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 3.2: Privacy and security in key EU and International policy documents: Updated overview

Authors:	David Bernard-Wills, David Wright (Trilateral)
Reviewer:	Charles D. Raab (University of Edinburgh)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	31 March 2014
Submission date:	17 April 2015

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)

Document history

Version	Date	Changes
1.0	17 April 2015	

CONTENTS

EXECUTIVE SUMMARY

Deliverable 3.1 of the PRISMS project reviewed policy documents related to privacy and security in the EU, the USA, international organisations, and a sample of EU Member States from 2001 to 2012. Using the search terms "privacy" and "security", as well as closely related terms and keywords such as "surveillance" and "data protection", Deliverable 3.1 reported the results of the analysis of 56 documents selected from a long list of 983 documents; the methods used in this process was described at length in that Deliverable. This update report builds upon the findings of the first deliverable, and includes an updated list of policy documents related to privacy and security published since the first report in March 2013 and the time of writing in February 2015. This report reviews the key findings and claims made in Deliverable 3.1; identifies 141 new, relevant policy documents; and assesses the findings and claims against a sample of nine of the new policy documents to see if the policy documents published during the study period reflect major changes, a period which coincides with the Snowden revelations about the intelligence services' conduct of mass surveillance. As with the previous study, the aim of the review is to provide insight into the way concepts of privacy and security are used in European and other policy contexts, and also to inform the survey research and decision support tools to be developed in the PRISMS project. The report examines nine key policy documents in detail. For each it provides a summary of the content and context of the document followed by an analysis in terms of security, privacy, the relationship between those concepts, technology, surveillance other factors.

The review finds some marked discursive changes between the sample of policy documents included in this updated report when compared with the policy documents covered by the initial analysis. Whilst some trends remain constant, there are noticeable changes, which may be traceable to the Snowden revelations and the resulting public attention and political fallout. Several of the analysed policy documents serve to open up the rhetorical space around the concepts of privacy and security. In brief, they do this by exploring the ambiguity of security (including the increasing prominence of information security as a component part of contemporary security) and the contingent ways in which surveillance is understood as contributing towards security. In this context, the traditional opposition between security and privacy is increasingly challenged.

The most substantial difference is the prominence given to the digital mass surveillance. This greater focus actually allows for a more nuanced, if contested, model of what surveillance (and particularly mass surveillance) is. Several documents demonstrate the emergence of a narrative of the need for a "re-balancing" between security and privacy. A new topic emerging in these documents, in part as a response to the political problem of digital mass surveillance is the extent to which the European Union has any competency with regard to national intelligence services. The difficulty of achieving accurate understanding of surveillance and intelligence activities is explicitly raised in several texts. Privacy-enhancing technologies, and economic and technological methods for increasing privacy and information security for citizens, even in the absence of a policy or regulatory shift, are the subject of detailed discussion, whereas these were particularly absent in early policy discussions. Finally, the relationship between the EU and the US is described in a different, more cautious and potentially competitive manner.

1 INTRODUCTION

Deliverable 3.1 of the PRISMS project conducted a review of policy documents related to privacy and security in the EU, the USA, international organisations and in a sample of EU Member States (the Netherlands, France, Germany, Italy, Romania and the UK) from 2001 to 2012. [1] The aim of the review was to provide insight into the way the concepts "privacy" and "security" were used in European policy and also to inform the survey research and decision support tools to be developed in the PRISMS project. Security and privacy are concepts that regularly feature in policy documents. The way that these concepts are framed, understood and communicated between political actors has implications for the politics of security and privacy, particularly in the ways that these concepts are embedded into policy and regulation. Policy documents are part of the way that government, broadly conceived and including intergovernmental actors, reflects upon, co-ordinates and seeks justification and legitimacy for its activity.[2] The way that these concepts, and closely related ones such as "surveillance" and "data protection" are articulated in policy documents also acts as important reference points for other actors. An analysis of the patterns and regularities in the language of privacy and security is part of the identification of structures of policy language and discourse, and particular political ways of understanding and constructing the world.[3]

Deliverable 3.1 of the report on this review included a discussion of 983 identified policy documents, including many from international and non-EU European organisations, short analyses of 56 selected documents of high importance, and a horizontal analysis of these documents showing how security and privacy were framed within European policy discourses, identifying salient differences between countries and over time that could be discerned based upon the sample of documents. The second part was a critical discourse analysis of a smaller number of selected British, Dutch and EU policy documents, which pursued the question of framing in more detail...[4] This update report builds upon the findings of the first deliverable, and includes an updated list of policy documents related to privacy and security published since the first report March 2013 and the time of writing in February 2015.

This period included the series of media stories based on the revelations of mass surveillance and document leaks from NSA contractor Edward Snowden.[5] These events, and the resulting public and political attention, demonstrate a changed context that is directly relevant for policy documents relating to privacy and security. They offer an opportunity for either the

[1] Bodea, Gabriela, Noor Huijiboom, Sander van Oort, Merel Ooms, Bas van Schoonhoven, Tom Bakker, Livia Teernstra, Rachel L. Finn, David Barnard-Wills, David Wright, Charles D. Raab, *Deliverable 3.1,Draft Analysis of privacy and security documents in the EU and US: Part I an overview of privacy and security policy documents in the EU, six Member States and the United States,* PRISMS project, 28 March 2013 , http://prismsproject.eu/wp-content/uploads/2013/05/PRISMS-D3-1a-policy-docs-13-March-13-FINAL.pdf

[2] Barnard-Wills, David, *Surveillance and Identity: Discourse, Subjectivity and the State*, Farnham, Ashgate, 2012, p.170.

[3] Philips, Louise, and Marianne W. Jørgensen, *Discourse Analysis as Theory and Method*, London, Sage, 2004, p.2, Chouliaraki, Lilie & Norman Fairclough, *Discourse in Late Modernity: Rethinking Critical Discourse Analysis*, Edinburgh, Edinburgh University Press, 1999, p. 1

[4] A version of the horizontal analysis was subsequently published as Barnard-Wills, David, "Security, Privacy and Surveillance in European Policy Documents", *International Data Privacy Law*, 3(3), 2013, pp.170-180, [4], whilst the discourse analysis informed Huijboom, Noor & Gabriela Bodea, "Understanding the Political PNR-debate in Europe: a Discourse Analytical Perspective", *Perspectives on European Politics and Society*, Published online, 14 Jan 2015.

[5] For a timeline compiled by the Open Rights Group, see:
https://wiki.openrightsgroup.org/wiki/Guardian_and_Snowden_revelations_2013

reconfirmation and shoring up of existing discourses, or for the emergence of new or different ways of articulating privacy and security, particularly in the context of mass surveillance. This context has informed the selection of particular policy documents. Deliverable 3.2 can therefore also be seen as an analysis of the reactions to these revelations as reflected in policy documents.

The objectives of this report are to:

- Review the key findings and claims made by the initial policy document review. These are summarised below, in section Two.
- To identify new, relevant policy documents published between the first deliverable and the present (March 2013 to February 2015)
- Check the older findings and claims against a sample of the new policy documents to see if they still hold, or if there have been major changes in the policy documents published during the study period. A summary of the key policy documents is provided in section Three. The findings of the collective analysis are presented in section Four.

Throughout the PRISMS project, the focus has been upon the concepts of privacy and security and the nature of their inter-relation. Many of the policy documents included in the review have significant implications for other concepts and issues (for example the relationship between security, surveillance and freedom of expression, which became particular prominent later in this period). However, the present review is a more focused one, and for reasons of space does not encompass these discussions.

Criteria for selecting documents

The selection of documents for this report focused on the European and international-level policy institutions, and searched for documents produced by the same institutions and bodies as in the first report. These are documents that are most relevant to the analysis of the pan-European survey in PRISMS as well as the decision support system. The search criteria included documents that relate to one or more elements of the policy process in various sectors in which privacy and security play a major part. Documents are related to decision-making and action, including policy formation, implementation or evaluation, by governments or other authoritative bodies (including international ones). International organisations were included because of the participation of the EU and its Member States in those bodies. The key criterion for analysis was that a policy document emerges from a major EU or international bodies on the topic of privacy and security.

This analysis contains no single-country documents (and as part of this no documents from the USA). The focus is instead upon the EU discussion, which appears (from the first analysis) to be at a significant point in relation to the relationship between privacy and security, but also influential on other actors. The horizontal analysis found evidence for the influence of European policy discourses on those of Member States, support a restricted focus upon EU and international organisations in this analysis. There is a significant emerging politics in this period as the EU comes to terms with the Snowdon revelations, in different ways in different sections of the EU policy-making structure. Given the status of the organisations that produced them, as well as the effort put into their production, many of the documents selected for analysis could not have been ignored in any meaningful analysis of the relationship between security and privacy in European and international policy

documents. For several organisations, these texts represent the most detailed and specific statement on the relationship during this period (rather than a mention in passing in the context of another policy issue). The in-development DSS will itself operate in a EU context and is being designed at that level. In addition the first sample suffered from small samples at the M/S level. However, its generalisation about EU-level activity is more reliable. It is worth continuing this trend here, given the limitations upon what it impossible to analyse, and what it is possible to adequately contextualise. The analysis here moves away from spending too much attention on the conceptualisation of security in the absence of privacy. In the initial sample, privacy was absent in many defence-centric texts, and security-related texts outside of the context of information- or cyber-security, making analysis of how those sectors perceived the relationship between security and privacy somewhat speculative (although highlighting this absence is an important finding and is reflected in the purpose of the PRISMS decision support system). The analysis should acknowledge that in many such texts, privacy is still likely an ellipsis or rhetorical elision. This report does not include court cases and legal findings in this study (for example the European Court of Justice Ruling on the EU Data Retention Directive in April 2014), nor does it include legislation (although it does include a document containing both a European Parliamentary Resolution and its extensive, relevant explanatory notes). Court cases and legal findings have been addressed in the legal analysis work package and resulting publications.[6] Further, the analysis excludes newspaper, media and academic documents, even those commenting on the Snowden revelations or on other policy documents.

[6] González Fuster, Gloria, Serge Gutwirth, Bernadette Somody, Iván Székely, *Deliverable 5.2: Consolidated legal report on the relationship between security, privacy and personal data protection in EU law*, PRISMS project, 19 December 2014. http://prismsproject.eu/wp-content/uploads/2015/02/PRISMS-D5-2-Consolidated-legal-report.pdf

2 SUMMARY OF THE FINDINGS OF DELIVERABLE 3.1

This section provides a summary of the key findings from the initial policy document analysis. Further detail can be found in the report itself. It should be noted that these findings are dependent upon the methodology used.

Procedurally, policy documents in this field appear to be produced with the following stated motivations:

1. As responses to legislative requirements, processes or consultations
2. Responses to changing security contexts or the emergence of new security threats
3. Responses to particular events or identified public concerns
4. Reminders or re-affirmations of principles or clarifications of laws
5. The results of scrutiny, inquiry or evaluation of existing policies and programmes
6. Responses to increased surveillance practices and technological developments over a longer term (often associated with 3).

