioned in the minutes: - the Dutch Data Protection Law and - the Committee Brouwer-Korf report "Gewoon doen: beschermen van veiligheid en persoonlijke levensfeer" [Just do it: Protecting security and individual privacy] - A report by the Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid, WRR) that still had to be published at the time this meeting took place. The report lists more than a dozen references to (research) reports that were published by the organisations with which the experts in this meeting were affiliated. Some of these studies were commissioned by government organisations, others were independent (e.g., by universities).
Key points in the document The report covers presentations given by the five experts, who reflect on and evaluate the research and knowledge their respective organisations had at the time concerning the privacy-security debate. Geert Munnichs from the Rathenau Institute (Research and debate on science and technology): presented the conclusions of a research into six digital data systems with a focus on en-

cryption, centralised and decentralised storage, inspection rights and risks. The main findings were: (1) security/protection of data is a recurring issue (as are cost considerations); (2) incorrect entries in registrations are a concern (affects the legal position of citizens); digitalisation makes citizens more dependent and vulnerable; (3) appropriateness of databases comes into question (how effective are they really? Are they used for the goal they were originally designed for?). The same research formulated a number of recommendations, among them: (1) implement a variety of digital measures to protect data; (2) strengthen the position of citizens; (3) facilitate and improve ways to inspect and correct data; (4) keep it simple.

Thomas Wijsman from the Court of Audit (supervisory body for government's public spending and policymaking): presented three main recurring issues. (1) insufficient control over authorisation (who is allowed to work with which data?); (2) inadequate division of functions of individuals who work with data at different phases; (3) the protection of data. Main conclusions: (1) solid information provision is crucial to the functioning and performance of the government; (2) IT projects by the government are, generally, too ambitious and complex, and as a result are delivered too late and are too expensive; (3) technology is overrated; it is though that IT can solve, in a simple way, very complex problems.

Jacob Kohnstamm, chairman of the Dutch Data Protection Authority (College bescherming persoonsgegevens, CBP) and of the Article 29 Working Party: made a number of general points, without reference to concrete research. He considered two main problems concerning citizens' rights: (1) damage and harm are in most cases not material but immaterial (emotional); (2) the scope/magnitude of any damage re individual data, spread over thousands of databases, is incalculable. Conclusions: in future laws, privacy by design and privacy impact assessments should be central/required; privacy should be a priority at the earliest stages of new projects. And: the power/authority of supervising authorities should be increased, for example by giving the right to fine organisations when security/privacy is breached.

Peter Hustinx (EDPS): most points made were in line with speaker 3. Privacy and protection of data have never been more prominently on the political agenda than they are today. One of the most significant moments in this respect is marked by the Lisbon Treaty (2009), which recognises also the right to the protection of personal data, besides the right to privacy. At EU level, there is growing awareness that protection/security should not always prevail over privacy/protection of personal data. Further, it seems that the notion of what the 'private sphere' is, is expanding to the area of public spaces (surveillance cameras) and working environments. Overall: many things concerning privacy and security are already taken care of. However, it is important to focus on the effectiveness of safeguarding/guaranteeing existent laws/policies/regulations.

Corien Prins, chairperson of the Dutch Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid): reflected on the responsibility of the government regarding the impact of IT on the relationship between citizens and their government. Main issues addressed by this speaker: (1) the dilemma of how the government should assist its citizens in managing their personal data included in a myriad of databases; With which tools are they provided at the moment? (2) the need to think about the 'quality' or 'classification' of data. What type of data is the object of discussion, and should different types be handled differently? For example, there should be distinctions between fragments of information, profiles and personal data.

The expert presentations were followed by a round table discussion with the members of the

Dutch Senate. Additionally, best practices in other countries (US, Canada, UK), were discussed as well as the possibility of a general IT government/public authority and the need for strict personal data use limitation.
Assessment of the importance or significance of the document The report covers the proceedings of an expert meeting intended to inform members of the Dutch Upper Chamber of Parliament about current issues concerning privacy and security.in view of the announced changes in the Dutch Data Protection Law. A Google search yielded primarily results from within the government domain.

598. Parliament of the Netherlands, *Bestrijding internationaal terrorisme; Verslag algemeen overleg op 17 oktober 2001, over terrorismebestrijding en veiligheid [Fighting international terrorism; report of a general meeting about fighting terrorism and security]*, Tweede Kamer, The Hague, 1 November 2001. 33 pages.

What domain (health, transport, policing, etc.) does it address?

- Anti terrorism, security

Various topics addressed:

- Fighting international terrorism
- Security
- Airport security
- Bioterrorism
- Exchange of information between Europol and national police
- Biometric identification
- Security gates
- Privacy regulations

Target audience of the document

Dutch Parliament

Stated purpose of the document

Minutes of a meeting of several Parliamentary commissions (Justice, Internal Affairs, Defence and Finance) with the Dutch Prime Minister, the Minister of Internal Affairs, the Minister of Justice and the Minister of Finance about fighting terrorism and security.

Context of the document

The discussion was prompted by the terrorist attacks on September the 11th 2001 in the US and took place about a month after the attacks.

Other relevant documents referred to: none.

Key points in the document

- Effective means to fight international terrorism
- The need for a generally agreed upon definition of terrorism.

- The exchange of information between police and internal security agencies. The legality and legitimacy of such exchanges of information were questioned, as was the exceptional status granted to requests for exchanges of information between law enforcement agencies.

- Security measures at airports, border control. Questions were asked about the rules that should apply for better border control. It was stressed that cooperation between international airports should be improved, so that security measures are well attuned.

- The exchange of information as *the* way to prevent terrorist attacks, also internationally. Participants to the debate deemed such exchanges at the time as inefficient and incorrect and in need of improvement.

- Freedom of the individual vs. national security. The Dutch junior minister for Internal Affairs stated in the European Council on behalf of the Dutch government that EU privacy regulations needed to be adapted in the interest of improved national security.

- Concerns about security measures at Schiphol Airport. Concerns were expressed about a then recent security system which didn't work correctly. Demand for increased security measures at the airport, including comprehensive rather than random checks of passengers and their baggage.

- The substantive role of the army in the protection against terrorism.

- Proportionality and effectiveness of anti-terrorism measures. Some participants expressed the view that such measures would need to be weighed against the fundaments of the legal system, such as the right to privacy.

- Mandatory (biometric) identification of citizens and related privacy aspects that should be considered.

- More safety/security as a potential threat to privacy. Opinions were expressed about such a threat in relation to the use of new technologies for example in tracing suspicious money flows.

- The consequences of terrorist attacks for privacy and the need to redefine the relation between privacy and security in the light of such attacks.

- The limitations imposed by privacy regulations. The need to explore and inform Parliament 'in how far privacy regulations are limiting for the tracing and persecution of terrorist activities'

Assessment of the importance or significance of the document
(Evaluation on the basis of Google search hits, English language results)
First in a long series of similar documents/debates on this topic. Relative low importance of the document, but the starting point for the on-going debate on special measures necessary in the fight against terrorism.

A Google search returned few hits, mainly mirrors of the document on various sites of the Dutch government.

644. Raad voor het openbaar bestuur (Rob), *Rob-advies Veiligheid en vertrouwen [Advice to Parliament re security & trust]*, The Hague, November 2010.
http://www.rob-rfv.nl/documenten/migratie/boekje_advies_veiligheid_en_vertrouwen.pdf
86 pages.

What domain (health, transport, policing, etc.) does it address?
Social safety/security

Target audience of the document
The Dutch Government and Dutch public authorities (the report is written by an advisory council)

Stated purpose of the document
There is a growing realisation that there is a waning trust in the Dutch government by its citizens. The report is explicitly meant as an advice to the government about the interplay between trust and safety in order to improve the organisation and functioning of the Dutch government in this field. Ultimately, this should lead to more trust of citizens in governing authorities.

The document seems to loosely follow from an earlier report, Vertrouwen op democratie [Trust in democracy] by the same organisation, which concluded that the organisation and functioning of the Dutch government is largely vertically oriented, whereas citizens are mainly involved into horizontal networks.

Context of the document
See also previous section. The document takes into account the current fast changes in society to which the government ought to respond in terms of organisation, facilitation, policy making, etc.

Key points in the document
The advice takes into account a number of issues, among which privacy and security. Overall, it gives recommendations as to what the required conditions are that the government needs to create in order the improve citizens' trust.

Regarding privacy and safety/security, the authors of the report remark the following:

- Privacy and safety/security are at odds with each other. Therefore, often it is a question of hierarchy: Which of the two prevails? However: both are important and interests should be balanced.
- The EU can contribute to promoting trust by stressing the importance of protecting basic rights, collaboration with Member States and sound information provision. At the same time, trust can be at risk as a result of the way in which the EU is portrayed by a number of political actors.
- Government actors need to have the same, good understanding of citizens' concerns about privacy, safety and security in order to improve citizens' trust.

Assessment of the importance or significance of the document
Significance or importance does not seem have been very substantial. The report is a general advice as to what the Dutch government should be considering and which societal and political debates should be initiated in the coming years.

A Google search returned a number of hits, most of them links to sites covering the part of the report detailing perceptions of safety/security.

658. Commissie Veiligheid en persoonlijke levenssfeer ("de commissie Brouwer-Korf"), *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer [Personal data treatment for increased security]* – advice to the Ministry of Justice, Ministry of the Interior, January 2009.

102 pages

What domain (health, transport, policing, etc.) does it address?
- Security
- Handling of personal data by (security) professionals

Topics included:
- Security
- Privacy (practice)
- Governmental policy
- Technological developments
- Societal developments

Target audience of the document
Dutch Ministers (main target audience), Dutch Parliament

Stated purpose of the document
The Ministry of Justice and the Ministry of Internal Affairs asked the commission on 'Security and private life' to advise about possible changes in regulation, operating procedures and protocols concerning the handling of personal data to increase the security of persons.

Provide advice on how security measures adopted in the context of the fight against terrorism could impact citizens' privacy.

Context of the document
The policy programme 'Samen werken, samen leven' [Work together, live together], the Dutch government programme, which set as priority a decrease in aggression, violence and criminality whilst taking into account all relevant privacy and data protection issuses.
Large investments by the Dutch government as part of the new policies to increase the security of citizens.

Increased use of personal data by government agencies as part of policies aimed at increasing security. The increasing number of professionals in the area of security handling these data and related risks.

Other documents referred to:
- Article 10 of the Dutch Constitution. Order by government to enact a law to protect private life and personal data
- Article 8 of the Dutch Constitution. Wet Bescherming Persoonsgegevens [Protection of personal data]
- Bosma (2007). Report 'Data voor daadkracht' [Data for vigour]
- Commission Franken (2000). Report 'Grondrechten in het digitale tijdperk' [Rights in the digital age]
- Zwenne, G-J, Duthler, A.W. et al (2007). Evaluation report 'Eerste fase evaluatie Wet bescherming persoonsgegevens' [First stage of the evaluation of the data protection

law]
- Roepman, J.R. (2008). *'Revocable privacy'* in: Privacy & Informatie, 3, p.114-118

Key points in the document

- Information exchange. The commission stated that 'everyone' (the Dutch government and public) agreed that certain information needed to be exchanged for crime prevention, but that such information exchanges should be limited

- Security vs. Privacy. The commission stated that citizens demanded security, but they didn't want government to interfere with their private lives.

- Large government investments in new preventive policy which enabled much more intrusions in citizens' private lives

- Relation between new technologies and privacy and security. New technologies like RFID offered opportunities for increasing safety, but also posed threats to privacy.

- The need for a complex assessment of the social impact of security measures in the context of new technological developments, increased international complexities and interdependencies, the fight agains international terrorism and organised serious crime

- Privacy as policy area. The commission advised that privacy be included as a policy domain. To this end a number of issues would need to be clarified: How to engage stakeholders? What safeguarding mechanisms to put in place? How to integrate privacy in technical systems (privacy by design)? What to stimulate compliance?

- Handling of personal data in practice.

- Redefining the role and responsibilities of the Dutch data protection authority. The commission underlined the need for an independent data protection supervisor focusing on compliance with data protection rules and regulations.

Assessment of the importance or significance of the document

A very significant report – it effected changes in the organisation of government departments, the responsibilities attributed to the Dutch Data Protection Supervisor, legislation, public debate on issues of security and privacy.

A Google search on the title of the report rendered 1.870 results. The hits consisted of links to mirrors of the report, official responses to the report, and other (critical) views on the findings.

A search on Google Scholar returned 4 results.

670. Adviescommissie Informatiestromen Veiligheid, Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse [Data decisiveness. Data safety: observations and analysis], report commissioned by the Ministry of the Interior, Ministry of Defense, Ministry of Justice, The Hague, April 2007.

What domain (health, transport, policing, etc.) does it address?
Public security, with primary focus on fighting crime, fighting terrorism and crisis management.