The broadest finding emerging from the horizontal analysis was that, at least in terms of policy documents, there were significant differences in focus, emphasis, and key threats related to understandings of both privacy and security in different countries, although there were also strong commonalities. Different European Member States appeared to focus upon different aspects of security in their policy documents, which would support an analysis of these states as having (at the same time) different security contexts to which policy is seen as needing to respond, different insecurity perceptions, as well as different internal security policy cultures. For example, the UK shared with other European states an analysis of the international security climate (post-cold war, increasing importance of non-state actors, terrorism and other shared sources of instability), but it had a particular focus upon the security situation in Northern Ireland that was not shared by other EU states. Although concepts of security were heterogeneous, there was a relatively stable core of what were seen as security threats, and the concepts were all more expansive than traditional concepts of national security, with multiple areas of life seen as contributing to security. Concepts and definitions of security increasingly included information/cyber security.

The EU position on the conflict between security and fundamental rights (including privacy) seemed to be that these were complementary, rather than in contradiction. Both are rights to be respected. This complementary formation is relatively recent, and the more familiar language of "balancing" between security and privacy, which may be seen as a trade-off, was seen in documents at national levels. A "balance" is heavily dependent upon context, as it can serve as a justification for security measures, even if they impact upon privacy. Whilst there was a commonly articulated and strong consensus on what privacy is, at least within policy, particular issues appeared to have had increased salience as threats to privacy in some countries in comparison to others. For example in the UK, the state was the key threat in policy documents, in Germany it was law enforcement, and in Italy the private sector.

Broad principles involved in privacy, data protection and surveillance include proportionality, accountability, transparency, trust, consent, and the rights of the data subject. "Technological determinism" was commonplace even though solutions to privacy problems are less likely to be technological rather than policy, legal, or regulatory, or involve individual responsibility to taking steps to preserve individual privacy.[7]

[7] "Technological determinism" is the theoretical model that holds that technologies strongly impact upon (or determine) the direction of social change. This position often underplays the role that social choices, institutional

The discourse analysis

The second part of the D3.1 study involved a discourse analysis of selected Dutch, British and EU policy documents.[8] The approach understood a "discourse analysis" to be a scientific approach to the analysis of texts, based upon a deconstructive reading. The approach was focused upon identifying the epistemological and ontological assumptions, as well as the motivations and interests, behind a particular text. The approach that was used focused upon story lines, metaphors, and key actors. A "story line" is a condensed statement summarising complex narratives, used by people as shorthand in discussions.[9]

The findings from the discourse analysis were broadly supportive of the findings from the individual and horizontal analysis earlier in the study. In addition, the UK case identified four key discursive regularities: the concept of the "surveillance society", finding a proportionate balance between security and privacy, the associated social benefits of surveillance and security, and supporting the surveillance industry. The analysis suggested that UK policy documents, in contrast to EU sources, were concerned with the development of surveillance, but also tended to use the "balancing" metaphor, constructing privacy and security as oppositional concepts in tension. The Netherlands case found that the framing of security and privacy was strongly dominated by terrorism and strongly influenced by particular critical events, including the assassination of Theo Van Gogh and the 9/11 terrorist attacks in the US. Security and privacy occurred primarily as separate debates, with relatively little intersection between them until around 2007, when they began to converge. The discourse also became more detailed over time with a focus upon specific issues within privacy.

The EU discourse analysis is most pertinent for this study update. Again, the EU discourses on privacy and security were strongly influenced by the 9/11 attacks. Many of the debates analysed involved the mediation of positions between the US government, the European Commission and the European Parliament over the issue of access to sensitive data on European citizens. The analysis suggested that US statements and proclamations on security were quite influential over EU policy documents in that period. Key themes were combating terrorism, passenger name records, and the Stockholm Programme setting out the EU's priorities for the area of justice, freedom and security.[10] The 9/11 attacks were framed as an attack on western (including European) values and provided a sense of urgency for measures to combat terrorism. Debates in the European Parliament were also important in this field, and reflected some criticism of elements of the counter-terrorism measures, particularly the provision of airline passenger name details to the US authorities. Fundamental freedoms were

---

policy and discourses have on technological development, and that pre-existing or indigenous factors may be absorbed by technological capacities. It is often (but not necessarily) linked to belief in the efficacy of technology. See Heilbroner, Robert, L. "Do Machines Make History?" in Robert C. Scharff & Val Dusek (eds), *The Philosophy of Technology: The Technological Condition*, Oxford, Blackwell, 2003 and Lyon, David, *Surveillance Studies: An Overview, Cambridge,* Polity, 2007, p.54

[8] Bodea, Gabriela, Noor Hujiboom, Sander van Oort, Merel Ooms, Bas van Schoonhaven, Tom Bakker, Livia Teernstra, Rachel Finn, David Barnard-Wills, David Wright, Charles Raab, *Deliverable 3.1: Draft Analysis of privacy and security policy documents in the EU and US: Part II, a discourse analysis of selected privacy and security policy documents in the EU*, PRISMS project, 28 March 2013. http://prismsproject.eu/wp-content/uploads/2013/05/PRISMS-D3-1-part-II-discourse-analysis-FINAL.pdf

[9] Hajer, Maarten, "Coalitions, practices and meanings in environmental politics: from acid rain to BSE", in Howard, D. & J. Torfing, (eds), *Discourse theory in European Politics: Identity, policy and governance,* Basingstoke, Palgrave-Macmillan, 2005, p.304

[10] European Council, The Stockholm Programme – An open and secure Europe serving and protecting citizens, OJ 2010/C 115/01, 4.5.2010, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010XG0504%2801%29&from=EN

invoked on both sides of this debate. The analysis found that after 2009 a discourse coalition had emerged, that emphasised the importance of protecting European citizens' data beyond the EU borders, and perhaps demonstrating a shift towards the privacy side of security-privacy trade-off. The analysis also noted that in many cases in EU discourse, "privacy" was narrowed down to "data protection", whilst security discourses had become more fully embedded in institutional police practices.

3 SUMMARY OF KEY POLICY DOCUMENTS IN THE RECENT PERIOD

This update report now examines nine key policy documents. For each it provides a summary of the content and context of the document followed by an analysis in terms of security, privacy, the relationship between those concepts, technology, surveillance, and other factors based on the analysis of the documents. The texts are presented in chronological order.

3.1 INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, RESOLUTION ON ANCHORING DATA PROTECTION AND THE PROTECTION OF PRIVACY IN INTERNATIONAL LAW, SEPTEMBER 2013[11]

The text of this Resolution was agreed by the participants at the 35th International Conference of Data Protection and Privacy Commissioners, held in Warsaw in 2013. The ICDPPC is the annual gathering of the heads of data protection authorities and similar organisations from around the world, and the Resolution was one of four passed in 2013. ICDPPC Resolutions are not legally binding but reflect the shared position of data protection authorities. The short (two-page) text starts by recalling previous Resolutions of the Conference that bear upon the issue of data protection and privacy in international law, including previous calls for international standards, and attempts at binding international agreements. The text also recalls existing international law instruments.[12] The Conference Resolution identifies the need for a binding international agreement on data protection and proposes the addition of a protocol to Article 17 of the International Covenant on Civil and Political Rights based on standards developed by the Conference in order to create globally applicable standards for data protection and the protection of privacy in line with the rule of law.[13]

Analysis

Privacy is articulated in this text as a fundamental human right, enshrined in some international agreements (Article 17 of the ICCPR), but lacking complete and formalised international consensus. Protection of personal data is closely linked to privacy, seen as part of protecting privacy, and automated processing of personal data is constructed as a threat to privacy. Privacy is also closely linked to family, home and correspondence. If privacy is infringed, this should not be unlawful or arbitrary,[14] and there are several constraints upon the processing of personal data about people, including regulation by law, effective security, and the rights of individuals to determine what information is held about them.

Security is mentioned very briefly as a competing interest that can be opposed to privacy. The content of security is not defined in this text, and there is no account of security threats. The text does use "balancing" terminology in claiming that the right balance needs to be struck between human rights to privacy and personal data on one side, and security, economic

[11] https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf

[12] 35th International Conference of Data Protection and Privacy Commissioners, Resolution on anchoring data protection and the protection of privacy in international law, Warsaw, 26th September 2013, p.1 https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf

[13] Ibid, p. 1

[14] Ibid, p. 2

interests and freedom of expression on the other. Information security is discussed, but in the terminology of the "integrity of networks".[15]

The stated motivation for the text is that it contributes towards on-going work in the area of international standards for data protection; it is therefore a reaffirmation of existing principles and a call to action in support of these (and as a result, a call for privacy). It does not provide substantial coverage of the context for this need: it does not, for example, refer to the Snowden revelations, the first of which had been in the public domain for three months at the time of the Conference. The text does not mention particular countries, other than a footnote mentioning that the United States Federal Trade Commission abstained from voting on this Regulation. The text is fairly orthodox: it uses "balancing" terminology, but privacy is seen as a fundamental right.

3.2 European Parliament, National Programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, October 2013[16]

This text is a study conducted the Centre for European Policy Studies (CEPS) at the request of the European Parliament's committee on Civil Liberties, Justice and Home Affairs (LIBE), following from the Snowden revelations, into the surveillance practices of the UK, Sweden, France, Germany and the Netherlands. The study includes an initial analysis regarding surveillance, data protection and national security, and an analysis of the surveillance capacities and abilities of five EU countries. It concludes with an analysis of how EU competencies and institutional powers may apply to such programmes. They key conclusions of the report are that recent media reports have revealed a reconfiguration of surveillance on a scale previously unknown; that the breadth of this surveillance raises questions about its legitimacy; and that there does not appear to be adequate accountability for intelligence services in this regard.[17] The study of particular EU states finds surveillance programmes operating in several of them, and that these programmes can be engaged with through EU law mechanisms.