Target audience of the document
The Dutch government, and specifically the Ministries of the Interior, Defence and Justice. Affairs.

Stated purpose of the document
It is noted that the number of information streams and databases, from both the public and private sectors, are increasing, and that these streams and databases are increasingly being used by a wide variety of actors, including criminal investigation departments. The report aims to encourage decisive action to ensure security, and to provide the necessary information for the political debate. At the time when the report was drafted, there was no systematic approach as to how investigation services should retrieve and use information from the various sources at their disposal.

Context of the document
The report was commissioned because of a number of developments including: (1) the growing number of automated databases; (2) missing, incorrect and unavailable information at the time when terrorist attacks (mainly 9/11) took place; (3) increasing 'intelligence-led policing'. With regard to privacy, it is argued that 'information privacy' is now at stake (e.g. because governments can breach privacy by storing, connecting and mining personal data) as well as 'communications privacy' (such as by means of wiretapping, storing information about telephone and Internet use). Thus, it should be of great priority to maintain a justified balance between the privacy incursion of innocent citizens and suspected/guilty citizens'.

The report contains more than a 100 references to a variety of sources. The main sources are domestic and foreign government reports and documents as well as scientific/popular reports. A selection of the first sources that are cited:

- The letter from the Ministry of Defence and Ministry of Justice in which this research was commissioned
- Projectgroep Organisatie Structuren (1977). Politie in Verandering. 's-Gravenhage, Staatsuitgeverij (report about how the Dutch police should function)
- Raad van Hoofdcommissarissen, Projectgroep Visie op de Politiefunctie, Politie in Ontwikkeling, Den Haag, 2005, pp. 92-93 (similar report, published later)
- Digitale opsporing komt capaciteit te kort, in: Automatisering Gids, 2 februari 2007 (magazine article)
- John F. Gantz, e.a., The Expanding Digital Universe, A Forecast of Worldwide Information Growth Through 2010, uitgave van IDC, maart 2007, p. 7
- National Commission on Terrorist Attacks Upon the United States, the 9/11 commission report, Washington, July 2004, p. 353
- Commission on the Roles and Capabilities of the United States Intelligence Community, Preparing for the twenty-first century An appraisal of U.S. intelligence, Washington, March 1996, p. 43

- Wijk, R. de en C. Relk, Doelwit Europa, complotten en aanslagen van moslimextremisten, Amsterdam 2006
- Inspectie Openbare Orde en Veiligheid (IOOV), Landelijke coördinatie en uitwisseling van politie-informatie, een evaluatie van het project landelijke informatiecoördinatie DNP, Den Haag, 2004, p. 15

Key points in the document

- The fundamental change is the explosive data and database growth and an increase in the possibilities to use those data. This has several implications for the relationship privacy-security.
- Not enough government attention to the significance of the data to the security domain, including the possible consequences of these data and the use of new data analysis techniques.
- The risk that government will, in their fight against terrorism, allow for too much (discretionary) power to LEAs and intelligence services, so that, as a result, the balance between privacy and security would be at risk.
- Data retrieval systems relying on external databases do not always meet the necessary criteria in terms of form requirements, societal controls, effectiveness and appropriateness.
- There is no complete or general overview of rules and regulations concerning the use of data from external databases and there seems to be little or no policy and regulation coherence in general.

Assessment of the importance or significance of the document

Some indication of the relevance of this document:

- The Dutch Ministry of the Interior who commissioned the report released a statement in which it expressed its disagreement with the main conclusions of the report
- A regular Google search shows that many news organisations and online news sites discussed the results and implications of the report.

Google Scholar yields few hits.

2.5 FRANCE POLICY DOCUMENTS

696. Senat, Proposition de loi, visant à mieux garantir le droit à la vie privée à l'heure du numérique, [Proposed legislation to better protect the right to privacy in the digital age -- unofficial translation], 23 mars 2010, 18 pages

What domain (health, transport, policing, etc.) does it address? Privacy, Education, Security
Target audience of the document National Assembly of France, French parliament, French government
Stated purpose of the document The purpose of this proposed legislation is to meet the new challenges of the digital era. The document proposes to enhance privacy by amending Articles 2 to 12 of the French Data Protection Act. The proposed law wants to better ensure the right to privacy in the digital age by, among other things, calling for an increased involvement of individuals in the protection of their own privacy and increasing the control of the CNIL.
Context of the document Concerned by the growing use of social networks, the Commission of Constitutional Law, of the Legislation and General Administration of the Republic instructed the senators Anne-Marie Escoffier and Yves Détraigne to undertake a reflection on the subject of privacy in the era of digital memories. Published in May 2009, the report they produced has led to the draft of this proposed law. The proposed law intends to complete or amend several articles from the following documents: French code of education French code of criminal procedure French penal code Law n° 2003-239 for homeland security, March 2003. Law of 6 January 1978 on information technology, data files and civil liberties amended by the act of 6 August 2004 relative to the protection of individuals with regard to the processing of personal data.
Key points in the document The document covers the following key points: **Awareness of young people to protect their privacy** In the context of teaching civic education, the objective of the proposed law is to make individuals become the primary actors in their own protection by increasing awareness in school about the dangers of exposing ourselves and others on the Internet. **Legal qualification for IP address?** The document gives a legal qualification to the IP address, and puts an end to the differences

of jurisprudence. IP address would become then a personal data (article 2).

Legal regime for website cookies
Articles 6 and 9 change the legal regime of cookies in order to:
• Reinforce obligation to inform by data processors
• Require the consent of the user before the installation of cookies on his/her computer.

Recognition of the right to oblivion
The proposed law gives greater effectiveness to the right to digital oblivion by clarifying the exercise of the "right to be forgotten", (article 8).
Thus, from the collection of personal data and prior to any disclosure, any individual is in a position to object to the use of their data for marketing purposes.
When personal data have been processed, any person establishing its identity has the right, for legitimate reasons, to require their removal, except in few stated cases.

The obligation to notify the existence of security vulnerabilities
The document requires the data processor to implement all appropriate measures, given the nature of the data and the risks presented by the processing, in order to ensure data security.

The refocusing of tasks and power control of the CNIL
The document would implement that organisations with more than 50 employees accessing or processing personal data would be required to appoint a data protection officer ("DPO") who will report to the CNIL. Acting in an independent manner, a DPO must inform and advise any person working on behalf of the data controller on issues relating to data protection, as well as maintain and regularly update a list of all the data processing activities carried out by the data controller (article 3).

State files more framed by the CNIL
The document reaffirms that treatments of personal data implemented on behalf of the State and of interest to the security of the State or defence are authorised by order of the competent ministers after asking for a published reasoned opinion of the CNIL. The proposed law reinforces the CNIL power by, among other things :
• allowing the CNIL unannounced inspections,
• specifying that the four parliamentarians from the CNIL must be designated "in order to ensure a pluralist representation".

Assessment of the importance or significance of the document
This proposed law anticipated the publication on 25 November 2009 of Directive 2009/136/EC amending Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. The document could have served as a working basis for the implementation of the 2009 European Directive. The proposed law has been registered to the Presidency of the National Assembly on 2 July 2012 and the legislative procedure is still running its course. However, there have been media reports that the French government are not in favour of this proposed law.

707. Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, Le livre blanc sur la défense et la sécurité nationale, [The French white paper on defence and national security – unofficial translation], Paris, 17 juin 2008. http://archives.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html. 332 pages.

What domain (health, transport, policing, etc.) does it address?
National security and defence

Target audience of the document
Security and defence stakeholders with France, as well as external audiences. Document is written in English.

Stated purpose of the document
A white paper, produced as the end result of a wide ranging review of defence and security policy including, for the first time, participation by the Parliament and with a higher level of public transparency and consultation. The white paper sets out a new French defence and security strategy.

Context of the document
The document is produced in a context of globalisation, with new powers emerging, shifts of power towards Asia, and the end of the post-cold war era. This leads to increased complexity and uncertainty. The boundaries between domestic and foreign security are now blurred. France is also building an all-professional army. This new environment apparently leads to the requirement for a new security strategy. The goals of this strategy are to ensure that France remains a major military and diplomatic power, with the capacity to guarantee the independence of France and the protection of French citizens. The document replaces the previous strategy document from 1994, focused upon projection of power and peacekeeping missions.

The document occasionally refers to the previous Defence white paper from 1994.

Key points in the document
The post-cold war period is over. International relations are dominated by globalisation and transformation. Major strategic upsets could occur at any time, and this environment is characterised by uncertainty, complexity, reduced predictability and a wide range of global risks that can be both intentional and accidental. France's ambition is to not to have to submit to this uncertainty, and to harness the knowledge and information revolutions to be able to anticipate, respond to and influence international developments. This requires modernisation, breaking down institutional boundaries and speedy decision making.

"We have now entered a world not necessarily more dangerous, but certainly less predictable, less stable and more contradictory that the one that emerged in 1994." (p.14)

A major point in the document is the innovation of a policy that engages with not just defence, but with national security, a new concept for French security strategy combining defence and security.

"From this process a new concept has emerged: that of a national security strategy that treats defence policy, foreign policy and economic policy as part of a whole, whilst not losing sight

of their distinctive characteristics." (p.10).

Globalisation is understood as having both impacts and positive developments, producing growing interdependence, enhanced telecommunications and a border-free world, with a reduced number of armed conflicts and a greater capacity for mobilisation of international security. The European Union project is advancing and the 'security questions' of many European states are answered at a EU level. The downside is the rapid spread of crises, undermining the states capacity to regulate, identity-based responses to uniformity, social and economic inequality with implications for international stability, global warming and pressures on strategic natural resources, and weapons proliferation. The logic of state power has not disappeared with globalisation, however there are changing forms of violence including terrorism and the privatisation of armed violence. There is also a rise in global military spending and still large areas of conflict and fragile states. Because of its security actions there is an external perception that the west behaves aggressively. Systems of collective security are seen as fragile and suffering a crisis of legitimacy. Interruptions to global flows can trigger unexpected regression in security and there are new nuclear powers.

The implications for France and Europe of this are four critical regions (the "arc of crisis" from the Atlantic to the Indian Ocean, sub-Saharan Africa, the European continent, and major conflicts in Asia), new vulnerabilities, and new parameters of security. The top three perceived threats to France (and Europe) are terrorism, major cyber attacks and missile threats. Other perceived threats include espionage and strategies of influence, serious criminal trafficking, new natural and health risks, heightened technological risk and the exposure of citizens abroad. The new parameters of security include the growing connectivity of threats and risks (such as terrorist links, contagion between unstable regions), thus requiring a wide ranging response, with combined and preventative policies. The document highlights the continuity between internal and external security, with the traditional distinction no longer relevant in the new strategic environment. The document suggests the need to define overarching security strategies and integrate all dimensions of security. There is the possibility of sudden strategic upsets (uncertainty, sudden breaks, new weapons, technological developments in biotech, nanotech and space), and of changes affecting the nature of military operations, for example increasing urban settings for conflict. The document states that technological superiority has failed to give guarantees of victory and that the human factor remains decisive.

The document identifies France's strategic position as at the extremity of the European continent and at the intersection of major air and sea routes, with significant overseas possession, a strategic presence on the UN national security council, a founding member of NATO and the EU, a nuclear power, a growing population, and with a high quality armed forces. The security strategies aims are to: defend population and territory, contribute to European and international security (which fits with both France's needs and responsibilities), and defend the values of the Republican compact. The principles of the security strategy are anticipation and responsiveness, all-round capability, allowances for surprise and upset, resilience and a capacity to build up forces if necessary.

The document identifies a range of strategic functions, the combination of which is intended to provide national security. **Knowledge and anticipation** allows the understanding of developments, is the first line of defence and permeates all civil and military authorities. This is seen as an area of French excellence. The battle for the 21st Century is anticipated to be on the field of knowledge and information. Society as a whole is perceived as benefitting from increased resilience when it is known that the government is looking to the future, analysing

and avoiding risks. **Prevention** is the ability to act on the causes of risks in a timely fashion. The EU and UN have key roles in prevention, as does generally improving the international system and managing tension. Preventative diplomacy and the International Criminal Court are seen as key tools. The (strictly defensive) nuclear **deterrent** is seen as the key guarantor of strategic autonomy. Nuclear policy is closely aligned with allies; the document states that it does not anticipate a nuclear threat to the UK, for example, that does not also threaten France. **Protection** requires new organisations and new methods, including increased interaction with civil society and the private sector. Intervention capacity is required to guarantee strategic interests and to shoulder international obligations. Unilateral military intervention is only anticipated in the case of protection of French citizens abroad, otherwise it will be multilateral. There is a sizable section on the legality of any interventions.