The report discusses the scope of surveillance, based upon the documentary sources made available through media reporting, including the access and processing of EU citizens' data by the US National Security Agency (NSA) and others on a large scale. This surveillance was done through access to Internet cables and servers of US-based private companies; co-operation of the United Kingdom's signals intelligence agency GCHQ with the NSA; and the subjection of EU institutions to US-UK spying.[18] A particular consequence of note from this is that EU citizens' data appear to be accessed and analysed by US intelligence agencies without any legal framework for remedy.[19]

[15] Ibid, p. 1
[16] Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi & Armandine Scherrer, *National Programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, European Parliament, October 2013.
http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf
[17] Ibid, p. 5
[18] Ibid, p. 7
[19] Ibid, p. 9

Regarding EU surveillance operations, the report finds that, based upon publicly available information, the UK, Sweden, Germany and France are engaged in large-scale interception and processing of communications data, including practices that involve directly tapping into communications infrastructure. It also finds that the activities of the other three countries are smaller than those of the US and UK; that there are multiple intelligence networks that are overlapping and transnational; that legal frameworks can be ambiguous in relation to mass surveillance; and finally that oversight bodies have limited capacity.[20]

On legal modalities of action at EU level, the study finds that surveillance programmes in the EU Member States are incompatible with minimum democratic standards of the rule of law as derived from the EU Charter of Fundamental Rights (CFR), and the European Convention on Human Rights (ECHR); that the concept of national security in EU law, as applicable to national surveillance programmes, is strictly delineated by Fundamental Rights commitments. ; Member States' surveillance programmes jeopardise the EU principle of "sincere cooperation" (Article 4.3 of the Treaty on the European Union) as well as the privacy of EU nationals; large scale electronic surveillance blurs the line between national security and that the boundary between domestic and foreign intelligence is also blurred by data exchange between national services.[21] The impacts on the security of EU institutions (the Commission, the Parliament) and the use by some of these (Frontex, Europol) of data shared by national security agencies brings these matters within the ambit of EU competencies.

The study makes nine policy recommendations for the European Parliament to exercise its responsibility to safeguard the rights of EU citizens.[22] The study recommends that the European Parliament should use its powers to suspend the Terrorist Financing Tracking Programme (TFTP), reschedule the Transatlantic Trade and Investment Partnership (TTIP) negotiations; to launch an enquiry to require explanations from the US; and to further investigate EU Member States' collaboration with the NSA. It argues that the EU should set a professional code for the transnational management of data, which would set out "red-lines" and best practices for intelligence agencies; that the European Parliament should submit a proposal on limiting the actions of private contractors while keeping in mind the free circulation of the Internet and the possibility of a European Privacy Cloud;[23] and that it should ensure that key provisions in the Draft Data Protection Regulation (Article 43a on international transfer of data, Article 79 sanctions) are maintained during negotiations with the Council.[24] It urges the development of a EU policy infrastructure capable of proving effective follow up to intelligence revelations; the exercise of its powers to promote minimum standards set by the European Court of Human Rights (ECtHR);[25] more scrutiny and monitoring of EU home affairs agencies (Europol) in the field of security and information exchange; the exploration of the potential for EU-level protection for whistleblowers; and finally the commissioning of further research on large scale surveillance practices by EU Member states.[26]

[20] Ibid, p. 19
[21] Ibid, p. 27
[22] Ibid, p. 42
[23] Ibid, p. 44
[25] Ibid, p. 46
[25] Ibid, p. 46
[26] Ibid, p. 47

Analysis

The study is explicitly critical of the reduction of the analysis of European surveillance programmes to a question of a balance between data protection versus national security. For the authors the very scale of surveillance means that the issues should instead be framed in terms of collective freedoms and democracy.[27] The authors state that "if derogations to data protection exist, national security cannot be a justification for the structural transformation of the rule of law and democratic expression of civil societies in an open world of information."[28]

The study examines strategies apparently used by intelligence agencies to avoid the accusation of privileging security over liberty. These strategies include arguing that European partners are aware of the surveillance; that surveillance has been strictly limited to counter-terrorism operations; that surveillance takes place on a small scale, or that large scale data collection is used to confirm information gathered through other means (and is therefore not data-mining); and that operations are conducted for cyber security and cyber defence and are therefore part of national security. The nature of these strategies suggests that the report's authors believe that privileging security over liberty is an explicit strategy and not just a feature of the language used. The strategies discussed are about arguing or demonstrating that the privileging of security over privacy is legitimate and legal in these contexts, not that no such trade-off has been made.[29]

Threats to privacy in this text are primarily from large-scale surveillance as conducted by state intelligence agencies. The study considers that access to data is an invasion of privacy in itself, and in this particular context turns all citizens into potential suspects. There are also other non-privacy threats arising from the same source, including impacts upon the fairness of competition between EU and US companies,[30] and the risk to the EU of being subject to a strategy of "full spectrum dominance" by the US under cover of international collaboration on counter-terrorism and law enforcement.[31] This is very distinct from the strong sense that international EU-US co-operation was almost inherently supportive of security, which was evident in the first documentary analysis.

Security is discussed in this text in relation to its legal framing, rather than as a protection against particular threats. The concept of national security is linked to an existing legal framework (particularly ECHR case law and the EU Charter), which is seen as giving this concept meaning, setting it's conceptual boundaries, and legitimacy through compliance with the framework. The security of EU institutions is seen as being potentially violated and put at risk by intelligence agency surveillance.[32] The discussion of surveillance and the concept of "sincere cooperation" also a raises a discussion of the risks to the security of EU citizens, institutions and the Union as a whole, and how particular activities of intelligence agencies might put this into conflict with the national security activities of Members States.[33] This is a relatively traditional, if supranational understanding of security. In addition to being a threat to privacy, large-scale surveillance is also constructed in this report as a threat to various

[27] Ibid, p. 5
[28] Ibid, p. 18
[29] Ibid, p. 18
[30] Ibid, p. 8
[31] Ibid, p. 17
[32] Ibid, p. 27
[33] Ibid, p. 35

forms of security. The report states: "The violations of democratic rule of law and fundamental rights inherent to large-scale surveillance, and their supranational nature and fundamentals, affect the security of the Union as a whole."[34]

The study report provides quite a nuanced and complex concept of surveillance, in part as a result of trying to understand the extent of surveillance activity. It describes a "reconfiguration of surveillance" in terms of scope and capacity due to developments in technological capacity that allow for more data to be collected. It also draws a distinction between targeted surveillance (which can be legitimate if framed within the law) and large-scale, mass, untargeted surveillance. A key distinction is a shift from targeted surveillance to "non-centralised and heterogeneous assemblage of forms of surveillance".[35] It argues that the purpose and scale of surveillance are what differentiates democratic and police states.[36] Large-scale surveillance has two controversial elements: a technological question about what such technologies can do, and political question about their use.[37] Although the legal and theoretical scope of surveillance can be identified, this report also raises epistemological questions about the knowledge of the extent and nature of surveillance, particularly the targets of surveillance and the collection, filtration and analysis of data.[38] The report also highlights several methodological issues that complicate the gathering of data in this field and the production of a clear analysis.[39] The report's authors acknowledge that information and time constraints preclude even a clear analysis of the controversy and public debate.[40] [41] The second recommendation of the report, for a professional code, does some substantial work on setting out a framework for what would constitute a legitimate surveillance activity. Surveillance activity must have sufficient sustainable cause and integrity of motive; it must use proportionate methods, have right and lawful authority, and a reasonable prospect of success; the recourse to secret intelligence must be a last resort, and different lifestyles should not be confused with suspicious criminal activity. [42]

Although the LIBE committee of the Parliament requested the study[43], its authors provide a normative motivation in the statement that the Snowden revelations reveal something hitherto unknown about the scale and scope of intelligence agency surveillance, including of EU institutions, which requires some reflection and intervention. The report's authors associate inaction in this context with a loss of trust and confidence.[44]

[34] Ibid, p. 35
[35] Ibid, p. 8
[36] Ibid, p. 5
[37] Ibid, p. 9
[38] Ibid, p. 6
[39] Ibid, p. 9
[40] Ibid, p. 11
[41] For example, the inadequacy of intelligence oversight is determined by the low staffing level of various Member State oversight bodies..
[42] Bigo, et al, 2013, op. cit., pp.43-44
[43] The views put forward in the study report are therefore the views of the authors and do not necessarily represent the views of the Parliament. This document is still worth including in the study because it is contributory to the policy making activities.
[44] Bigo, et al, 2013, op. cit., p.6

3.3 STATEMENT OF HEADS OF STATE OR GOVERNMENT, ANNEX TO CONCLUSIONS OF THE EUROPEAN COUNCIL, 24/25 OCTOBER 2013[45]

This text is primarily a short statement from the heads of state or government as part of the European Council on discussions in the Council concerning intelligence issues and the concerns these have raised for European citizens. The brief statement makes four points:

- They underlined the close relationship between Europe and the USA and the value of that partnership. They expressed their conviction that the partnership must be based on respect and trust, including as concerns the work and cooperation of secret services.
- They stressed that intelligence gathering is a vital element in the fight against terrorism. This applies to relations between European countries as well as to relations with the USA. A lack of trust could prejudice the necessary cooperation in the field of intelligence gathering.
- The Heads of State or Government took note of the intention of France and Germany to seek bilateral talks with the USA with the aim of finding before the end of the year an understanding on mutual relations in that field. They noted that other EU countries are welcome to join this initiative.
- They also pointed to the existing Working Group between the EU and the USA on the related issue of data protection and called for rapid and constructive progress in that respect.

The broader conclusions to which the above statement forms an annex also make several statements that are relevant to privacy and security, primarily in terms of information technology. Big data and cloud computing are seen as important enablers for productivity and better services, and contributing to growth and European competitiveness.[46] The EU should "provide the right framework conditions for a single market for Big Data and Cloud Computing"; part of this is by "promoting high standards for secure, high-quality and reliable cloud services".[47] A lack of interoperability and a lack of data portability are seen as barriers to the use of digital services.[48] Digital services, such as e-health, e-government, e-invoicing and e-procurement, are seen as part of the desirable modernisation of public administration.[49] Collection of citizens' data is linked to data protection through the idea that citizens' data should be collected only once.[50] There is a discussion of the need for the support and development of digital skills amongst European citizens and business, but this is not linked to either privacy or security in this text.

In the context of migration flows into Europe, the document also contains a call for the swift implementation by Member States of the European Border Surveillance System (EUROSUR) for the purposes of detecting vessels and illegal entry at the EU's external borders.[51]

[45] European Council, 24/25 October 2013 Conclusions, Brussels, 25 October 2013, , http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf
[46] Ibid, p. 1
[47] Ibid, p. 2
[48] Ibid, p. 4
[49] Ibid, p. 4
[50] Ibid, p. 4
[51] Ibid, p. 18

Analysis

This text is notable largely for the absences that it does not make explicit. The majority of the text is about economic development; encouraging European growth through exploiting technology and innovation; increasing services and trade through the single market; reducing barriers to these; and economic and social policy. The statement on intelligence as a conclusion is a departure from these main themes, but is brief. The statement reiterates that the Council sees intelligence gathering, international co-operation and information sharing as vital to the fight against terrorism. However, what form intelligence gathering takes is left undefined. The document does not, for example, make a distinction between legitimate and illegitimate intelligence gathering, apart from the question of trust and co-operation. The document is neutral on the extent to which concerns expressed by European citizens are valid. The problem addressed in this text is a loss of trust in the relations between sovereign governments (rather than the privacy of European citizens), which can be resolved through talks and working groups at the international level.[52] There is no active definition of the concepts of security and privacy in this text. Terrorism stands out at the main security threat identified. To the extent to which analysis of such a brief statement is possible, it appears strongly to align with many of the conclusions about the role of terrorism in structuring security discourse that were identified in the initial period in the discourse analysis conducted as part of D3.1, including those at national levels.