The Document sets out France's ambitions for Europe and being at the forefront of a progressive EU political union, and as a presence on the world stage. The EU is perceived as a relatively new but increasingly important international security actor. It identifies high support for CFSP. France wants Europe to be equipped with civilian and military capability to be a major player in international crisis management. The document recommends an intervention force, capability for two to three peacekeeping operations, and increased planning capacility and restricting of the European defence industry. EU and NATO are seen as complementary.

The white paper advocates improved technological development, and also additional programmes in relation to intelligence and preparation for the future, knowledge and anticipation including 'knowledge based security', observation, early warning, development of surveillance and armed drones as well as both offensive and defensive cyber war capabilities. The document also sets out the new structure of the armed forces and the financial effort to be directed towards defence.

Assessment of the importance or significance of the document

There has been a change of government since this document. However future governments will have to respond to the characterisation of the security environment set out in this document, and it likely affects some long term policies. This strategy document has not yet been superseded; therefore it remains a very significant, high-level policy document with effects throughout French security culture.

716. Secrétariat générale de la défense et de la sécurité nationale, *Orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information* [*Guidelines for research and development in terms of security of information systems* -- unofficial translation], Agence nationale de la sécurité, des systèmes d'information, Paris, 10 avril 2008, 12 pages.

What domain (health, transport, policing, etc.) does it address?
Security, new technologies, privacy

Target audience of the document
General public, various government organisations, information systems security research companies

Stated purpose of the document
This report intends to guide, orient and incentivise research and development strategic choices in the field of information systems security.

Context of the document
The security of information systems is becoming a more critical need for society. Faced with this situation, the French government created by decree (Decree No. 2001-694) the interdepartmental Committee on Security of information systems. Its mission is to develop a public policy report for research and development in terms of information systems security. This document is the 2008 update of the public policy report produced by the interdepartmental Committee in 2006.

The following documents were mentioned in the body of the text:

Decree No. 2001-694 of 31 July 2001 establishing the interdepartmental commission for the security of information systems.

Common Criteria for Information Technology Security Evaluation, international standard (ISO/IEC 15408) for computer security certification.

Key points in the document
This document is a public report that aims to guide and incentivise strategic choices in research and development in the field of information systems security.

- Regarding issues of security of information systems the document stresses the importance of the following items:
  -Information control
  According to this document the ability to assess security products must be ensured in all areas that may involve security. This requires the development of formal design and control methods which should be available for all actors.

  -Protection of privacy
  The first issue related to the development of the information society is the protection of privacy, which includes the confidentiality of information processed. It is also highly important to ensure trust in digital society.

-Availability
Modes of assistance should be provided to address any possible problems in order to ensure the infrastructure availability and continuity of e-Services.

- The report also stresses that security is impacted by the evolving of information systems such as data aggregation, administration and supervision, the ubiquity of digital identity and nomadism, media streams and "wireless" or "contactless" devices.

- All products and information security systems are based on a number of items that contribute to the global security of a system such as the foundations of security of information systems, systems architecture, electronics and microelectronics and other theoretical tools. According to this report, it is essential and necessary to master the integration of these technologies to allow efficiency, security and therefore trust in the information system security.

Assessment of the importance or significance of the document
This report was created in accordance with the French White Paper on defence and national security, and wishes to contribute to the orientation of national and European research in the security of information systems. However, the impact of this specific document is difficult to measure. First, only a few reports at a national level refer to it. Second, impact of this report may lose its strength quite rapidly because of the extraordinary rapidity of developments in this field.

718. Secrétariat générale de la défense et de la sécurité nationale, *Référentiel Général de Sécurité* [The General Security Regulatory Framework -- unofficial translation], Agence nationale de la sécurité des systèmes d'information, Paris, 6 mai 2010. 33 pages.

What domain (health, transport, policing, etc.) does it address?
Security of information systems, Privacy, Security

Target audience of the document
Government entities and industry / private companies that provide government entities with security products.

Stated purpose of the document
The General Security Regulatory Framework (RGS) is established by the French Network and Information Security Agency (ANSSI) and the Agency for the development of e-administration. Its goal is to regulate all electronic exchanges of information among and between government entities and citizens. The RGS provides a regulatory context for strengthening security systems.

Context of the document
The ANSSI and the Agency for the development of e-administration want citizens and users to be able to trust the electronic services offered by the administration, particularly in regard to protection of their personal data. An ordinance (No. 2005-1516) was created in 2005 "The General Security Regulatory Framework", because of an awareness of the fact that techniques used in cyberspace by malicious individuals or groups of individuals are more and more efficient and electronic exchange between governmental entities and citizens is continuously growing. The conditions under which the RGS is drawn up, approved, modified and published are set out in the Decree No. 2010112 of 2 February 2010 related to the application of Articles 9, 10 and 12 of the 2005 ordinance.

This document refers to the following other documents:

Ordinance No. 2005-1516 of December 8, 2005 "on the electronic exchanges between users and administrative authorities and between Legal the administrative authorities"

Decree No 2010-112 from 2 February 2010.

Decree No. 2010-112 of February 2, 2010 taken for the application of Articles 9, 10 and 12 Order.

Decree n ° 2001-272 of 30 March 2001 adopted in application of Article 1316-4 of the Civil Code relating to electronic signatures.

Ordinance of 26 July 2004 on the recognition of qualifications of providers services, electronic certification and accreditation bodies conducting their evaluation.

Law No. 2000-321 of 12 April 2000 on the rights of citizens in their relations with government

ANSSI, Standards for information security, 2009.

ANSSI, "SSI Policy" Guide, 2004.

ANSSI, "SSI maturity" Guide, 2007.

ANSSI, Method of risk analysis, 2010.

ANSSI, "Management and Integration SSI Projects" Guide, 2006.

Key points in the document

The enforcement of the «General Security Framework» (RGS) and its development is meant to allow public authorities to significantly raise the protection levels of their information systems. The RGS sets out the rules for all French administrations that deal with information security and use electronic signatures, authentication, confidentiality, or timestamp.

The RGS also contains good practices about the security of information systems (SSI) in order to guide the administrative authorities and service providers in the choices they face in terms of SSI.

The RGS also provides necessary clarifications on how to take full account of the regulations, particularly regarding risk analysis and security accreditation of an information system.

The RGS requires French administrations:

- to identify information that needs to be protected and threats that need to be considered using a risk analysis,
- to determine the necessary security features in order to address the risks identified,
- to respect RGS rules regarding the following items: electronic signature, authentication, encryption, time stamping, and in general any mechanism and cryptographic key management process etc…, and
- to formally certify that it has taken responsibility for account security by acquiring a security accreditation.

Assessment of the importance or significance of the document

The RGS is in the same vein as the Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services. The RGS requires the French administrations to comply within three years after its publication for existing systems prior to publication, and 12 months for systems created within 6 months following the RGS. However, only two years after the RGS publication the ANSSI sought to change part of the document, and the updated version of the RGS ANSSI will aim to enable the qualification of new types of providers (including auditing SSI), to harmonise schedules with new versions of European Standards, to correct or clarify some inaccuracies of the first version and take into account the laws and regulations related to security of information systems published since May 2010.

739. Commission nationale de l'information et des libertés (CNIL), Délibération n°2008-174 du 16 juin 2008 portant avis sur un projet de décret en Conseil d'Etat portant création au profit de la direction centrale de la sécurité publique d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE » [Deliberation No. 2008-174 of 16 June 2008 giving an opinion on a draft decree of the Council of State in favor of establishing the Central Directorate of Public Security of automated processing of personal data referred to as "EDVIGE"-- unofficial translation], juillet 2008.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000019796251&fastReqId=636228208&fastPos=1 8 pages

What domain (health, transport, policing, etc.) does it address?
Privacy, security

Target audience of the document
Public document intended for the Ministry of the Interior.

Stated purpose of the document
The document contains the CNIL Deliberation, it aimed at giving an opinion about two draft decrees authorising the creation of two databases processing personal data called « EDVIGE » (Documentary exploitation and valorisation of general information) and « CRISTINA » (Centralising inland intelligence for homeland security and national interests).

Context of the document
The implementation of the draft decrees results from the reform of the French intelligence services in effect from the 1st of July 2008. One of the CNIL's responsibilities is to check whether data controllers comply with the Data Protection Act. Hence, as the draft decrees aimed at centralising and analysing information related to a large number of natural and legal persons, the CNIL was asked to deliberate on the matter and to give its opinion.

The following documents were mentioned in the opening paragraph and in the body of the text:
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 108

European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Law No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties as amended by Law 2004-801, of 6 August 2004 relating to the Protection of Data Subjects as Regards the Processing of Personal Data

Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties (Amended by Decree 2007-451 of 25 March 2007) Consolidated on the 25th of March 2007

Decree No 85-1057 of 2 October 1985 on the organisation of central administration within the ministry of Interior and of decentralisation, article 12

Decree No. 91-1051 of 14 October 1991 implementing the computerized files, manual or

mechanized and managed by the intelligence services of the provisions of Article 31, paragraph 3 of Law No. 78 - 17 of 6 January 1978 relating to data, files and freedoms , Official Gazette No. 241 of 15 October 1991 Page 13 498

Decree No. 91-1052 of 14 October 1991 on computerised terrorism database implemented by the intelligence services of the Ministry of the Interior

Decree No. 2007-914 of 15 May 2007 adopted in application of Article 30 of Law No. 78-17 of 6 January 1978 relating to computers, files and freedoms.

Draft decree No. 85-1057 of October 2, 1985 as amended relating to the organization of the headquarters of the Ministry of the Interior and Decentralization, and the draft decree on the decentralized organization of the Central Directorate of Public Security.

Key points in the document

In the document the CNIL observes and raises concerns on the following key points of the draft decrees:

The means and purposes

The CNIL acknowledges the purposes of the draft decree and data collections. The CNIL thinks it would be necessary to specify the conditions and nature of administrative investigations that may be carried out.

Data retained and categories of data (Physical description, photography, behaviour and movements, document of identification, legacy and tax related information, criminal records, data relating to the environment of the individual, the motives for recordings)

- The CNIL thinks that the recording of data on public figures (union organisers, local and national religious or political figures) should be much more limited than stated in the draft decree and should not include the recording of "behavior" or "movement" of these public figures.
- The CNIL regrets that the collection of information on ethnic origin, health and sexual life of people is not accompanied by adequate safeguards. The CNIL suggests that the data on sexual orientation or health of these persons are registered in exceptional cases.
- The CNIL wishes that the EDVIGE processing should be subject to no cross, no reconciliation or any form of linking with other files, including those of the police.

Minors

The CNIL has affirmed its commitment to the principle that such a collection should be exceptional and should be surrounded by particularly strengthened guarantees. In particular, it expressed the wish that the minimum age linked to the collection of information on minors should be 16 years old, not 13 years old.

Retention periods of the data

According to the CNIL a limited period of 5 years should be implemented with respect to information collected on a person subject to an administrative investigation for access to certain jobs.

Security measures

The CNIL asks for more specific information on security levels surrounding the technical operation of the file "Edvige" or on the possible existence of a traceability system that

would verify the conditions of access by public authorities to the data in the file.

The rights of individuals and the control exercised by the CNIL

The CNIL has requests that the text be published so that the public debate can exist.

The CNIL acknowledges the annual obligation imposed on the Director General of the National Police to report to the CNIL on update and deletion of information stored in "Edvige".

In this deliberation the CNIL verifies the validity of the new draft decrees and check that it doesn't break the rules of other decrees in the matter of privacy.

Throughout the document the CNIL acknowledges the engagements of the Ministry of Interior; raises concerns on various privacy issues and suggests that a number of precisions should be added to the draft decrees.

Besides the introduction, the rest of the document only refers to the EDVIGE draft decrees, and does not mention CRISTINA. This may be because CRISTINA is covered by defense secrets.

Assessment of the importance or significance of the document

Following on the CNIL deliberation the Ministry of the Interior published a new decree including a number of the CNIL recommendations, such as:

- the reconciliation or any form of linking with other files
- a prohibition on recording the "behavior" or "movement" of public figures
- the publication of both the decree and the CNIL opinion
- the limit on the shelf life of recorded data

In contrast to the above changes, the Ministry of the Interior also ignored a large number of issues raised by the CNIL, and the CNIL reaffirmed its reservations about these (following) items in a press release on 02 July 2008:

- the collection of information relating to minors
- the guarantees for the collection of information on ethnic origin, health and sexual life of people
- the security levels surrounding the technical operation of the file "Edvige" or on the possible existence of a traceability system
- the formalised procedure for updating and clearance files.

Being a public document the numerous concerns that the CNIL raised eventually fed into the concerns of the population. Consequently, due to a massive mobilisation in France, the government had to withdraw the EDVIGE decree in November 2008. EDVIGE was then replaced by EDVIRSP which was integrated in the Law on the orientation and programming for performance of domestic security on 14 mars 2011.