3.4 European Commission Communication the European Parliament and the Council – Rebuilding Trust in EU-US data flows, November 2013[53]

The Commission communication reiterates that the relationship between the EU and the US is strategically important, particularly for security, but that this relationship has been negatively affected by revelations of US intelligence operations, and that this has resulted in a loss of trust. It states that transatlantic transfers of personal information are commercially important, very common, and governed by a series of arrangements to ensure adequate protection of EU citizens' personal data. The communication summarises these existing agreements (Safe Harbour, mutual legal assistance agreement, TFTP, agreements between Europol and the US, PNR agreements, umbrella agreement on data protection in the field of police and judicial cooperation), against the context of technological and commercial development and the position of the US in the ICT sector. Large-scale US intelligence programmes are represented as affecting the fundamental rights of EU citizens, and as potentially having an economic impact. The Commission expresses its wish to agree proper protection of personal data without affecting other elements of EU-US relationships, and exempts negotiation on data protection standards from the Transatlantic Trade and Investment Partnership (TTIP) negotiations. It raises the issue of a lack of procedural safeguards for non-US persons, and the question of necessity and proportionality of US surveillance activities for national security. In order to restore trust, the communication recommends the rapid adoption of the EU data protection reform package; improvements to Safe Harbour; strengthening data protection safeguards in law-enforcement co-operation; addressing European concerns in the on-going US reform process; and promoting privacy standards internationally.

[52] Ibid, p. 19

[53] European Commission, Communication from the Commission to the European Parliament and the Council – Rebuilding Trust in EU-US data flows, COM(2013) 846 final, Brussels, 27 November 2013, http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

3.5 European Parliament report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens

This document is the Report of the European Parliament Civil Liberties, Justice and Home Affairs (LIBE) Committee's inquiry into the electronic mass surveillance of EU citizens.[54] The inquiry was set up in direct response to the Snowden revelations. The full publication consists of a number of component documents. These include two Resolutions of the European Parliament and five working documents, as well as lists of hearings and of experts who participated in the hearings (and those who were invited but did not participate), and background and procedural documents.[55]

As acknowledged in the Report's introduction and in the 2014 Resolution, the inquiry was conducted in the context of the LIBE Committee's dealing with the legislative process of the General Data Protection Reform (GDPR) package.[56] [57] The Report is broad in its coverage and is intended to provide a basis for strengthening digital rights, including developing concepts of digital *habeas corpus*.[58] The Resolution claims that the EU Parliament, perhaps in contrast to the authorities in some Member States and other EU institutions, is taking its obligations to investigate seriously.[59]

The 2014 Resolution suggests that most existing national oversight bodies for intelligence agencies were either set up or revamped in the 1990s and may not have been adapted to the contemporary technological environment that is characterised by the large-scale exchange of personal data. It suggests that the majority of EU and US oversight bodies lack technological capabilities in particular. It also suggests that there is a gap between intelligence oversight activities that are performed at the national level and increasing international co-operation between intelligence agencies.[60] The resolution finds that international treaties and EU and US legislation have failed to provide necessary checks and balances for democratic accountability.[61] It reiterates the role of the EU and rejects the notion that all issues relating to mass surveillance programmes are purely a matter of national security.[62]

The Report calls for an end to blanket mass surveillance. The Resolution states that mass surveillance of human beings is incompatible with fundamental rights as enshrined in the

[54] European Parliament, LIBE Committee inquiry: Electronic surveillance of EU citizens. 2013-2014. http://www.polcms.europarl.europa.eu/cmsdata/upload/7d8972f0-e532-4b12-89a5-e97b39eec3be/att_20141016ATT91322-206135629551064330.pdf

[55] The Resolutions are the European Parliament "Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))"; and "Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU Citizen's privacy (2013/2682(RSP))". The working documents provide additional background information and cover topics including US and EU surveillance programmes; the relation between surveillance practices in the EU and the US and EU data protection provisions; US surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation; democratic oversight of member state intelligence services and EU intelligence bodies; and on foreign policy aspects of the inquiry on electronic mass surveillance of EU citizens.

[56] Ibid, p. 5

[57] Ibid, p. 23

[58] Ibid, p. 6

[59] Ibid, p. 15

[60] Ibid, p. 25

[61] Ibid, p. 27

[62] Ibid, p. 28

EU's CFR and in the ECHR.[63] It also calls upon Member States (and in particular the UK) to review their national legislation and practices governing the activities of their intelligence services, and ensure that these are in line with, in particular, the ECHR and EU data protection law.[64] The Report advocates the suspension of the Safe Harbour principles and the TFTP agreement, finding that large-scale access by US intelligence agencies to EU personal data processed through Safe Harbour does not meet the criteria for derogation from the agreement on the grounds of national security,[65] and calling for the Commission to repeal the decision on the adequacy of Safe Harbour[66] and find alternate legal solutions.[67] The resolution notes previous discussions around adequacy. The LIBE Committee had attempted to ascertain if other US government departments had access to SWIFT (Society for Worldwide Interbank Telecommunication) data outside of the TFTP agreement, but was not able to do so on the basis of information provided by the US government.[68]

The Report also advocates the swift passage of the data protection reform package, in particular calling upon the Council to accelerate its work.[69] The reforms are seen by the Parliament as important in demonstrating credibility to third countries, and in protecting the fundamental rights of European citizens.

The Report makes a case for stronger IT security in the EU as a direct response to mass surveillance practices. This includes taking into consideration the rules, legislation and intelligence agency access to any cloud service providers that might be used by public institutions without the Union.[70] Further, the Resolution calls for the banning of the use of backdoors in information systems by law enforcement, and the adoption of open source software in environments with IT security is a concern.[71] Significant sections of both Resolutions advocate a number of measures to increase EU information security, ranging from European leadership on Internet governance and reshaping Internet architectures to European-based infrastructure, cloud services and social networks.[72] This is based upon reducing the risk "associated with unnecessary routing of traffic through the territory of countries that do not meet basic standards on fundamental rights, data protection and privacy."[73]

Analysis

The Parliament Report explicitly identifies the privacy rights of EU citizens as a political priority against a background of mass surveillance and a loss of trust in related institutions. Data protection and privacy are clearly expressed as fundamental rights in Resolution 2013/2188, with information flows needing to be "as secure from intrusion as private

[63] Ibid, p. 17
[64] Ibid, p. 29
[65] Ibid, p. 31
[66] European Commission, Decision 2000/520/EC 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, OJ L 215, 25.08.2000. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML
[67] European Parliament, LIBE committee inquiry, 2013-14, op. cit., p. 19
[68] Ibid, p. 33
[69] Ibid, p. 34
[70] Ibid, p. 35
[71] Ibid, p. 39
[72] Ibid, p. 42
[73] Ibid, p. 43

homes".[74] Privacy is not a "luxury right" but rather the "foundation stone of a free and democratic society".[75] The 2014 Resolution calls upon EU member states to protect their citizens from surveillance that falls outside of the scope of the ECHR. Privacy is not reduced to data protection in the Report or Resolution, but is placed alongside (and seen as contributory to) the full range of fundamental human rights. The 2014 Resolution and explanatory statement call for an extension of habeas corpus to the digital era, recognising that risks to privacy, integrity and dignity of the individual do not just come from criminal activities and the activities of non-democratic states, but also from the intelligence agencies and law enforcement of democratic states.[76]

The Resolution articulates a substantial number of concerns, which can be understood as the particular threats to privacy identified in the Report. These concerns are: the extent of US and EU member state surveillance systems; the violation of EU legal standards, fundamental rights and data protection standards; the degree of co-operation and involvement of certain EU states with US surveillance programmes or their own equivalent programmes; lack of control and effective oversight by relevant political authorities over intelligence communities; the possibility of mass surveillance operations being used for reasons other than national security and the fight against terrorism in the strict sense; the undermining of press freedom and professional confidentiality; the respective roles and involvement of intelligence agencies and private IT and telecommunications companies; the blurred line between law enforcement and intelligence activities; and in general, the threats to privacy in a digital era and the impact of mass surveillance on citizens and societies.[77] A non-privacy related concern that is located in close proximity to privacy concerns is the degree of trust between the EU and the US. Similarly, intelligence operations between EU Member States are seen as violating the principle of sincere cooperation.[78]

Security as a concept is present in the document. In the Resolution, co-operation between the US, EU and its Member States on counter-terrorism is seen as critical for security and safety of all partners.[79] National security is defined in a relatively strict sense in this Report. The Report expresses concern that surveillance measures may be used for reasons beyond what it considers to be national security and the fight against terrorism.[80] The Resolution discusses the EU's competencies in the field of security, primarily based upon the Treaty on the Functioning of the European Union (TFEU). This includes a call for a restrictive definition of national security, based upon the Vienna Convention, the principle of sincere cooperation among EU Member States, and the human rights law principle of interpreting exemptions narrowly.[81] Whilst strongly denouncing terrorism, the Resolution finds that the fight against terrorism can never be the justification for untargeted, secret or even illegal mass surveillance programmes, and that such programmes are incompatible with necessity and proportionality in a democratic society.[82] The scale of mass surveillance programmes, and the number of citizens they collect data on, indicates to the Parliament Committee that these programmes are likely not only to be guided by the fight against terrorism.

[74] Ibid, p. 13.
[75] Ibid, p. 27
[76] Ibid, p. 53
[77] Ibid, p. 14
[78] Ibid, p. 45
[79] Ibid, p. 13.
[80] Ibid, p. 14
[81] Ibid, p. 17
[82] Ibid, p. 26

The Resolution does deploy the language of balancing in recalling the EU's belief in the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights.[83] The documents do recognise that various protections on privacy can be limited for national security, public interest, or law enforcement reasons (for example in the case of Safe Harbour), but think these limitations and exemptions should be interpreted restrictedly and limited to what is necessary and proportionate in a democratic society.[84] Special powers granted to intelligence agencies are granted on the basis that these are necessary to protect fundamental rights, democracy and the rule of law, citizens rights, and the state against internal and external threats; but that these powers are themselves only legitimate if exercised in within the legal limits imposed by fundamental rights, democracy, the rule of law, and with proper scrutiny.[85] The Explanatory Memorandum states that the core problem is that an increasing focus upon security combined with developments in technology has enabled states to know more about citizens than ever before.[86] The result is a shift from targeted surveillance to mass surveillance that has not been subject to prior public debate or democratic decision-making,[87] and therefore legislative frameworks may be insufficiently precise.[88]

The Report discusses information security and cyber security in detail, particularly in relation to cloud computing and how US intelligence agencies may have access to data on and belonging to European citizens stored on cloud services. Information security is considered to be massively undermined by US intelligence agencies systematically attempting to undermine cryptographic protocols and stockpiling zero-day exploits (previously undiscovered ways to attack computers, valuable because defences against them have not yet been prepared).[89] Information security is linked to the trust citizens have in information technology and related services, and through this to potential economic impact.[90] IT security is linked to privacy, and is also introduced into the balance between law-enforcement access and individual privacy: "while legitimate law enforcement and intelligence concerns need to be taken into account in order to support the fight against terrorism, they should not lead to a general undermining of the dependability of all IT systems".[91] Following an assessment of the "acute vulnerability" of EU institutions to sophisticated cyber attack (referencing the hacking of Belgacom)[92], the Parliament considers the EU cyber security strategy to be neglecting the threat from state actors.[93] Therefore, additional resources are seen as necessary for "preserving Europe's independence and self-reliance in the field of ICT". The Resolution also calls for an increased mandate for Europol to be able to initiate its own investigations into malicious attacks on networks and information systems, [94] as well as a review by the Commission on the level of resources and capabilities of the European Network and Information Security Agency (ENISA), CERT-EU and the European Data Protection Supervisor (EDPS) so they can play appropriate roles in securing European information systems.