756. Commission nationale de l'information et des libertés (CNIL), Vidéosurveillance / vidéoprotection: les bonnes pratiques pour des systèmes plus respectueux de la vie privée [*Video surveillance / CCTV*: *best practices for systems more respectful of privacy* -- unofficial translation], Communiqué de presse, juin 2012. 14 pages

What domain (health, transport, policing, etc.) does it address?
Privacy, Security, policing

Target audience of the document
General public

Stated purpose of the document
The CNIL reports on its inspections of video surveillance / CCTV systems and wishes to assist professionals and individuals in a process of compliance by creating guidance documents.

Context of the document
On 14 March 2011 the Law No. 2011-267, called "LOPPSI 2" was implemented. This law empowered the CNIL with a new mission, to oversee all video-surveillance systems installed on the public highway. Prior to the adoption of this law, the CNIL only had jurisdiction over video-protection systems installed in private premises.

In 2011, the CNIL conducted many inspections on the 935,000 cameras installed in France. The CNIL reports on its work through this press release.

The following documents were mentioned in the body of the text :

Law of 6 January 1978 on information technology, data files and civil liberties amended by the act of 6 August 2004 relative to the protection of individuals with regard to the processing of personal data.

Law n° 2003-239 for homeland security, March 2003.

Code of Interior Security

The French white paper on defence and national security, Paris, 17 June 2008.

Key points in the document
In this document the CNIL reports on its investigations in video surveillance and CCTV throughout the French territory. The CNIL has conducted more than 230 inspections of these devices between March 2011 and June 2012. The inspections focused on the private (75%) and public sectors (25%).

The CNIL mentions different regulatory issues surrounding CCTV in France:

The CNIL mentions the distinction between video protection and video surveillance:

• video protection: refers to cameras installed in the streets or in places open to the public. It is subject to the Code of Interior Security. It needs the opinion of a departmental committee chaired by a magistrate and a prefectoral authorisation. It is controlled by the CNIL.

• video surveillance refers to cameras installed in places that are not open to the public (a company office, residential buildings). It is subject to the Data Protection Act and must be

declared to the CNIL.

In an educational approach, the CNIL invites any video surveillance users to go on the CNIL website and consult the six practical information sheets available.

Video surveillance and video protection statistics:
The CNIL gives figures relating to video surveillance activities between 2008 and 2011. For example, the CNIL reports that 175 complaints were registered regarding the use of video surveillance in 2008 and 363 in 2011. In 2008, 2588 video surveillance devices were declared to the CNIL and 5993 in 2011. Regarding the video protection, in 2011, 170,042 cameras were installed on the streets or in places open to public (13% more than in 2010). Today, around 38,000 cameras watch the streets in France.

What should not be done:
The CNIL lists the 10 most common mistakes that go against the regulations, such as:
- Hide cameras to film employees without their knowledge
- Filming inside private apartments or apartment doors
- Filming the playground of a school 24h/24
- Filming the streets to watch your own car
- Filming the office of an employee permanently
- Filming the break rooms of a company
- Filming the entrance of a local union of a company
- Putting a camera in a hotel room
- Filming the locker room of a swimming pool or a gym
- Filming the toilets of a restaurant or of a company
- Saving images indefinitely.

Focus on the video of tomorrow:
The CNIL seeks to anticipate new uses and new technologies that will change the need for regulation in the coming years. Therefore the CNIL examines the emerging and the most prominent trends, namely: predictive and analytic video and the use of other technologies (sound, facial recognition) in the video surveillance.

Throughout the document the CNIL identifies the following points as critical:
- clarification of the legal regulations;
- information for lay persons lacking or insufficient;
- improper positioning of cameras and insufficient safety measures

Assessment of the importance or significance of the document
This document clearly has an educational purpose and tries to inform video user and others people subject to be recorded by those video of the regulations. This document is one of the first documents published by the CNIL in its new task of overseeing video systems. In this press release the CNIL lays the foundation of the work it will have to undertake in order to make video surveillance more respectful of privacy.

2.6 ITALY POLICY DOCUMENTS

770. Italian Council of Ministers, Relazione sulla Political dell'Informazione sulla Sicurezza-2010 [Report on the Information Policy on Security-2010 – unofficial translation], 2010. 67 pages.

What domain (health, transport, policing, etc.) does it address? Cyber security, economic security, terrorism, weapon proliferation, organised crime, illegal immigration, environment, civil protection, health and new technologies.
Target audience of the document This is a report prepared for the Italian Parliament.
Stated purpose of the document The document details the intelligence activities that the Italian government carried on in 2010 to protect Italian security and their key findings.
Context of the document This is a report to brief the Italian Parliament on the result of the intelligent strategies and activities conducted by the Italian government in 2010 as well as the key areas of risk for Italian security based on these intelligent gathering and activities. The intelligent and security activities required greater efforts compared to previous years due the fiscal and economic crisis that exacerbated security risks in several domains (e.g., economic, socio, political, cyber, etc).
Key points in the document The document details the key security risks for Italy both within its border and internationally. Key areas identified as of highest concerned for security are: 1) Vulnerability of the Italian economic and productive system. This covers: energy dependency for Italy including political instability in energy producing countries, economic espionage, attempts to acquire Italian technological know-how, infiltration of criminal activities into the Italian economy, strong competition for Italian companies operating overseas and illicit money transfer (money laundering); 2) Increasing number of cyber attacks from hackers, terrorist and criminal groups exploiting new viruses (e.g., botnet and super virus) and the militarisation of cyber space; 3) Continuous proliferation of weapon of mass distraction with focus on Iran's activities; 4) Increased risks for Italian military contingencies involved in overseas operations, specifically in Afghanistan, Pakistan, Middle East, North Africa and Horn of Africa, 5) Rise of anti-western sentiments and nationalist groups (e.g., al Qaida, Jamaah Islamiyyah); 6) Terrorist threats in Europe and in Italy; 7) Organised crime with the consolidation of the "mafia enterprise" in Central-Northern Italy and the emergence of other criminal national groups such as Chinese, Balkan, African and South American; 8) Illegal immigration, which is highly correlated with organised crime; 9) Internal political extremism (e.g., ranging from political and economic riots to anarchism). As potential risk multipliers the report identified: 10) Climate change; 11) Resource scarcity;

12) Pandemics and health risks;
13) And the risk associated with the development of new technologies (e.g., biotechnology and bioterrorism).

Assessment of the importance or significance of the document

The report is of central importance both in shaping the thinking of Italian decision makers on security and driving the overall Italian security strategy.

774. Italian Defence Ministry, *Libro Bianco, 2002* [The White Paper, 2002 – unofficial translation], Centro Studi per la Pace, Rome, 2002. 244 pages.

What domain (health, transport, policing, etc.) does it address?
National defense, specifically transformation of armed forces, evolution of civil and military relationships and international co-operation on defense.

Target audience of the document
The document is mainly directed towards the Italian government, decision-makers, practitioners and experts dealing with Italian defense.

Stated purpose of the document
The document presents a review of the Italian armed forces and their activities. It aims at stressing the centrality of defense, above all the centrality of Italian armed forces in promoting Italian security, as well as providing a strategic vision of the context of military security and defining the conceptual and international reference points that will guide the process of continued transformation of the military (e.g. Europe and NATO).

Context of the document
This review followed a gap of 16 years since the previous white paper on defense was issued in 1985. During this period major international and internal changes had occurred, specifically:

- the end of Cold War and the emerge of a new world order, characterised by ethnic and nationalist tensions in several regions of the world (e.g. European periphery, Middle East, Asia, Northern Africa),
- the tragic events of September 11, 2001, and the rise of international terrorism,
- a stronger public opinion support for overseas military interventions ,
- a new Italian majority and government (the second Berlusconi government), and
- the beginning of a process of adaptation of forces, doctrine and capabilities of the Italian military.

Key points in the document
The document details the key areas of strategic focus for the Italian armed forces and the overall Italian defense strategy. Key points emerging from the document are:

1) Italian armed forces must develop the capability to dynamically face complex and transnational threats whenever and wherever they occurs since national security can no longer depend exclusively on the capability to guard and provide static defense of the metropolitan areas ("Homeland defense");
2) Italian forces must align and integrate with the activities of the European Union, NATO and UN, and therefore play a greater role in safeguarding the European-Atlantic area and promoting collective defense. This means an ever increasing tendency toward "joint" and "combined" forces, which will require not only a greater coordination and integration within the Italian armed forces but also an increased interoperability with the allied forces.
3) The development of a fully "professional" armed force of circa 190.000 men
4) Clear priorities and focus on spending on military equipments and infrastructures (above all in relation to naval and air forces). This spending should not be regarded as national anymore but should be part of international and co-operative efforts ;
5) The need for a reform of the military chain of command with a greater centralisation

of the direction of operations, requiring the elimination of intermediated functions and structures, which are not operational and not aligned with Italian key responsibilities and role within its international alliances;

6) The creation of armed forces balanced in their components and financially sustainable, with operational qualities and capabilities that correspond to security requirements;
7) In summary, planning must be oriented toward a measured reduction of the quantitative dimension of force structure, a marked enhancement of the qualitative dimension, increased financial sustainability and optimisation of the capability dimension.

Assessment of the importance or significance of the document

The report is of central importance in both shaping the thinking of Italian decision makers on defense and the role of armed forces and directing the activities and transformation of Italian armed forces.

788. Garante per la Protezione dei Dati Personali, *Annual Report for the Year 2001 – Summary*, 1 July 2002. http://www.garanteprivacy.it/garante/doc.jsp?ID=1751047 4 pages.

What domain (health, transport, policing, etc.) does it address?
Data protection and information security.

Target audience of the document
Anyone interested in Garante's activities. The document is written in accessible English as well as Italian.

Stated purpose of the document
The document presents a review of the activities of the Italian DPA during the year 2001.

Context of the document
The document was produced in July 2002, thus there was scope to consider some activities immediately after the events of Sept. 2001. However, the document does not mention 9/11, terrorism or security, or appear to examine any policies that might be related to security aside from CCTV in public space. The 2002 annual review includes mention of the SIS database and new a requirement that immigrants submit fingerprints, but neither of these are explicitly discussed in relation to terrorism either.

This document mentions the following other documents:
The European Data Protection Directive 95/46/EC

EC Directive 97/66 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Italian Data Protection Act (no. 675/1996)

Italian Legislative decree no. 467/2001, which modified the Data Protection Act

Italian Legislative decree no. 171/1998, which transposed EC Directive 97/66 into Italian law

Key points in the document
The document begins by outlining the "main legislative and regulatory developments" of 2001. This is primarily related to Italian Legislative decree no. 467/2001, which modified the Data Protection Act and Italian Legislative decree no. 171/1998, which transposed EC Directive 97/66 into Italian law. The first decree modifies the Data Protection Act to identify cases where the "ordinary" processing of personal data means that obtaining consent of the data subject is unnecessary. Garante will oversee such cases. It also includes a general notification requirement and streamlines the implementation of the Data Protection Act. The second decree assisted in implementing Directive 97/66 since the EC deemed that the original implementation was insufficient. The decree includes arrangements for making anonymous payments for telecommunication services and requires telecommunication services to provide better information to consumers about call line identification in emergency situations.

The document proceeds by outlining "main decisions by the DPA" and includes decisions on

issues such as:

- Protection of employees' personal data and evaluation data and access by employees to the data concerning them
- Medical data and data included in forensic medical reports
- Data concerning children
- Data processed by private detectives
- Data processed by private credit referencing agencies
- Telephone traffic data
- Setting up of large data banks and population census
- Video surveillance
- Processing of biometric data
- Codes of conduct and professional practice

The document ends by outlining their communication practices, particularly those which are geared towards members of the public.

Assessment of the importance or significance of the document

The report does not have much significance in terms of legislative policy, it simply seeks to explain legislative policy, perhaps to non-policy makers and/or lay persons. However, it reinforces Garante's commitment to reviewing legislation, conducting inspections and making recommendations around safeguarding personal data.

819. Garante per la Protezione dei Dati Personali, Decision on Video Surveillance, 8 April 2010. http://www.garanteprivacy.it/garante/doc.jsp?ID=1734653 13 pages

What domain (health, transport, policing, etc.) does it address?
Policing and private security

Target audience of the document
Those who deploy CCTV surveillance systems.

Stated purpose of the document
This decision is aimed at those who deploy CCTV surveillance systems and sets out a number of obligations with which users of CCTV systems must comply.

Context of the document
This document has been drafted due to a lack of specific legislation regulating video surveillance in Italy and the reliance on data protection legislation to provide a regulatory framework in this context. It also is intended to address "the considerable amount of questions, reports, complaints and prior checking applications lodged with the Italian DPA".

The document also mentions the following pieces of legislation:
Decree no. 196 dated 30 June 2003 (Personal Data Protection Code);
Article 15 of the DPA's Rules of Procedure no. 1/2000

Key points in the document
The document defines personal data as "any information related to a natural person that is or can be identified, whether directly or not, by reference to any other type of information" and states that the collection, recording or storing of images entails the processing of personal data.

Video surveillance may be used to ensure the protection and integrity of individuals (including urban security and public order), protect property, detect and prevent breaches of the law and collect evidence. However, those who control video surveillance systems must ensure "a high level of protection of fundamental rights and freedoms" and not interfere with data subjects' rights and freedoms to an "unjustified" extent. For example, data controllers must ensure that they comply with civil and criminal laws preventing unlawful interference in private life, employees from being monitored in the workplace and regulatory instruments surrounding video surveillance in spaces such as museums, sports grounds, passenger ships and transport hubs.

The document further describes data controllers' obligations:

Data controllers should always inform data subjects that they are about to enter an area under video surveillance.

Data controllers should carry out a prior checking exercise that demonstrates that the system takes into account any risks to data subjects' rights and freedoms, or their dignity, in the processing of personal information. This document should be lodged with the DPA. Data systems that use biometrics, for example facial recognition must consider risks to data subjects' rights, freedoms and dignity.

Notification of data processing to the DPA is only necessary in specific cases.

Data controllers must provide adequate data security, including measures that minimise destruction, loss, unauthorised access, unlawful processing and unlawful retention. Data should be retained for no longer than 24 hours unless there are exceptions for police investigations, festivities, normal closing hours, etc. Municipalities may not retain data for more than seven days unless exceptions are in force.

Individuals have the right to exercise their data protection rights, including right to access information held about them, to check the purpose and underlying logic of the data processing.

Discusses the use of CCTV in specific private sectors, including:
- *Employment Relationships*
- *Hospitals and Treatment Centres*
- *Schools*
- *Public Transportation Safety*
- *Use of web cams and/or online cameras for promotional, tourism and/or advertising purposes*
- *Integrated Video Surveillance*

Specific rules for each sector, such as CCTV in employment contexts can monitor company property, but not be used to surveil the behavior of employees.

CCTV may also be used by public bodies in respect of the following tasks:
- *Urban Security (However, the DPA does not feel that it is within its scope to define "urban security")*
- *Waste Disposal*
- *Detect Traffic Violations*

Assessment of the importance or significance of the document

The document applies data protection legislation to a particular, growing area of surveillance that has generated significant questions and controversies in Italy. It outlines the legal obligations of data controllers using video surveillance systems and continually focuses on fundamental rights and data protection principles. It will have significance for those procuring and operating video surveillance systems both in the present, and in the future if such systems become more fully integrated with advancements such as biometrics.

822. Garante per la Protezione dei Dati Personali, Data Sharing and Tracking of Transactions in the Banking Sector, *Official Journal*, No. 127, 3 June 2011. http://www.garanteprivacy.it/garante/doc.jsp?ID=1868766 online, approx.15 pages

What domain (health, transport, policing, etc.) does it address?
Banking

Target audience of the document
The decision is directed initially towards the Ministry of Justice for publication, but is primarily important for the Italian banking and financial industry, then secondarily for banking customers.

Stated purpose of the document
This decision is aimed at setting forth the requirements that apply to the processing of customer data by banks so as to ensure compliance with personal data protection principles under the terms of decree no. 196/2003 (Personal Data Protection Code). These requirements concern the sharing of customer data by banks and the traceability of the bank transactions performed by bank employees.

Context of the document
The document follows on from an inquiry and taking into account various reports, complaints and inquiries lodged with the DPA over the preceding years. Some of these involved the accessing of data held by banks without authorisation. The DPA carried out inspections at some banks, as well as an anonymous survey with 340 banking entities in Italy. As a result of this it was decided to lay down a comprehensive set of appropriate as well as necessary measures that could provide additional guidance for both sector-specific practitioners and customers.

The document also mentions:
Decree no. 196 dated 30 June 2003 (Personal Data Protection Code);
Article 15 of the DPA's Rules of Procedure no. 1/2000

Key points in the document
The document gives details on the result of this investigation. For example, the investigations detected two main situations in relation to sharing of personal data within the same banking group:

- Only data relating to crediting and debiting operations were shared between offices of banks all belonging to the same group, i.e. no information could be accessed on the balance of and/or the full list of the transactions performed on an account if that account was held at another bank within the group;
- All kinds of data could be shared within the banking group, i.e. balance data and other banking information could be accessed by bank tellers (who had been appointed as persons in charge of the processing based on the respective tasks and authorisation profiles) without any limitations.

The finding was that banks were acting as separate data controllers, and that data sharing between members of that group should be treated as communication with third-party recipients, thus requiring informed consent before being shared. The sharing of customer data between branches or offices of a bank is seen as the flow of data within a single organisation and does not require the data subjects' consent as it entails no third-party communication.

Data handling systems, including logs of access are handled both internally and by external companies through supply agreements. The document makes a decision on when outsourcing companies can be counted as the data controller: "a bank should be regarded as the sole data controller if customers' personal data are processed by an outsourcee according to arrangements whereby the aforementioned powers – which may only be vested in a data controller pursuant to section 4(1)f. and section 28 of the DP Code – continue to be vested in the bank, i.e. they are not factually vested in the outsourcee(s)."

The document also gives the results of the investigation into internal audit procedures. Nearly all banks had measures in place to protect consumer assets, however, not all banks had auditing procedures in place to regulate processing or requests for personal data.

The document concludes with a set of measures that the DPA considers necessary, and those that it considers appropriate. The former lists includes appropriate identification out outsourced companies as data controllers, IT controls on the processing and accessing of personal information, including keeping log files of access for at least 24 months, and setting up appropriate alerting methods. Appropriate actions include banks notifying data subjects that they may share information with other branches of the same bank, and notifying both subjects and the DPA of any unlawful processing or access by people with access to their data.

Assessment of the importance or significance of the document

The document is largely an extrapolation from existing Italian data protection legislation, and gives clarification and guidance for the requirements and obligations placed upon banks processing personal data. It will have significance for the banking and financial industry in Italy.

2.7 GERMANY POLICY DOCUMENTS

840. Bundestag, Plenarprotokoll der 14. Sitzung vom 19.01.2010 [Report of plenary session of the Bundestag (discussion about body scanners) - unofficial translation], 19 January 2010. http://dip21.bundestag.de/dip21/btp/17/17014.pdf 120 pages

What domain (health, transport, policing, etc.) does it address?
(Fight against) Terrorism, data protection, information freedom

Target audience of the document
The German National Parliament

Stated purpose of the document
Report of a plenary session of the German National Parliament.

There are two recurring causes that are being cited by the speakers in the document that seem to have prompted this discussion:

- The recent (unsuccessful) terrorist attack on a flight from Amsterdam to Detroit in December 2009, which was attempted by the so-called 'underwear bomber' (therefore the discussion touched on the topic of body scanners)
- The recent data leaks at large Germany companies (many personal data of employees was leaked).

Context of the document
It was prompted by recent data leaks at German companies and the terrorist attack in the Amsterdam-Detroit flight (see previous comment).

Referred documents:

- The German Data Protection Act
- German Criminal law

Key points in the document

- A substantial part of the document covers discussions about privacy of citizens, body scanners, anti-terrorism measures and security.
- Several parties expressed their opinions on the developments in these areas, and in general they expressed that they were more or less content about the (financial) attention and care for privacy-related issues in relation to the possible introduction of body scanners as well as the topic of 'data protection'.
- Also, there was a lot of discussion about terminology (naked scanners vs bodyscanners) and whether citizens' privacy (concerning their private/intimate body parts) can be warranted. The opinion generally shared was that the scanners should only be considered to be introduced once they worked properly, didn't pose risks to people's health and did not infringe upon their privacy.
- On another topic, some of the parties/members asked for more legislation, particularly concerning the protection of data of employees (as a result of recent data leaks at some larger German companies).

Assessment of the importance or significance of the document
This report is likely to have been of little significance. However, the document reflects in a very clear way the importance of privacy-related issues in German politics and society.

A Google search of this document returned no hits.

849. Bundesregierung, Vorratsdatenspeicherung und Sicherheitslücken [Answers of the Bundestag to members of Parliament about the storing of telecommunications and internet data for six months in favor of fighting terrorism and crime and security gaps - unofficial translation], 22 April 2010.
http://dip21.bundestag.de/dip21/btd/17/014/1701482.pdf

8 pages.

What domain (health, transport, policing, etc.) does it address?
Fight against terrorism, mail and telecommunication (data retention)

Target audience of the document
The German National Parliament

Stated purpose of the document
This report contains questions from members of the German National Parliament to Government (answered by the Minister of Justice) about the Directive 2006/24/EC which had been declared unconstitutional by the German Federal Constitutional Court.

Context of the document
In 2006, the European Data Retention Directive (Directive 2006/24/EC) was issued, which required Member States to store telecommunication data of their citizens for a period between 6 and 24 months. The German Federal Constitutional Court ruled that the new German law that would have implemented the Directive was unconstitutional. This report covers the discussion about how, if at all, already stored information would be deleted and how successful the provisions that resulted from of the European Data Retention Directive (Directive 2006/24/EC) had been.

Referred documents:
- The German Act for the Amendment of Telecommunications Surveillance (Gesetz zur Neuregelung der Telekommunikationsüberwachung)
- The German Telecommunications Act (Telekommunikationsgesetz)
- The German Code of Criminal Procedure (Strafprozessordnung)
- Directive 2006/24/EC

Key points in the document
- The effectiveness of the Directive 2006/24/EC. Members of the German Parliament raised questions about the value added (e.g. more suspects identified? More crimes solved?) of the law that transposed the Directive.
- The retention of telecommunication data. Now that the law has been ruled unconstitutional, what are the consequences? What will happen to the data that had been stored hitherto? Can it still be used or not?
- When asked about the successfulness/effectiveness of the new law, the German Minister of Justice could not provide most of the statistics and indicated that no data were available. Some statistics were given, but in general it remained unknown how much value added the Directive had regarding fighting crime/terrorism.

Assessment of the importance or significance of the document
The document is likely to have been of relatively limited significance. However, the discussion recorded by the report was highly significant in that it reflected the critical view taken by

the German National Parliament on a specific EU Directive and its role in allowing far more options to invade citizens' privacy with regard to telecommunications, and breach constitutional rights. Similar processes have taken place in other Member States.

A Google and Google Scholar search did not yield other results than websites from the German National Government and one of the political parties.

852. Bundesregierung, Rahmenprogramm der Bundesregierung "Forschung für die zivile Sicherheit (2012 bis 2017)" [Report of framework programme "Research for civil security"], Berlin, 25 January 2012. 24 pages.

What domain (health, transport, policing, etc.) does it address?
Civil security; Cyber security

Target audience of the document
The German National Parliament

Stated purpose of the document
In 2007, a national research program about civil security was launched in Germany, and in 2010 the High-tech Strategy 2020 for Germany was launched. This 2012 report outlines the follow-up, namely the second research program for civil security (Research for Civil Security).

Context of the document
See previous paragraph. It is a follow-up of the first research program, launched in 2007, about civil security. A main focus shared by both programs is cybersecurity. It is repeatedly noted that this issue is becoming increasingly important.

Most important referred documents:
- High-tech Strategy 2020 for Germany
- Research for Civil Security 2007-2010
- Research for Civil Security 2012-2017

Key points in the document
- It is proposed to continue focusing on cyber security, mainly in terms of research and policy development.
- The biggest challenge for the German government is regarded to be the ability to protect citizens' offline and online security while at the same time protecting and respecting their privacy and personal data.
- Integrity, authenticity and confidentiality of data are mentioned as very important.
- The document underscores the German government's aims to create and maintain an expert position in the field of security technologies; establish international collaborations; further knowledge and capacities within society by establishing a better scientific basis regarding knowledge about cyber security.
- Set up research that taps into the legal and social requirements and safety conditions to develop privacy-enhancing technologies on the basis of the principle of "privacy by design".

Assessment of the importance or significance of the document
The report clearly states what Germany's plans are for the future in the field of cyber security (research). It highlights privacy and security as topics at the top of the political agenda.

On various German websites there is a reference to the fact that this second research program - Research for civil security – would be launched.

854. Parlamentarische Kontrollgremium (PKGr), ***Bericht gemäß § 14 Abs. 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5 und 8 dieses Gesetzes (Berichtszeitraum 1. Juli 2004 bis 31. Dezember 2005), Bericht gemäß § 14 Abs. 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5 und 8 dieses Gesetzes [Notification about anti-terrorism measures and consequences]*****, 7 September 2006. http://dip21.bundestag.de/dip21/btd/16/025/1602551.pdf**
12 pages.