[83] Ibid, p. 27
[84] Ibid, p. 20
[85] Ibid, p. 25
[86] Ibid, p. 49
[87] Ibid, p. 48
[88] Ibid, p. 73
[89] Ibid, p. 24
[90] Ibid, p. 24
[91] Ibid, p. 40
[92] Ibid, p. 39
[93] Ibid, p. 40
[94] Ibid, p. 38

The Parliament's investigation does pay attention to domestic developments within the US, particularly activities of district courts and the President's review group on Intelligence and Communication Technologies. The Resolution notes those reviews that draw attention to the need simultaneously to protect privacy and national security,[95] but also highlights those that do not recommend granting non-US persons the same rights as US citizens in relation to protections against electronic surveillance. The Resolution calls upon the US to revise its legislation to bring it into line with international law, to recognise the privacy and other rights of EU citizens, to provide judicial redress for EU citizens, and to put their rights on an equal footing with those of US citizens.[96] The Resolution has a substantive discussion about trust between the EU and US, noting important historical relationships and shared values, but also that the potential for mass surveillance and surveillance of EU political leaders has the capacity to undermine trust in this relationship.[97]

The Report responds to a particular event, the Snowden surveillance revelations. The Resolution considers that the information provided by these revelations as well as expert testimony and other sources are compelling evidence of "the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store, and analyse communications data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner."[98] The Resolution considers that these events have put political leaders under the obligation to address the challenges of oversight and accountability in relation to the activities of intelligence agencies and the ways that their activities might impact upon fundamental rights.[99]

The Explanatory Statement provides its own analysis of the discursive positions in the "post-Snowden debate". Arguments against EU action include intelligence and national security as a Member State competence; weakening national security; the lack of legitimacy of the leaked documents; the need to maintain a strategic relationship with the US; and the presumption of lawful and good governance. The Statement contrasts these with the historically evidenced danger of surveillance; the importance of human rights; the parallel EU competence in internal security; the gap between national oversight of intelligence and the international nature of security threats, which threatens to leave traditional oversight mechanisms out-dated; and the chilling effect upon media and whistleblowers. The Statement sets out a clear choice:

"The European Union is called upon to choose between a 'business as usual' policy (sufficient reasons not to act, wait and see) and a 'reality check' policy (surveillance is not new, but there is enough evidence of an unprecedented magnitude of scope and capacities of intelligence agencies requiring the EU to act)."[100]

[95] Ibid, p. 15
[96] Ibid, p. 30
[97] Ibid, p. 44
[98] Ibid, pp.25-26
[99] Ibid, p. 14
[100] Ibid, p. 52

3.6 ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 04/2014 ON SURVEILLANCE OF ELECTRONIC COMMUNICATIONS FOR INTELLIGENCE AND NATIONAL SECURITY PURPOSES, APRIL 2014[101]

This document is the Opinion from the collective body of European data protection authorities, issued in response to discussions in the media on the surveillance activities of intelligence agencies. It examines the relationship between mass surveillance and fundamental rights to privacy and data protection, and makes recommendations that the Working Party sees as necessary to restore the rule of law. The Working Party concludes that "secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security."[102]

The Opinion acknowledges that the operation of the intelligence services of EU Member States is not subject to EU law (including the Data Protection Directive 95/46/EC) due to the national security exception in the founding treaties and the Directive. In many Member States there are exemptions to general data protection law for intelligence services (for example on the right to be informed and the right to access by the data subject).[103] However, the Opinion finds that the provisions of the ECHR and the Council of Europe Convention 108 on the protection of personal data do still apply. The Opinion indicates that companies may be in breach of European law if they grant access to European personal data on a mass scale to third-country intelligence agencies, or allow this to occur. The Opinion notes that this may place companies in the difficult position of deciding which legal regime they should comply with, but that this does not preclude enforcement action on the part of European DPAs.[104] [105] The Opinion discusses the nature of meta-data in some detail, based upon existing European jurisprudence. Meta-data can reveal sensitive data about individuals, and are sometimes easier to process and analyse than content because of their structured nature. In the understanding of the Working Party, meta-data are personal data and should therefore be protected.

The Working Party recommends greater transparency on how surveillance programmes work, more meaningful oversight of intelligence agencies, and enforcing the existing obligations of Member States and parties to the ECHR to protect the rights of respect for private life and to protection of one's personal data.[106] The Working Party further notes that Safe Harbour, standard contractual clauses or binding corporate rules do not provide legal justification for the transfer of personal data to a third-country authority for the purposes of mass surveillance. The Working Party also calls upon EU institutions to finalise the data protection reform package[107], and for negotiations on an international agreement to grant individuals adequate protection in the context of intelligence activities. [108] More meaningful oversight would include fully independent checks upon the data processing activities of intelligence agencies by an outside body with effective enforcement powers.[109] The Opinion calls for the development of a global instrument providing for enforceable high-level privacy and data

[101] Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, WP125, Brussels, 10 April 2014
[102] Ibid, p. 2
[103] Ibid, p. 10
[104] Ibid, p. 7
[105] Ibid, p. 14
[106] Ibid, p. 2
[107] Ibid, p. 14
[108] Ibid, p. 3
[109] Ibid, p. 8

protection principles as agreed upon by the ICDPPC in the Madrid Declaration of 2009.[110] The Opinion contains recommendations on the protection of EU data from international intelligence agencies, including discussion on the appropriate legal mechanisms for access in cases of specific suspicion; the requirements for Member States to ensure that relevant national laws regarding the sharing of intelligence data are being followed; the inadequacy of secret cooperation agreements; and the benefits and limits of the so-called Umbrella Agreement that was being negotiated between the EU and the US.

Analysis

The text was produced in response to media reports based upon the documents leaked by Edward Snowden regarding the electronic surveillance activities of the intelligence agencies, the discussions that these reports have stimulated, and the questions raised about the powers of intelligence agencies.[111] The text notes that data protection authorities have extremely limited oversight roles in relation to intelligence services (no powers at all in nine Member States), and defers to comment on recent documents on which the Working Party has insufficient evidence.[112] A second motivation for the Opinion is a request from the Vice President of the European Commission to the Article 29 Working Party to determine what the role of data protection authorities might be in supervision of surveillance activities.[113]

Privacy, in this text, is clearly defined as a fundamental right, enshrined in law (particularly in the ICCPR, the ECHR, and the EU's CFR. The right to privacy is therefore something that should be politically protected. Privacy rights can be overridden by national security concerns, but if this is done in an indiscriminate manner then this is illegitimate. Restrictions to fundamental rights can only be accepted if the measure is strictly necessary and proportionate in a democratic society. Surveillance measures that are indiscriminate and use blanket collection of personal data do not meet requirements of proportionality and necessity. Furthermore, interference with fundamental rights must be foreseeable, and this requires greater transparency about surveillance programmes.[114]

The key threat to privacy in this text is electronic mass surveillance as potentially (based upon evidence available to the Working Party) conducted by intelligence agencies in the US and some EU Member States. Electronic mass surveillance involves the sophisticated, and often automated collection of communications data. Protecting privacy is a difficult challenge. The report states that even people "who are careful about how they run their online lives can currently not protect themselves against mass surveillance programmes".[115] Data protection authorities also face a challenge in providing protection in this context.[116] The Working Party states that there is a need to set limits to surveillance. The Opinion's analysis of meta-data questions the claim that the collection of meta-data is in some way less significant or less serious than the collection of communications content, arguing that such information about a communication may reveal sensitive data about a person.[117] Based upon legal judgements on

[110] Ibid, p. 16
[111] Ibid, p. 4
[112] For example, the interception of submarine Internet cables.
[113] Article 29 Data Protection Working Party, 10 April 2014, op. cit., p. 8
[114] Ibid, p. 12
[115] Ibid, p. 6
[116] Ibid, p. 6
[117] Ibid, p. 4

data retention, privacy can be threatened merely through the retention of communications data.[118]

The Opinion calls for the concept of national security to be clarified in EU law, particularly as national security operates as an exemption to many areas of privacy and data protection law. The document expresses concern that the concept is poorly defined.[119] Security is also discussed in the context of the remit and roles of intelligence agencies in EU Member States, in particular in relation to the distinction between internal and external national security threats, and civilian and military responsibilities.[120] This raises the Working Party's concern over the extent to which the national security exemptions on personal data collection and processing reflect reality when the work of intelligence services is increasingly intertwined with that of law enforcement, which could fall under EU law. [121]

There is no direct mention of the US in relation to the activities of intelligence agencies, other than through the placeholder of "third countries", in reference to the negotiation of the Umbrella Agreement, and to the EU-US High Level Contact Group on information sharing and privacy report from 2009.[122] The international agreements are seen as currently inadequate for the protection of citizens.

3.7 UN High Commissioner for Human Rights report "The right to privacy in the digital age" – June 2014[123]

The Office of the United Nations High Commissioner for Human Rights issued this Report on the 30th June 2014 following the General Assembly resolution 68/167 of December 2013. The resolution expressed concern at the negative impact upon human rights resulting from surveillance and the interception of communications. In addition to calling upon states to review their procedures and legislation relating to surveillance, and affirming that rights held offline must also be protected online, the General Assembly had requested the High Commissioner for Human Rights to prepare a report on the right to privacy in the digital age and to examine "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale". The Report is based upon research and consultation exercises performed by the High Commissioner's office, including workshops and a survey of member states.