What domain (health, transport, policing, etc.) does it address?
Telecommunication, Mail/Personal communication, Data retention and Terrorism/Crime

Target audience of the document
The German National Parliament and the German Government

Stated purpose of the document
This document is a report by a special committee of the German Parliament, the Parliamentary Control Panel (PKGr). PKGr is "responsible for scrutiny of the work of the intelligence services at Federal level. The Panel can demand the submission of detailed information by the Federal Government on the federal intelligence services' general activities and on operations of particular importance."

The document contains information about how German intelligence services had been dealing with the rules and regulations in the field of telecommunication and data retention. More specifically, it contains the findings of an investigation of this committee about the extent to which intelligence services have violated citizens' privacy, and if they did, whether it was based on legal grounds (criminal investigation, anti-terrorism).

Context of the document
The report is a recurring audit report intended to check the functioning of the German domestic intelligence services.

In the document, many other documents are cited. They are primarily in the following categories:

- German law and regulation, mainly the German Constitution
- German policy documents
- Previous reports by the Parliamentary Control Panel.

Key points in the document

- The Parliamentary Control Panel reports on the integrity/functioning of the domestic intelligence/security services
- In general, the committee is satisfied with the way intelligence services had functioned and with the extent to which they had balanced privacy concerns and criminal investigation priorities.
- However, it is noted that the procedures followed by the intelligence services in their day-to day activities (e.g. wiretapping) are too complex, bureaucratic and time consuming. This potentially leads to security/safety risks, for example when lives are at stake.

- The advice of the committee was therefore to simplify legislation so that investigation procedures could become easier.
Assessment of the importance or significance of the document Limited significance. A Google search returned mainly internal hits (i.e. bundestag.de).

864. Enquête-Kommission, "Internet und digitale Gesellschaft" Datenschutz, Persönlichkeitsrechte. Fünfter Zwischenbericht der Enquete-Kommission "Internet und digitale Gesellschaft" Datenschutz, Persönlichkeitsrecht [Report of the project group 'Data protection and personal rights' of the Committee of inquiry 'Internet and digital society' (fifth report)], Bundestag, Berlin, 15 March 2012. http://dip21.bundestag.de/dip21/btd/17/089/1708999.pdf 92 pages.

What domain (health, transport, policing, etc.) does it address?

- Internet, the digital society
- Data protection

Specific topics that are addressed:

- Data protection laws
- Exchange of personal data
- Internet use and data protection
- Social networks and data protection
- Telecommunications and data protection
- Systematic tracing of persons by the police

Target audience of the document

The German National Parliament (the Bundestag)

Stated purpose of the document

The Committee of Inquiry 'Internet and the digital society' was set up by the German National government as a response to the growth of Internet use by German citizens and the personal data that are processed. The Committee has several project groups, addressing topics such as 'Education and Research' and Media literacy. One of these groups dedicated to 'Data protection and personal rights', was set up in 2010.

The Committee of Inquiry has written a number of reports on the topics addressed by its various project groups. The reports are meant to provide an overview of the state of affairs in each of the area covered. The overall purpose of such an overview is to inform the German National Government and provide input for debate in Parliament.

Context of the document

The report starts by stating that the Internet led to more personal data being processed, therefore data protection is important for everyone. The Internet, with its data streams and social networks, forms a challenge. The document discusses ways in which personal data can be protected in Germany.

Examples of other documents/sources referred to:

- Albers, Marion: Umgang mit personenbezogenen Daten und Informationen, in: Schmidt-Aßmann, Wolfgang (Hrsg.). Grundlagen des Verwaltungsrechts, Band II (§ 22). München: Verlag C. H. Beck 2008.

- Bergmann, Lutz/Möhrle, Roland/Herb, Armin: Datenschutzrecht – Kommentar. Stuttgart [u. a.] : Boorberg, Stand April 2010.

- Ennulat, Mark: Datenschutzrechtliche Verpflichtungen der Gemeinschaftsorgane und -einrichtungen. Frankfurt am Main: Peter Lang GmbH, 2008.

- Schaar, Peter: Privacy by Design. Identity in the Information Society, 2 (2010) 267–274.

- Kloepfer, Michael/Schärdel, Florian: Grundrechte für die Informationsgesellschaft – Datenschutz und Informationszugangsfreiheit ins Grundgesetz? JuristenZeitung (JZ), 64 (2009) 453–462.

- Deutscher Bundestag. Enquete-Kommission Internet und digitale Gesellschaft: Diskussionsforum. https://fo rum.bundestag.de/forumdisplay.php?22-Fragen-der-Pro jektgruppe-Datenschutz-Pers%F6nlichkeitsrechte&s=56 665542d673002b7588eb0752606b8a

- Rosen, Jeffrey: The Web means the End of Forgetting. The New York Times vom 21. Juli 2010. http://www.nyti mes.com/2010/07/25/magazine/25privacy-t2.html

- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Bizer, Johann: eGovernment: Chance für den Datenschutz. 2005 https://www.datenschutzzent rum.de/e-government/dud-200507.htm

- ZEIT ONLINE: Verräterisches Handy. Artikel vom 31. August 2009. http://www.zeit.de/datenschutz/malte spitz-vorratsdaten

Key points in the document

The document mainly covers the subject of data protection in different areas, from online social networks, to police activities, to smart grids, and payment systems. Within many of these topics, the issue of data security is discussed rather than data protection. The report also covers the German position on data protection in an international context. No explicit reference is made in the report to the relation between privacy and security.

Other issues covered by the report:

- An inventory of data protection regulations in force at the time the report was drafted.

- Exchange of personal data with the US. Concerns whether the US would treat personal data that is exchanged with them at the same levels of data protection that exists in the European Union by way of the data protection law.

- The need to provide a consistent level of data protection in US – EU data exchanges.

- Safe Harbor Principles.

- Data protection not just as a legal matter, but also as a social challenge.

- Data protection in the context of external (security) policy, differences from the German interpretation, the role of the German Supreme Court.

- Internet surveillance; profiling in relation to the informational right to self-determination.

- The German right to data protection is based on the difference between the protection

of data in the public sector and in the private sector (i.e. stricter for the former in order to provide protection against government interference in the lives of its citizens)..

- Video/photo surveillance in public places in relation to individual privacy.

Assessment of the importance or significance of the document
Indications of the importance of the document:

Limited impact.

A Google search returned a number of hits: mirrors of the document, references to the documents on sites of the federal and regional (such as Schleswig-Holstein) governments, blog entries (mostly by member of the Committee).

A Google Scholar search returned only one hit.

874. Schaar, Peter, Wie nachrichtendienstliche Erkenntnisse und polizeiliche Daten zukünftig verschmelzen werden – neue Herausforderungen für die Aufsichtsbehörden? Vortrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen der Conference of DPA's of Federal and Plurinational States [How intelligence data and police data will merge in the future - new challenges for supervision? Speech by Federal Data Protection Commissioner at Conference of DPA's of federal and plurinational states], Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 19 March 2009.

http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2009/PlurinationaleKonferenzMaerz.html 9 pages.

What domain (health, transport, policing, etc.) does it address?
Security
- Intelligence services
- Police
- Law enforcement

Target audience of the document
The Data Protection Commissioners of the German federal states

Stated purpose of the document
Speech by Peter Schaar, Federal Data Protection Commissioner, at the Conference of Data Protection Authorities of federal and plurinational states. The report highlights the tendencies and threats, based on historical examples, that emerge when intelligent services and the police merge and use each other's data and herewith violate the constitution.

It does not follow from some specific policy or document, but rather from recent developments (see below).

Context of the document
In light of the terrorist attacks (9/11, Madrid, London), and threats from the last decade there has been a growing discussion in Germany about more intense cooperation between intelligence services and the police. More specifically, the debate concerns the merging of their data. However, merging data or using each other's data is in most cases unconstitutional, because of the strict separation between intelligence services and the police/law enforcement (given the history of Germany, in particular activities of the Gestapo and Stasi).

Referred documents:
- The German Constitution;
- The constitutions of individual German federal states;
- A letter from the Allied military governors to the German Parliamentary Council of 14th April 1949 concerning the Federal Government's law enforcement powers;
- 1991 Act regarding the Records of the State Security Service of the former German Democratic Republic (Stasi Records Act).

Key points in the document
- It is noted that law enforcement agencies and intelligence services are increasingly cooperating in response to the terrorist attacks and threats in recent years. Cooper-

ation initiatives had been set up in order to prevent terrorism. However, such initiatives should comply with the Constitution, which is often not the case.
- The key reason for separating (activities of) the intelligence services and the police is to separate intelligence gathering (which is not necessarily started in response to a specific illegal act by an individual) and law enforcement (which would require probable cause before coming into action). The historic caution quoted by the document refers to the Gestapo (the secret police in the Third Reich) and the Stasi (the secret police in East Germany) where intelligence and law enforcement were not separated.
- The document refers to two recent developments in Germany that lead to the blurring of the the separation of the two services:
    - 1. The police had been granted additional rights to conduct preventive investigation in the context of the fight against terrorism;
    - 2. More centralised structures were created, such as the Joint Counter-Terrorism Centre (GTAZ) set up in December 2004 and the Joint Centre for Illegal Migration Analysis and Policy (GASIM) in May 2006,
- More specifically, the joint counter-terrorism database that was setup in 2007 had been used in unconstitutional ways in recent years (e.g. in cases deemed urgent, the police used personal data that had been gathered by intelligence services).
- It is stressed that the government should rethink whether it is possible to effectively fight and prevent terrorism while respecting the separation of the two services
- The most important note in the report regards the consequences of merging data and blurring intelligence and law enforcement, with significant effects for citizens and their right to privacy.

Assessment of the importance or significance of the document
This speech is likely to have been of limited significance.

Google and Google Scholar search – inconclusive.

2.8 ROMANIA POLICY DOCUMENTS

880. Parlmentul Romaniei, Camera Deputatilor, *Raportul comun suplimentar asupra propunerii legislative privind retinerea datelor generale sau prelucrate de furnizorii de retele publice de comunicatii electronice si de furnizorii de servicii de comunicatii electronice destinate publicului, 22 May 2012 Bucuresti [Report and debate about the transposition of the data retention directive]*, 22 May 2012. http://www.cdep.ro/comisii/juridica/pdf/2012/rp010.pdf 46 pages.

What domain (health, transport, policing, etc.) does it address?

- Telecommunications
- Data retention
- Security (the fight against terrorism and serious crime)

Concerns about potential privacy infringements were a primary motivation for drafting the current report.

Target audience of the document

The Romanian Parliament (National Assembly and Senate).

Stated purpose of the document

To discuss and suggest a number of amendments to the second version of the Romanian law transposing the EU Data Retention Directive.

To advice adoption of this second version with the suggested amendments.

Context of the document

The present document comments on the second proposal for a Romanian law transposing the EC Date Retention Directive.

The first law proposal had been declared non-constitutional by the Romanian Constitutional Court.

The second proposal also met with objections/negative advice expressed by the Romanian Senate, the Romanian Parliament's Commission for European affairs and Commission for human rights and minorities affairs; the Romanian National Association of ISPs. The basis of the objections/negative advice was, once again, the non-constitutional character of the proposed law and its potential impact on citizens' privacy.

In 2011, the European Commission started the infringement procedure against Romania for not transposing the Directive within the set time (potential fine for non-compliance: EUR1,710,000 plus over EUR44,770 per day).

The (proposed) law received unfavourable press coverage and was dubbed the "Big Brother" law.

Documents referred to:

- EC Directive 2006/24/CE (Data Retention Directive);
- Version one Romanian Data Protection Law proposal;
- Various memorandums of industry groups;

- Advices of various Romanian Parliamentary Commissions re data retention law proposal;
- the Romanian Penal Code.

Key points in the document

This supplementary report consists of three sections:

- a first section detailing the events that led to the drafting of the report;
- a second section listing the amendments deemed necessary for the adoption of the law and
- a third section listing amendments that were put forward but eventually not deemed necessary/appropriate to be included.

The main points in section two of the supplementary report address a number of issues among which:

- restore the legal basis for any data requests by LEA;
- make additional provisions re the retention period;
- specify conditions under which unused data is to be destroyed;
- set penalties for wilful misuse of data;
- specify the categories of authorities entitled to request data.

Assessment of the importance or significance of the document

Important document in that it effected changes in the proposed data retention legislation.

(Evaluation on the basis of Google search hits)

Inconclusive.

881. Romanian government, Stenograma audierii publice din ziua de 27 iunie 2006 «*Libertate individuală versus securitate naţională. Echilibrul între transparenţă şi secretizare*» [*Minutes of the public debate organised by the Romanian Government on the subject: "Individual freedom vs. national security – balancing transparency and secrecy*], 27 June 2006. http://www.cdep.ro/pls/dic/site.page?den=ap200606_8 12 Pages.