The Report frames privacy in terms of international human rights law, particularly Article 12 of the Universal Declaration of Human Rights and the ICCPR, as well as regional and national instruments. It states that there is universal recognition of the fundamental importance and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded.[124]

[118] Ibid, p. 5
[119] Ibid, p. 3
[120] Ibid, p. 9
[121] Ibid, p. 15
[122] Ibid, p. 15
[123] United Nations General Assembly, Resolution adopted by the General Assembly on 18 December 2013 68/167. The right to privacy in the digital age, A/RES/68/167, 21 January 2014. http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167
[124] United Nations High Commissioner for Human Rights, The right to privacy in the digital age, Report, 30 June 2014, p.5, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

The Report examines how interference in privacy is defined, and in particular the extent to which interception of data about a communication, rather than the content of the communication, can be understood as an interference. Like the Article 29 Working Party, the Report finds that the "metadata" distinction is not persuasive from the perspective of the right to privacy, that subsequently any capture of communications data is potentially an interference with privacy, and that, additionally, this is the case regardless of whether the data are subsequently used or analysed.[125] The report also discusses the definitions of "arbitrary" and "unlawful", and the relation between national law and international covenants.

The UN Report discusses the protection of the law, and the necessity for the interference of privacy to be based upon publicly accessible laws, as based upon article 17 of the ICCPR.[126] It states that secret rules and interpretations do not have the necessary qualities of law and that because surveillance practices can be secret, the relevant laws must be drafted with additional precision. It finds that networks of intelligence agencies co-ordinating surveillance practices to "outflank" protections from domestic legal regimes also fails the test of lawfulness. On the topic of protection against extraterritorial surveillance, the Report reiterates a commitment that international law requires that states may not avoid their international human rights obligations by taking action outside its territory that it would be prohibited from taking "at home", and that this equally applies to surveillance practices if the surveillance involves the state's exercise of power or effective control.[127] The report is critical of distinctions between "foreigners" and "citizens", and of unequal access to privacy protections.

The Report makes a clear statement with regard to procedural safeguards and effective oversight. It finds that "a lack of effective oversight has contributed to a lack of accountability for arbitrary and unlawful intrusions on the right to privacy in the digital environment."[128] It is cautious about reliance solely on judicial oversight and advocates the adoption of mixed methods of oversight, including administrative, judicial and parliamentary oversight, and potentially even some kind of public interest advocacy in the process.[129] It acknowledges the challenge of protecting the right to privacy, in the context of a persistent lack of transparency about surveillance practices online, and recommends that efforts in this direction will require the involvement of multiple stakeholders and continued vigilance in ensuring that surveillance policies are in compliance with international human rights law. It advocates that states immediately undertake reviews of their own laws, policies and practices and take steps where there are shortcomings, particularly in the area of effective and independent oversight regimes.[130]

The Report does not name or otherwise discuss Edward Snowden and his revelations in anything other than the most oblique manner, referring instead to "some governments". The Report is generally framed in the language of possibility in relation to its legal conclusions.

[125] Ibid, p. 7
[126] Ibid, p. 10
[127] Ibid, p. 11
[128] Ibid, p. 12
[129] Ibid, p. 13
[130] Ibid, p. 16

Analysis

Much of this Report is a definition of the concept of privacy, at least to the extent that this is captured in international human rights law. Therefore the document provides a clear picture of that concept. Much of this discussion is framed in the conventional language of proportionality, necessity and legitimacy of aim. As part of this exercise, the Report does discuss the impact of surveillance measures relative to the harm threatened.[131] It is clear that the report considers protection of the right to privacy and its exercise to be a responsibility of states under international human rights law. Interference with the right to privacy for certain legitimate ends is permissible, but only with a strictly circumscribed legal framework. At points in the Report, privacy is discussed in terms of a set of protections against surveillance practices.[132] Threats to privacy emerge primarily from the surveillance programmes of national governments, bolstered by technological developments, although private companies are also implicated in these activities to an increasing extent.

Unlike the concept of privacy, which in investigated in detail, the concept of security is somewhat (although not totally) absent in this report. The introduction does not make great mention of the supposed motivations for surveillance practices, and the most detail on security is provided in the analysis of legitimate interference with the right to privacy. The Report acknowledges that, when conducted in compliance with the law, surveillance of electronic communications data can be a necessary and effective measure for legitimate law enforcement or intelligence purposes. However, it qualifies this judgment by attributing it to contributions from states themselves, and expresses concern that recent revelations have raised questions about the extent to which such measures are consistent with international legal standards.[133] In its discussion of legality, the Report does note that states frequently justify digital communications surveillance on the basis of national security.[134] It states that surveillance on the grounds of national security or for the prevention of terrorism or crime can count as a legitimate aim, but that the degree of interference with privacy must be assessed against the necessity of the measure to achieving the intended aim and the actual benefit that the measure provides.

The Report starts with a commentary on technology, and how technological developments in communications technologies have both had benefits for the exercise of human rights, but have also resulted in the removal of limits of scale and duration from state surveillance capabilities. This could be understood as technologically determinist in that the Report does not enquire into the origins of these technologies. This picture is more nuanced in the account of the conflicts between efforts to anonymise large data sets and the converse efforts at re-identification, where the Report notes that the investment in the latter is many times greater than in the former.

3.8 European Parliament, Science and Technology Options Assessment (STOA) Mass surveillance – December 2014

The European Parliament's Science and Technology Options Assessment (STOA) on Mass Surveillance comprises four parts: Part I – risks and opportunities raised by the current

[131] Ibid, p. 9
[132] Ibid, p. 12, note this is reminiscent of Daniel Solove's work on the concept of privacy.
[133] Ibid, p. 6
[134] Ibid, p. 8

generation of network services and applications,[135] and a supporting annex;[136] and Part II – Technology foresight options for longer term security and privacy improvements,[137] again with a supporting annex. This analysis will treat the various sections as a single cohesive policy document. Part I examines the risks of data breaches for public Internet services and the impacts upon them and European information society; technological advances in the collection and analysis of mass data for surveillance purposes; technological and organisational methods; key stakeholders; and risk reduction policy options. The annex contains detailed answers to 35 questions posed to the Report's authors by its commissioners. Part II of the study provides the Parliament with policy options for the protection of Europe's information society from mass surveillance. The annex again contains detailed answers to specific key questions. Part I of study was conducted by Technalia, and part II by Capgemini Consulting, working independently, but both on behalf of the Parliament STOA, an official organ of the European Parliament.[138]

The analysis of the risks of breaches is based upon a technical analysis of various components of mass surveillance, including the concept of meta-data; the application of big data analytic technologies as an integral part of mass surveillance; software vulnerabilities and their exploitation; the technical credibility of national security agencies hacking capabilities; and commercial surveillance software. The report also engages with "cryptographic reliability in a post-Snowden world" and efforts to undermine encryption. It highlights the way that subversion of encryption is related to standards and specifications. The report calls for a process to check, validate and certify cryptographic chain implementations are correctly mapped to their requirements.[139] It discusses encryption in response to efforts to undermine encryption, and as part of a set of security measures that can help (but cannot guarantee to) protect individuals from surveillance, and calls for policy action that "guarantees European citizens access to certified, resilient and open source implementations of different encryption specifications."[140] It states that the increasing concerns of citizens about their privacy is pushing more and more Internet service providers towards offering (communication) services that are secured, and encrypted by default.[141] In addition, it calls for the adoption of open source operating systems and applications, and investing and stimulating the integration of user-friendly utility-software software in this domain.[142] One of the conclusions of the report is that the only currently technical means of protection against surveillance and of preserving privacy is by guaranteed uncorrupted end-to-end encryption of content and transport channels, but that this is complex for most technically inexperienced users.[143] The report includes

[135] European Parliament STOA, Mass Surveillance, Part 1, Risks and opportunities raised by the current generation of network services and applications, Study, December 2014, http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Study%20Mass%20Surveillance%20Part%201.pdf

[136] European Parliament STOA, Mass Surveillance, Part 1, Risks and opportunities raised by the current generation of network services and applications, Annex, December 2014, http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Annex%20Mass%20Surveillance%20Part%201.pdf

[137] European Parliament STOA, Mass Surveillance, Part 2, Technology foresight, options for longer term security and privacy improvements, Study, December 2014, http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Study%20Mass%20Surveillance%20Part%202.pdf

[138] European Parliament, "About STOA", Online, http://www.europarl.europa.eu/stoa/cms/home/about

[139] European Parliament STOA, part 1, p.16

[140] Ibid, p. 2

[141] Ibid,, p. 20

[142] Ibid, p. 2

[143] Ibid, p. 55

information on the known weaknesses of various privacy protecting technologies[144], and both parts acknowledge that the threat posed by mass surveillance practices cannot be solved on a technical level but requires technology-based political action.[145] This being said, the report does provide significant detail on the technological options that might contribute towards greater privacy and security.

The report provides a set of technical and policy options with the intention of mitigating the risk to individual data created by the various elements of mass surveillance. Technical measures, include a combination of cryptography best practices, technical options for mitigating surveillance risks, and individual software choices and programs (e.g. encryption of data in storage and in transit; protection for email services; protection for voice and video communication; protection for web-browsing; chat; web searches; and privacy-aware operating systems). Short-to-mid-term policy options advocated in the report include an EU initiative to implement a resilient implementation for encryption; the promotion of open protocols, implementations and systems; regulation of telecom security and encryption standards; investment in user awareness; increasing citizen empowerment by regulating and investing data and information transparency; investment in integrated platform specific security and privacy acts; and regulations that require applications to adopt maximum privacy settings as default.

Part II is explicitly intended to support and inform the LIBE committee with technical background insight and detail on policy options. It is based on four technology foresight scenarios, each with multiple policy options. The "promote adoption" scenario discusses the promotion of end-to-end encryption, the promotion of open-source software, the promotion and stimulation of EU ICT services (cloud, social media, and search engines), and the promotion of secure software development.[146] The "build confidence" scenario includes developing security baselines and mechanisms for co-ordinated disclosure of security vulnerabilities in the EU.[147] Policy options in the "disrupt(ive innovation)" scenario include certification schemes for encryption and a European Internet subnet.[148] Finally the "innovate" scenario policy options are stimulating research and development into reduced trackability/traceability and detection of surveillance, promoting improvement of inherently insecure Internet protocols, and setting up an EU R&D programme for data-centric security.[149] These technological measures should be supported by legal, financial and promotional methods.[150] The report suggests several ways in which a market in secure software could be stimulated in the EU, ranging from a tougher position in the proposed data protection Regulation on data export, and leveraging the purchasing power of the EU and Member States. The report goes into some detail on the substance of various technical issues, including the implementation of encryption; the security advantages and disadvantages of open-source and closed-source software; certification scheme;, secure software development; and the economics of information technology.