What domain (health, transport, policing, etc.) does it address?

- National security.
- Counter-terrorism.
- Surveillance in the context of counter-terrorism.

Privacy and individual freedom in relation to national security were two of the main issues discussed.

Target audience of the document

The Romanian Parliament, the general public.

Stated purpose of the document

Public consultation on the proposed legislative package for national security. The legislative package, proposed as part of new or revised measures to counter terrorism, would have extended investigative powers, in particular those of the intelligence services.

Context of the document

- See section above.
- The fight against terrorism.
- NATO's New Strategic Concept and
- the EU Security Strategy.

Documents referred to in the transcript:

- Legea de organizare şi funcţionare a Ministerului Apărării Naţionale (editor's translation: Ministry of Defence Act)
- Recommendation 1402 (1999) of the Council of Europe, Parliamentary Assembly, Control of internal security services in Council of Europe Member States
- Declaration of the Rights of Man and of the Citizen (France, 1789)
- Lege nr.415 din 27 iunie 2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării (editor's translation: National Defense Supreme Council law)
- Marian Ureche, Istoria serviciilor secrete la români (editor's translation: The history of the Romanian secret services)
- United Nations Convention against Corruption, ratified by Romanian Law 365/2004
- Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (editor's translation: Parliamentary Scrutiny of Federal Intelligence Activities Act) (Germany, 1979)

Key points in the document

The consultation followed the same procedure as a US public hearing. It was preceded by the submission of written statements meant to substantiate the need for holding such a consultation. The written material and all supporting documents were made available online by the commission that took the initiative for the consultation. The commission included human rights advocacy groups and the Romanian association of professional journalists. Additional-

ly, a commission of experts was charged with drafting the meeting minutes and synthesising the statements of the witnesses into an advice to Parliament regarding the proposed legislation. The consultation was open to all those interested.

The document is a transcript of sixteen witness opinions. Witnesses included representatives of NGOs, human rights organisations, ordinary citizens, members of government.

Main points of concern raised by the witnesses:

- The scope for non-constitutional activities carried out by the intelligence services under the proposed laws;
- The conflict between NATO's New Strategic Concept and the EU Security Strategy;
- The lack of parliamentary, democratic and financial control of activities carried out under the proposed legislation;
- The increased scope for abuse of extended investigative powers;
- The adoption of intelligence services practices by the police;
- Limitation of individual privacy and freedom in the name of the protection of national security;
- Increased potential for conducting unwarranted surveillance;
- The possibility of private financing of public tasks (in particular those of the intelligence services);
- Discretionary powers of the intelligence services;
- Vague terms in which the proposed laws were formulated which would allow for broad interpretations;
- Lack of public debate on the topic of (far-reaching) national security (measures) in particular in view of practices and experience from the communist past
- Privacy vs. security

Assessment of the importance or significance of the document

A relatively significant document. Mostly owing to the procedure followed which implied a fair amount of media and public exposure (i.e. initiated by human rights advocates and journalists; accompanied by documentation made available online; results presented during a press conference, etc.)

(Evaluation on the basis of Google search hits, Romanian language results)

A Google search of "Libertate individuală versus securitate naţională Echilibrul între transparenţă şi secretizare" returned over 70 hits (sites of the Romanian government, national media, NGOs and social media).

A search on Google Scholar for the same text returned only two hits.

882. Presedintele Romaniei, *Strategia de securitate nationala a Romaniei, [Romanian President, Romanian national security strategy]*, Bucuresti, 2007.

http://www.presidency.ro/static/ordine/SSNR/SSNR.pdf 58 Pages.

What domain (health, transport, policing, etc.) does it address?

- Romanian national security strategy

The document makes no specific references to surveillance or privacy. It odes however mention intelligence activities and the role of fundamental rights and freedoms.

Target audience of the document

The Romania government and citizenry.

Stated purpose of the document

- To outline the Romanian security strategy of promoting, protecting and defending national values (spiritual, cultural, material values defining the national identity) and interests.
- To synthesise various security aspects and priorities (including health, energy, food, infrastructure, financial, informational security).
- To redefine the Romanian security strategy aligning its priority with those of the EU and NATO (in view of the then recently gained membership).

Context of the document

The terrorist attacks of 11 of September 2001,other terrorist attacks that followed (London, Madrid) and the changes in international security priorities they brought about.
- The need to protect and defend democracy, the fundamental rights and freedoms of the citizen, assert national identity.

Documents referred to:

- None.

Key points in the document

The document outlines the premises and context of the new national strategy.
It underlines the importance of national security – a fundamental, indispensible condition for state and nation; fundamental objective and legitimate activity of governing powers; indispensable safeguard of democratic and fundamental rights and values.
It defines risks to security: military and non-military, external and internal.
It underscores the international character of security risks and the ensuing need for international action (EU, NATO and UN co-operation) and regional-strategic measures.
It underlines the importance of fundamental rights and freedoms as both indispensable condition for realising security objectives as well as objective of national security.
It defines the legitimacy framework for security activities.
It stresses the need to find a reasonable and efficient balance between the protection of freedoms and democratic rights and restrictions and punitive measures (e.g. by means of increased transparency and the right to information).
It introduces the concept of "democratic security".
It indicates that a systemic and pre-emptive approach to addressing security risks would be favoured.
It stresses the importance of good government (including the modernisation and democratic reform of relevant institutions) and that of economic and financial stability and better educa-

tion.
It indicates the need for a reform of the defence industry – including privatisation and increased international security co-operation, research and development activities.

Assessment of the importance or significance of the document
The document, drafted in 2006, outlined the Romanian security strategy. It formed the basis for defining the strategy of various ministries with responsibilities in this area.
In 2010, a new strategy (renamed "defence strategy") was defined.

(Evaluation on the basis of Google search hits, Romanian language results)

A Google search of "Strategia de securitate naţională" returned over 1,800 hits.
Many of the links were mirrors of the document, references in official documents and commentary (mostly critical) in the national press.

883. Maior, George Cristian, Director of the Romanian Information Agency, *Societate, Democratie, Intelligence, proceedings of a round table, year 5, new series, number 13, [Romanian Secret Service – round table on society, democracy, intelligence* 8 October 2008) Bucharest, December 2008. http://www.sri.ro/upload/intellspecial.pdf 58 Pages.

What domain (health, transport, policing, etc.) does it address?
Intelligence; National security.

(Surveillance, privacy are not mentioned.)

Target audience of the document
The intelligence community, academics, civil society.

Stated purpose of the document
To discuss the role of intelligence agencies in the 21st century.
To discuss the proposed strategy of the Romanian Intelligence Agency.
To redefine the democratic basis for the activities of said institution and increase its professionalism.

Context of the document
Rapidly changing international context.
New nature of (international) security threats.
Reform/modernisation of the intelligence agencies as a result of joining the EU, NATO.
Negative image of the intelligence agencies in Romania, in view of the communist past.
Terrorist attacks t the beginning of the 21st century (US, UK, Spain, Georgia).
The role of intelligence agencies, academics and representatives of the civil society to inform and provide analysis to (political) decision makers.

References in text:

- The writings of Paul Kennedy
- The film Spy Game
- The film The Good Shepherd
- The Bible
- The writings of Sherman Kent
- The writings of Vannevar Bush
- The National Foundation Project (US)
- The Memex project
- The Johnson Doctrine
- Sociological studies conducted by Georg Simmel
- Dimitrie Gusti, Cunoastere si actiune in serviciul natiunii
- The writings of Mircea Eliade
- Karl Popper, Objective Knowledge

Key points in the document

The document records presentations of participants / invited speakers.
The presentations addressed:
- the new conditions under which intelligence agencies have to operate (constant threat of ter-

rorist attacks, international scope and interdependencies); changes in modus operandi ; challenges encountered (personnel competence, reporting, selecting relevant information, financial constraints).
- the challenge to overcome a tainted communist past and poor public image.
- the contradiction between the secrecy which characterises conducting intelligence activities and the need for more transparency;
- the negative role of the media in covering excessively obsolete topics;
- the opinion that activities of the Romanian intelligence agencies constitute the most significant effort to safeguard the national security;
- the difficulty of defining who "the enemy" in the post-Cold War era;
- the importance of open source information/intelligence;
- the (cultural, organisational) challenges of inter-agency co-operation;
- the issue of oversight of intelligence agencies in democratic societies.

Assessment of the importance or significance of the document
Possibly very limited/no impact.

(Evaluation on the basis of Google search hits, Romanian language results)

A Google search of „Societate, Democraţie, Intelligence" returned 12 hits.

2.9 USA POLICY DOCUMENTS

889. Doyle, Charles, *Terrorism Legislation: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Congressional Research Service, Report, 26 October 2001. 6 pages

What domain (health, transport, policing, etc.) does it address? Security strategy (USA PATRIOT Act).
Target audience of the document US Congress.
Stated purpose of the document Not stated, but it is a factual account of the Act on the day of the Act's publication. It does not analyse the Act in terms of the Act's various Titles (sections), but in terms of several categories: wiretapping; other investigation enhancements; immigration; money laundering; and crime, punishment, and procedure. Through short paragraphs of commentary and bullet-pointed lists, it points out the legal implications of various provisions (e.g., the new powers granted and the new crimes created), and how they relate to other Bills and Acts in the intelligence and security field.
Context of the document The Act was passed on the date of this document. It was, and is a very controversial Act with a history of commentary, debate, and legal challenge. The Act was passed very quickly into law, only several weeks following 9/11. The document refers to other US laws and legal measures that the Act affects (e.g., what the Act amends, repeals, etc.). These include, for wiretapping: 18 U.S.C. 2510-1522, popularly known as "Title III"; 18 U.S.C. 2701-2711 or "chapter 121"; 18 U.S.C. 3121-3127 or "chapter 206"; and the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801-1863 or "FISA"; for money laundering: the Bank Secrecy Act, the Right to Financial Privacy Act and the Fair Credit Reporting Act. The document's summary explains as follows: 'The Act is a merger of two bills, S.1510, andH.R.2975/H.R.3108 which had earlier passed in their respective Houses. It melds the money laundering bill, H.R.3004. A variant of the House sunset provision survives, but adjustments to the McDade-Murtha Amendment concerning the adherence of federal prosecutors to local ethical standards do not.'
Key points in the document Because this document is not a policy document in the sense of contributing to policy-making or debate by putting forward a point of view, but is basically a commentary on and clarification of what some of the main provisions of the Act do (rather like the Explanatory Notes used in UK legislation when Bills are introduced into Parliament), the main points have been covered earlier on in this brief document analysis.
Assessment of the importance or significance of the document No obvious importance except as a digest for Congress (and for whoever reads it) of the Act. Why the document was a WikiLeak (of 2 February 2009) is not clear, unless the document was a purely internal one within Congress and not publicly available before then.

896. Belasco, Amy, Total Information Awareness Programs: Funding, Composition, and Oversight Issues, Congressional Research Service, 21 March 2003. 22 Pages.

What domain (health, transport, policing, etc.) does it address?
Privacy
- Data processing, government access to data

Surveillance
- Data mining and data analysis technologies, bio-surveillance, databases

Security
- terrorist attack prevention, funding for anti-terrorist measures, data accuracy security, protection of intelligence sources
-

Target audience of the document
US Congress

Stated purpose of the document
Total Information Awareness (TIA) Programs are the research & development efforts of the Defense Advanced Research Projects Agency (DARPA) to create terrorist detection tools. The TIA System is the consolidation of all the programs.

This report exists to clarify the funding, composition and oversights of the TIA Programs. Concerns expressed prior to the report and regarding the TIA Programmes referred to:
- discrepancies in the reported levels of funding from the TIA Office when compared to other sources
- crucial oversights and
- the programme's excessive potential impact on individual privacy .

This document follows on from the Consolidated Appropriations Resolution 2003[18] (P.L. 108-7), especially the section *Restrictions on TIA in FY2003.*

Context of the document
It follows from the previous paragraphs and it came about because of congressional debate about the TIA system (its funding, purpose, effectiveness etc).
The idea of a Total Information Awareness System started in 2001, prompted by the 9/11 terrorist attacks. The report is not a direct comment on the (measures following the) attacks, but rather a report on the formation of the TIA office.