[144] Ibid, p. 41
[145] European Parliament STOA, part 2, op. cit., p.3
[146] Ibid, p.1
[147] Ibid, p.2
[148] Ibid, p.2
[149] Ibid, p.3
[150] Ibid, p.4

Analysis

The report is another response to the disclosure of mass surveillance programmes of intelligence and national security agencies. In particular, it focuses upon the risks of data breaches for users of Internet services, and the potential impacts upon citizens. It treats the issue as primarily an information security problem. In this sense the report is close to a Threat Landscape assessment as produced by ENISA. Security as a concept is therefore mostly *information security* more that it is represented as national security, and is a potential tool for protecting privacy. For example, in Part II, managing privacy risks and threats against privacy is to be conducted through a "robust security posture".[151] The second part of the STOA report does use the language of "balance" to discuss the relationship between security, privacy and the legitimate interests of intelligence agencies and law enforcement. The balance is interesting in this context because privacy and security of European citizens and business are placed on one side of the balance, with intelligence and law enforcements on the other. The particular balance is represented as currently distorted and in need of being restored by increasing by increasing privacy and security.[152] The policy options are therefore oriented in the direction of supporting such an increase.

STOA reports are primarily technical reports, with the intention of providing evidenced support for a range of policy options, but not to advocate a particular option or set of options (although this one does advocate a particular direction of policy). They are based primarily upon desk research, but acknowledge the limitations of this approach, particularly the extent to which the authors have had to base some conclusions solely upon leaked documents from the NSA and GCHQ. At several points the report articulates this lack of information (and participation from relevant organisations) as a point of political concern. The report finds, for example, that due to the lack of evidence it is difficult to ensure that surveillance tools are only used for legitimate targeted surveillance rather than also used for illegitimate mass surveillance,[153] and difficult to assess the extent to which national security agencies' capabilities are at, or surpass, the current state of the art.[154] Part II also defers the proper assessment of the "balance" between privacy and law enforcement, intelligence and marketing to political debate, rather than being anything inherent in technology, or something that can be left to market forces.[155] The report does however avoid issues of relations between countries and other explicitly political topics. Although technically focused, the report, and particularly Part II, should not be considered as technologically deterministic, as it highlights multiple ways in which technologies can be affected by social, political and economic decisions and influencing factors. It is clear that political choices can be made that would, through their impact upon technological development, have consequences for privacy and security.

The STOA report makes a distinction between targeted surveillance for the purposes of law enforcement and criminal investigation, and mass interception, the latter being considered unwarranted and indiscriminate.[156] [157] Mass surveillance is considered a threat to civil liberties. Indeed, it is the generalisation of surveillance, for the purposes of pre-emptive

[151] Ibid, p.3
[152] Ibid, p. 10
[153] European Parliament STOA, part 1, op. cit., p. 33
[154] Ibid, p. 35
[155] European Parliament STOA, part 2, op. cit.,, p. 4
[156] European Parliament STOA, part 1, op. cit., p. 1
[157] Ibid, p. 26

omniscience, which violates privacy rights and freedom of speech. The automation of this process, and the general lack of awareness of citizens, are seen as exacerbating factors in the violation.[158]

Threats to privacy emerge from national security agencies, in additional to commercial surveillance technology vendors;[159] analysis of meta-data;[160] commercial cookies (particularly due to lack of transparency and control by users); complicity between mass surveillance organisations and other parties;[161] incorrect and inappropriate implementation of encryption and other information security practices;[162], hacking and criminal activity; and vulnerabilities in software. The report makes a technical distinction between the content of communications and communications meta-data, but then discusses how much information about individuals and groups can be extracted from subjecting meta-data to data-mining techniques and in combination with other datasets.[163] The report acknowledges that mass surveillance is a commercial business sector,[164] and examines several key players in this industry. The insight derived from this is that "the usage and operation of commercial mass surveillance tools does not require exceptional technical or personnel resources which could only be provided by state or government agencies."[165] Part II identifies further technological threats to privacy that emerge from the potential development of quantum computing, which could render current encryption methods obsolete, and the spread of the Internet of Things, which could widen the capacity for surveillance and create new security and privacy risks.[166]

Part II reports upon, but does not endorse (given the policy options it advocates) the position of law enforcement experts (Europol, FBI) who argue against the spread of encryption. These experts make an analogy between the physical and digital world and argue that law enforcement must have some methods of access to encrypted communications, most likely some form of back door.[167] Inability to access this raises the likelihood that a law enforcement agency would resort to targeted surveillance with a potentially bigger impact upon privacy.

3.9 COUNCIL OF EUROPE REPORT ON MASS SURVEILLANCE – JANUARY 2015

The Parliamentary Assembly of the Council of Europe (CoE) adopted a resolution based upon the report by Pieter Omtzigt, a Dutch parliamentarian. The Committee on Legal Affairs stated: "Mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials. Instead, resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act."[168]

[158] Ibid, p. 55
[159] Ibid, p. 2
[160] Ibid, p. 11
[161] Ibid, p. 12
[162] Ibid, p. 17
[163] Ibid, p. 1
[164] Ibid, p. 26
[165] Ibid, p. 32
[166] European Parliament STOA, part 2, op. cit.,, p. 4
[167] Ibid, p. 14
[168] Council of Europe, "Mass surveillance is counter-productive and 'endangers human rights'", 26 January 2015. http://assembly.CoE.int/nw/xml/News/News-View-EN.asp?newsid=5387&lang=2&cat=5

The full Report consists of a draft resolution, draft recommendations, and an Explanatory Memorandum. Responding directly to the Snowden files, the Report found that the surveillance practices of the US and some (unnamed) CoE member states, as disclosed in the leaked files, endanger fundamental human rights, including the rights to privacy, freedom of information and expression, the right to a fair trial, and freedom of religion. The infringement of these rights without proper judicial control is also seen as jeopardising the rule of law.[169]

The Report (and therefore the Assembly when it passed the resolution) saw the surveillance practices as a threat to Internet security, in particular the practices of attempting to weaken or undermine encryption methods and security standards to allow for access by intelligence agencies. Efforts to subvert encryption are described as potentially counter-productive with the consequence of undermining Internet security.[170] "Installing backdoors, deploying malwares and deliberately weakening encryption systems creates new vulnerabilities in the targeted systems that other non-benevolent third parties can discover and exploit.

The Report does not just limit surveillance capacities to states, but notes with concern the surveillance capacities of private businesses.[171] It notes the development of a "surveillance-industrial complex". This highlights the difficulty of assessing the seriousness of alleged threats and the need for specific counter-measures, without the involvement of interested parties.[172]

The revelations are seen as having reduced trust between various parties internationally. In terms of measures for moving forward from this position, the Report advocates a legal framework at national and international level to ensure the protection of human rights, including the right to privacy. Protection of whistleblowers is seen as part of this framework.[173] It also encourages national-level accountability exercises such as inquiries.[174] Member States and observers are encouraged to ensure that collection and analysis of data has a sound basis in either consent, or in a court order granted on the basis of reasonable suspicion,[175] to ensure that state intelligence agencies are subject to adequate judicial and/or parliamentary control mechanisms, and to develop an "intelligence codex" laying down rules for international co-operation between agencies.[176] The Report notes that the CoE, unlike the EU, is not precluded from dealing with the national security aspects of human rights protection.[177] The report also calls for a strict ban on the creation of "backdoors" and other techniques to weaken or circumvent security measures or exploit their weaknesses.[178]

The Report provides a detailed account of the various capabilities and programmes revealed by the NSA and GCHQ documents, including some analysis of these and discussion on the limits of what can be known about them. It also covers collaboration for collusion and

[169] Committee on Legal Affairs and Human Rights, Parliamentary Assembly, Council of Europe, *Mass Surveillance: Report*, Provisional version, 26 January 2015, http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2, p.1
[170] Ibid, p. 17
[171] Ibid, Paragraph 6.
[172] Ibid, Paragraph 9.
[173] Ibid, Paragraph 14
[174] Ibid, Paragraph 15
[175] Ibid, Paragraph 17
[176] Ibid, Paragraph 17
[177] Ibid, p. 30
[178] Ibid, p. 30

increased attention to the surveillance activities of European states, NSA surveillance of US persons; spying for economic and diplomatic purposes; efforts to undermine encryption; and Internet privacy and security. The Explanatory Memorandum also provides accounts of the implications of mass surveillance for human rights, with a scathing critique of mass surveillance. This analysis draws upon human rights law, including the ECHR, and jurisprudence from the ECtHR. The report concludes by reiterating the costs of mass surveillance in terms of both privacy and the exercise of other human rights that are dependent upon privacy. It advocates legal restraint for intelligence agencies and other components of the surveillance-industrial complex, including parliamentary oversight and international agreements. This, it argues, would allow security agencies to continue to defend security using effective and proportional means.

Analysis

As with many documents in this period, this Report is issued clearly in response to particular events, in this case the revelations of NSA and GCHQ activities. This is a later document, and therefore responding to the widest range of new surveillance- related events. It is also able to refer to earlier policy documents, which are themselves reactions to the same events.

Security does not appear to be foregrounded in this Report. Various forms of the trade-off argument or assumption are not particularly present, and may be implicitly discounted. Rather, it is surveillance activities that are contrasted against privacy, as clearly and expressly damaging to it. The relationship between security and privacy is not antagonistic; rather, privacy is seen as contributory to security. The solutions suggested (legal frameworks, encouraging encryption) are therefore intended to encourage both security and privacy. In this sense, this document continues the development of the theme that security and privacy are not inherently antagonistic concepts.

Legitimate national security interests are strongly delineated in this Report, substantially more so that in many documents in the preceding analysis in Deliverable 3.1. It calls for the banning of the use of surveillance measures for political, economic or diplomatic purposes (at least among states participating in the "intelligence codex" agreement, and who have adequate domestic legal framework), limiting such measures to the fight against terrorism and organised crime.[179] Threats to national security are seen as arising from rogue states, terrorists, cyber-terrorists and ordinary criminals. Encryption is seen as protecting against these threats, as well as important in achieving privacy.[180] The Report discusses how surveillance capabilities are deployed against targets that it does not consider to be national security threats, including telecommunications intermediaries such as ISPs and systems administrators.[181]

"Balancing" does occur, but in the context of balancing of interests that arise in relation to the protection of whistleblowers.[182] The Report also attempts to weaken the link between security and surveillance, by highlighting findings in the EU and US that mass surveillance had provided only "minimal benefits" in stopping terrorism,[183] and by seeing mass Internet monitoring as performing less well in terms of cost and efficiency than other lower-tech

[179] Ibid, Paragraph 17.4
[180] Ibid, Paragraph 16.2
[181] Ibid, p. 18
[182] Ibid, p. 5
[183] Committee on Legal Affairs and Human Rights, Parliamentary Assembly, Council of Europe, Op. cit, p. 19

approaches.[184] In the Explanatory Memorandum, the Report refers back supportively to the European Parliament Report, to the UN General Assembly Resolution 68/187 and the UN High Commissioner for Human Rights June 2014 Report.