Other documents referred to:
- CRS Report RL31730, Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws
- Wyden amendment
- Consolidated Appropriations Resolution (aka P.L. 108-7; 2003)
- Defense Department Briefing Transcript, November 20, 2002
- DARPA, RDT&E Descriptive Summaries for FY2003
- the Data Mining Moratorium Act (2003)
- Paper: Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results (1997)[19]

[18] This was a resolution which outlined funding limitations to the TIA programs
[19] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.44.5003

- Newspaper articles:
  - New York Times, "5,000 Al Qaeda Operatives in The U.S," February 15, 2003, and
  - Washington Times, "5,000 in U.S. Suspected of Ties to Al Qaeda," July 11, 2002

Key points in the document

This document is about the research and development efforts (called Total Information Awareness Programs) by the DARPA, for creating tools designed to "detect, anticipate, train for, and provide warnings about potential terrorist attacks". (p. 1). These tools would be consolidated to form a TIA System, originally intended to provide intelligence support to senior government officials. The report focuses mainly on the funding, composition and oversight of these efforts.

The author's main issue with regards to funding for the TIA Office (i.e the office which manages the budget for the TIA Programs and system), is the lack of transparency for what is actually being spent for TIA, more specifically for its two components: the 'TIA system' and 'TIA programs'. The programs are the R&D efforts which would be consolidated to form the TIA system. Moreover, the TIA office could use any other R&D efforts from DARPA that could contribute to the TIA system (for example, automatic language translation tools which have been in development since 1996). Therefore, the total amount spent is difficult to be calculated.

One key oversight outlined by the author is the lack of monitoring of collaboration between DARPA and the users of the TIA system, including law enforcement and intelligence communities. The author states that DARPA collaborate with several other Department of Defense (DOD) offices, as well as agencies outside of the DOD (such as the FBI and Homeland Security). This collaboration exists to pool resources on data processing technologies and databases for the TIA system. However, it is noted that the increasing collaboration would raise questions about the role of each agency.

Furthermore, the author writes that sharing information among several users (in this case, the users would be law-enforcement authorities and intelligence agencies) "makes it more difficult to protect both intelligence sources and the privacy of individuals" (p. 11). To counter this, DARPA is said to be developing technological systems to secure these vast databases. However, the author recognises that there are significant difficulties to develop such tools.

The author states that there have already been restrictions and requirements imposed on the TIA[20]. One of the requirements is a joint report by the Secretary of Defense, the Attorney General and the director of the CIA, outlining the planned spending, setting target dates, evaluating the likely effectiveness of the system and assessing the impact of its implementation on privacy.. Furthermore, the joint report must include laws that may be effected by the deployment of TIA, as well as the Attorney General's recommendations on how to minimise adverse effects of implementation on privacy and civil liberties.

Finally, the author notes the difficulties of identifying actual terrorists from 'false-positives'[21]. The author asserts that DARPA intend to develop sophisticated algorithms and

[20] These are outlined in P.L. 108-7

[21] "In credit card fraud, for example, a false alarm or false positive would mistakenly identify a transaction as fraudulent" (p. 15).

templates to identify suspect behaviour. It is predicted that there may be 200 false leads for every one correct terrorist identification. This is recognised as another oversight of the TIA system.

Assessment of the importance or significance of the document
This report was considered and used as a point of debate when undertaking the decision to terminate the TIA Programs and System[22]. It has therefore made a significant impact in the US Government.

(Evaluation on the basis of Google search hits, English language results)

A Google search for: Total Information Awareness Programs: Funding, Composition, and Oversight Issues returned over 77,500 results. This indicates that many websites have mentioned at least the Total Information Awareness Programs, but perhaps not this document in particular. The most popular category of websites that link to the document are those on U.S. Intelligence law.

When searching for those terms in quotations, it is narrowed to 8,000 hits. This document has been mentioned in several books on topics ranging from U.S. Intelligence Law, Terrorism Information Sharing, Data Mining, Cyber-crime and the Internet. A search on Google Scholar returned 8 results, which also pointed to the same books that a regular Google search did.

The document was referred to in a report by the Congressional Research Service (CRS) about Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress (2011). It was also referred to in another CRS report on Data Mining(2004), as well as one titled 'Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws' (2003). This indicates that the document has made some impact in Congress.

A search on the USA Governmental portal site (USA.gov) for "Total Information Awareness Program" + Funding + Oversight returns 13 results (narrowed down from 124 with the original search for "Total Information Awareness Program"), however all but one were not related to this specific document. This indicates that TIA programs are not often discussed on the record in the US government departments.

Overall, Google searches would indicate that the document has made more of an impact outside of the government, due to being popularly referenced in books and law websites. The minimal referencing of the document in governmental releases could imply that it has not been debated or discussed.

[22] http://www.fas.org/sgp/congress/2003/tia.html

943. 9/11 Commission, *The 9/11 Commission Report*, 22 July 2004. http://govinfo.library.unt.edu/911/report/index.htm 585 Pages.

What domain (health, transport, policing, etc.) does it address?

- Airport Security (technology, processes)
- National security (processes, departments)
- Terrorism (technology, methods, counter-terrorism)

Surveillance is mentioned with regards to its role in terrorist and counter-terrorism efforts, but what kind of surveillance used is not clearly defined.

Privacy is also mentioned, but more as a side-note that individual privacy should be respected and retained when amending National Security measures.

Target audience of the document

The President of the United Sates, the United States Congress and the American public

Stated purpose of the document

To present the "facts and circumstances relating to the terrorist attacks of September 11, 2001" (p. xv). It is also aiming to provide the fullest possible account of the events surrounding 9/11 and to identify lessons learned.

Context of the document

This document is brought about by the terrorist attacks of 9/11 in New York. It is an extensive examination of the past, present and future of America's security in the face of terrorist attacks.

Documents referred to:

- National Commission on Terrorist Attacks Upon the United States (Public Law 107-306, November 27, 2002)
- The Foreign Intelligence Surveillance Act
- Goldwater-Nichols Act (1986)
- Nunn-Lugar-Domenici Domestic Preparedness Program
- International Emergency Economic Powers Act
- The USA Patriot Act (2001)
- Memorandum of Notification on Bin Ladin
- Survey of Intelligence Information on Any Iraq Involvement in the September 11 Attacks (2001, September 18)
- Preventing More Events (2001, September 17)
- Operation Enduring Freedom
- White House record, Situation Room Communications Log, Sept. 11, 2001.
- NSC memo, Summary of Conclusions of Deputies Committee Meeting (held by secure teleconference), Sept.11,2001.
- Intelligence report, interrogation of KSM, May 10, 2003.
- NSC memo, Summary of Conclusions for Principals Committee Meeting Held on September 13, 2001.
- DOS cable, State 158711,"Deputy Secretary Armitage's Meeting with General Mahmud: Actions and Sup-port Expected of Pakistan in Fight Against Terrorism,"

Sept. 14, 2001
- CIA memo, "Going to War,"Sept.15,2001
- Richard A. Clarke, Against All Enemies: Inside America's War on Terror (Free Press,2004)
- New York Times (1999). U.S. Hard Put to Find Proof Bin Laden Directed Attacks.
- Analysis of Aircraft pot
- Study for DCI by Robert Gates (1992)
- Article 3 of the Geneva Conventions
- Aviation and Transportation Security Act
- Homeland Security Act
- Maritime Transportation Security Act
- American National Standard on Disaster/Emergency Management and Business Continuity Programs
- National Preparedness Standard

Key points in the document

Chapter 1: This chapter covers mostly eyewitness accounts of the events that took place on 11th of September, 2001, starting with the first hijacking of American Airlines flight 11, and the reactions of all the officials involved. It emphasises the restrictions in communication between all the involved organisations (e.g. United airline, American Airlines, the Federal Aviation Administration etc.).

Chapter 3: This chapter widely covers the state of affairs pre-9/11 between the different government sectors that, in one way or another, dealt with counter-terrorism. There is once again emphasis on the difficulty of sharing information, where the paradigm of those times was to protect rather than disseminate/share information. The limited authority of each of the committees and agencies is also stressed.

Chapter 6: Discusses the funding that the CIA had for counter-terrorism, prior to 9/11 they still believed they were being underfunded. It also links back to the lack of information flow, where the Office of Foreign Assets Control was unable to freeze most Al Qaeda assets (prior to 9/11) due to this. There were also changes proposed to border control which included tighter security, increased surveillance and trans-organisational information flow. However, these were only beginning to be implemented before 9/11.

Chapter 10 : This chapter begins to touch on the issue of international cooperation in intelligence matters. The post-9/11 stance of the U.S was clarified: all resources would be dedicated to eliminate the threat of terrorism and punish those responsible for 9/11 (and those who harbor the responsible). In order to do this, the US intended to work with a coalition (including warlords) to eliminate terrorist groups and networks. This chapter also notes the US intent to avoid malice toward any people, religion, or culture.

Chapter 11: This chapter looks at 9/11 with the benefit of hindsight. It is noted that prior to the attacks, most intelligence agents did not have security clearance to access the intelligence on al Qaeda. Therefore, many were unaware of the hunts for and arrests of al Qaeda operatives until post-9/11. It is once more emphasised that the various departments did not have the possibility to link intelligence, sometimes inadvertently or due to legal misunderstandings. Information could also get lost in the handoff between foreign and domestic agencies. . The chapter goes on to suggest far-fetching solution for the future, such as finding ways to 'bu-

reaucratise imagination'[23] to prevent surprise attacks.

Chapter 12: Identifies the threat to be specifically *Islamic* terrorism, where politics and religion are not separated, and there is no common ground on which to negotiate. Recommendations specific to combating Islamic terrorism are made. These include the sharing of terrorist information across borders, cooperation in assisting Islamic nations to become more democratic, with specific focus on Afghanistan, Saudi Arabia and Pakistan.

Border security was also noted to become a national security measure. This is where the notion of biometric screening at borders is raised. It is recommended that the biometric information be checked not only against criminal and immigration records, but also financial. The department of homeland security and Transportation Security Administration are the departments expected to implement the checks/screening.

Chapter 13: Finally, recommendations on a restructuration of different government departments are laid out, all with the goal of enabling information (intelligence) flow. Incentives should be provided for information sharing between agencies. Congress is also thought to need a role in overseeing intelligence, as well as homeland security. The role of the FBI has been outlined to mainly specialise in surveillance.

Overall, there is a lot of emotive language used in this document (for example "a day of unprecedented shock and suffering in the history of the United States." Pg. xv). This language paints a clear picture of the frame of the authors. They state that "America stood out as an object for admiration, envy, and blame" (p. 340), which shows that the authors tried to find justification for the attacks, from an American point of view. Also, each of the relevant chapters emphasised the confusion of roles and lack of information sharing between American intelligence agencies.

The main point of the authors is that if the situation were different (if information flowed freely, if the departments knew exactly what their role was), 9/11 perhaps could have been avoided. This primes the reader to positively receive recommendations for increased sharing between governmental departments, both nationally and internationally. From the text, one can say that the events on 9/11 caused a paradigm shift, from valuing the protection of information, to openness and sharing across all departments.

Assessment of the importance or significance of the document

(Evaluation on the basis of Google search hits, English language results)

A Google search of "THE 9/11 COMMISSION REPORT" returned over 3.2 million hits. Many of the top links were just mirrors of the .pdf of the full book, or links to online stores where you can purchase the report. It is interesting to see that links which are not mirrors or stores, are links to websites and reviews that are very critical of the report.[24] Some reviews are from major websites like Harpers. Some links are to other books about the omissions and distortions from the official report.[25] The reviews displayed on popular American sites like

[23] "It is therefore crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination." (p. 344)
[24] One of the top 10 links was: http://www.911truth.org/article.php?story=20050523112738404

[25] http://www.amazon.com/The-Commission-Report-Omissions-Distortions/dp/1566565847

Amazon and Google books are more towards the positive side, for example "very informative and very thorough".[26]

A search on Google Scholar for the same text returned over 5,700 hits. Only the top link was a mirror to the online book. Thus the Google Scholar search was able to give a great overview on the popularity of the 9/11 Commission Report as a source, when authoring other books or journal articles. The type of documents which cited the report were varied, for instance; a report on the fragmentation and lack of information sharing within the report,[27] the implications of the recommendations on world politics,[28] the rise of premeditation with the 'war on terror',[29] and even arguments about the way the report was written to bring down barriers between personal and national experience.[30]

Since its release eight years ago, The 9/11 Commission Report has had a huge impact especially in the US: authors, reviewers and assignors; the general public; the US Government; the traditional and new (internet) media, popular culture.

The report has led to:

- New legislation pending following the recommendations in the report
- The reorganisation of intelligence agencies
- A change in priorities of law enforcement and intelligence agencies
- Many referrals in other (legal) texts
- Etc.

[26] http://books.google.nl/books/about/Nine_eleven_Commission_Report_Final_Repo.html?id=JufWziTyNnIC&redir_esc=y

[27] http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9299.2006.00002.x/abstract

[28] http://mil.sagepub.com/content/33/3/827.short

[29] http://sdi.sagepub.com/content/39/2-3/155.short

[30] http://journals.cambridge.org/action/displayAbstract;jsessionid=0035639B1544FBB1D3DA64C58763288B.journals?fromPage=online&aid=1379464

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