There is little or no sign of technological determinism in this Report. It does not, for example, spend much time considering how the Internet infrastructure might create surveillance potential, and it grants a high level of agency to particular national bodies and governments in how they operate in these fields.

[184] Ibid, p. 19, footnote 76.

4 CONCLUSION

There are some marked discursive changes between the sample of policy documents included in this updated report when compared with the policy documents covered by the initial analysis in Deliverable 3.1. Whilst some trends remain constant, there are noticeable changes that may be traceable to the Snowden revelations and the resulting public attention and political fall-out.

An analysis of these changes follows; this additional analysis allows us to continue to map the rhetorical-conceptual relationships between security, privacy and (critically) surveillance. "Rhetorical-conceptual" refers to the idea that concepts in a discourse can be defined and understood in different ways, often through the way they are associated with other concepts, and that these concepts (and their relationships) can be intentionally defined in particular ways to produce political arguments. These arguments can become commonplace, and thereby form part of the regularities of political discourses. The conclusions are necessarily limited by the collection of documents, the sample chosen for analysis, and the conduct of the analysis itself. We can identify apparent changes and consistencies in relation to the previous sample and its analysis, particularly as there were clearly documents of the type analysed here in the previous sample. The analysis here deals with significant documents, therefore in addition to the comparative analysis, we gain important insights about how the EU and international organisations are constructing privacy and security (in relation to each other) in the current milieu (and during the period of the PRISMS survey).

Several of the analysed policy documents open up the rhetorical space around the concepts of privacy and security. In brief, they do this by exploring the ambiguity of security (including through the increasing prominence of information security as a component part of contemporary security) and the contingency of the ways in which surveillance is understood as contributing towards security. In this context, the traditional opposition between security and privacy is increasingly challenged. The European policy documents in particular also continue to do some work in the creation of shared identity for European citizens, as having shared interests in both privacy and security, and as potential subjects of surveillance activity.

The statement by first ministers through the European Council is the most consistent with the discourse analysis from the previous study. In other words, the Council is more "traditional" in its attitude to privacy, security and trade-offs than the Commission and the Parliament. It maintains a conventional position that knowledge is important for security, and information exchange between nation states is equally contributory to security.

Several trends that were identified in the first analysis appear to continue through these documents. The most significant of these is the increasing importance of privacy in policy documents, and that importance has continued to expand. Also significant is the increasing inclusion of information security within the general concept of security, of both nations and individuals. The EU position that security and privacy are not inherently opposed continues to be reflected in these documents. The rhetoric of the terrorist attacks of 11 September 2001 is absent from these documents. Even if the fight against terrorism in general still figures, it is disconnected from the significant event. EU actors still continue to prioritise regulatory and legal methods and approaches as the appropriate responses to privacy threats, even as the range of privacy threats grows. However, as argued below, there are increasing technological responses starting to be discussed.

The most substantial difference is the prominence given to the digital mass surveillance activities of intelligence agencies, particularly the NSA and GHCQ, but also the intelligence agencies of other EU Member States. These issues are the subject of focused, in-depth, and specific policy attention, at least from the European Parliament, Council of Europe and the Article 29 Working Party, not just a side issue, or a consideration alongside methods for encouraging the digital economy. In a sense, a new problem of government has been articulated in these texts. This greater focus actually allows for a more nuanced, if contested, model of what surveillance (and particularly mass surveillance) is. Several documents discuss the distinctions between data and meta-data, mass surveillance and bulk collection, and other features of contemporary surveillance. The majority of documents (including the LIBE Committee Report, the UN Report, the CoE Report and the STOA report) find the distinction between data and metadata, and the assumption that the collection of metadata does not impact upon privacy, to be unconvincing.

With varying degrees of priority and focus, responses to the problem of mass surveillance found in the policy documents include policy reviews; re-balancing privacy and security; particular effort on the part of the EU; increasing accountability and transparency; technology-based political action; encouraging the development of security technologies (and their supporting industries); and protection for whistleblowers.

Several documents discuss the need for a "re-balancing" between security and privacy, where it is acknowledged that the two values are currently out of balance and that security may have been systematically privileged over privacy. This lack of balance may have emerged because of the law, or intelligence oversight mechanisms not keeping pace with technological developments that provide the capacity for mass surveillance. Privacy is frequently articulated in these policy documents as a fundamental right. In that respect, balancing is problematic, and a "trade-off" is unacceptable. Rather there exist in both EU and international law, a set of strictly delineated circumstances and exceptions that allow for the fundamental right to privacy to be overridden. Secret, massive, indiscriminate and arbitrary collection of communications is interpreted by several documents (the first Report for the LIBE Committee, the UN Report, the STOA report and the Article 29 Working Party Opinion) as outside of the acceptable limits provided by those exemptions, and therefore illegal. Other documents however, particularly those with an information security perspective, suggest that privacy and security are linked, rather than opposed. In this case what is needed is not a "re-balancing" as above, but rather a recognition of this link, and that security is reliant upon privacy, and policy action in line with this recognition. In this case, a trade-off has not been made to gain more security at the cost of privacy, but that such an imagined trade-off is not technically possible, and more security has not been gained.

A new topic emerging in these documents, in part as a response to the political problem of digital mass surveillance is the extent to which the European Union has any competency with regard to national intelligence services. Several documents feature a detailed discussion of the extent to which the activities of Member State (and third country) intelligence agencies fall within the competencies and capabilities of the European Union, despite national security remaining a Member State competency. The European Parliament Report, in particular, drawing inspiration from the CEPS Report it published previously, identifies mechanisms for the EU to exert influence over intelligence activities. These include the security responsibilities for EU institutions, the use by EU bodies such as Frontex and Europol of data that may originate through surveillance activities, and strictly delineating the definition of

national security within EU law. Other mechanisms are identified in these documents that are intended to provide the EU with a stronger negotiating position with regard to the US: for example, suspending the Safe Harbour and TFTP agreements, suspending negotiations on TTIP, and swiftly passing the GDPR.

The issue of weakening encryption and the resulting potential for generalised online insecurity is a new component of the post-Snowden discourses of security and privacy. It builds upon, and substantiates in a specific form, pre-existing accounts that were starting to include online security or information security in broader concepts of security.[185] The increasing uptake of encryption and encrypted services is interpreted as a public demand for privacy by several documents (including the STOA reports, which examine this in some detail). Privacy-enhancing technologies, and economic and technological methods for increasing privacy and information security for citizens, even in the absence of a policy or regulatory shift, are the subject of detailed discussion, where these were particularly absent in early policy discussions.

The difficulty of achieving accurate understanding of surveillance and intelligence activities is explicitly raised in several texts. The secrecy of intelligence operations raises a problem for policy documents, and particularly for supranational bodies, in that it complicates identifying political problems and constructing viable responses to them. For example, the LIBE committee expressed its difficulty at finding adequate answers to questions regarding the use of SWIFT data by US government departments, and the Council of Europe report includes an analysis of the limits of what can be known about intelligence programmes. Several texts recommend increased transparency and oversight for intelligence agencies as part of bringing these activities into the sphere of democratic accountability.

Few documents in the previous analysis examined European surveillance activity (this perhaps being the preserve of reports originating from civil society groups, such as Statewatch or EDRi), yet some of the recent policy documents do start to explore the extent of surveillance activity by the EU Member States.

The way that the relationship between the EU and the US is discussed is different in several of these documents to previously analysed texts, particularly in those originating with the European Parliament. Whereas previously, US statements on security were quite influential, and the relationship described as one of mutually beneficial co-operation, several of these documents are openly sceptical about the relationship between the EU and the US, and damage to this relationship and loss of trust brought about by mass surveillance activities. Even the statement by the Council of Ministers acknowledges the potential loss of trust. There is discussion of the EU institutions and EU citizens as a target of US surveillance, and (in the CEPS study for the Parliament) even discussion that this may place the EU at a strategic disadvantage. The CEPS study is, however, distinctly outspoken in its account that the US seeks "full spectrum dominance" through surveillance. Many texts still acknowledge that co-operation and co-ordination for counter-terrorism and law enforcement are important. This different perspective on the relationship is demonstrated in those policy suggestions that discuss ways of routing Internet traffic around the EU, and the development of a European Internet infrastructure.

[185] Barnard-Wills, D., "Security, Privacy and Surveillance in European Policy Documents", *International Data Privacy Law*, Vol. 3, No. 3, February 2013.

5 ANNEX: KEY EUROPEAN AND INTERNATIONAL POLICY DOCUMENTS ON PRIVACY AND SECURITY

5.1 EUROPEAN UNION

5.1.1 European Parliament

2015

European Parliament resolution of 11 February 2015 on anti-terrorism measures (2015/2530(RSP)). http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2015/02-11/0032/P8_TA-PROV%282015%290032_EN.pdf

European Parliamentary Research Service, Ten technologies which could change our lives: potential impacts and policy implications, European Parliament, January 2015, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/527417/EPRS_IDA%282015%29527417_REV1_EN.pdf

2014

European Parliament resolution of 17 December 2014 on renewing the EU internal security strategy (2014/2918(RSP)), http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2014/12-17/0102/P8_TA-PROV%282014%290102_EN.pdf

European Parliament STOA, Mass Surveillance, Part 2, Technology foresight, options for longer term security and privacy improvements, Study, December 2014, http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Study%20Mass%20Surveillance%20Part%202.pdf

European Parliament STOA, Mass Surveillance, Part 1, Risks and opportunities raised by the current generation of network services and applications, Study, December 2014, http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Study%20Mass%20Surveillance%20Part%201.pdf

De Hert, Paul & Vagelis, Papakonstantinou, The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area, Study, European Parliament, Brussels, November 2014, http://www.europarl.europa.eu/RegData/etudes/STUD/2014/510001/IPOL_STU%282014%29510001_EN.pdf

European Parliamentary Research Service, The Echelon Affair: The EP and the global interception system 1998-2002, Study, European Parliament, November 2014, http://www.europarl.europa.eu/RegData/etudes/STUD/2014/538877/EPRS_STU%282014%29538877_EN.pdf

European Parliament resolution of 27 November 2014 on supporting consumer rights in the digital single market (2014/2973(RSP), http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2014/11-27/0071/P8_TA-PROV%282014%290071_EN.pdf

Committee of Foreign Affairs, Draft Opinion on the draft Council decision on the conclusion, on behalf of the Union of the Agreement between Canada and the European Union on the transfer of Passenger Name Record data, 6 October 2014,

Bigo, Didier, Sergio Carrera, Nicholas Hernanz, and Amandine Scherrer, National security and secret evidence in legislation and before the courts: Exploring the challenges, Study, European Parliament, Brussels, September 2014, http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU%282014%29509991_EN.pdf

Bigo, Didier, Julian Jeanesboz, Meredic Martin-Maze, Francesco Ragazzi, Review of security measures in the 7th Research Framework Programme FP7 2007-2013, Study, European Parliament, Brussels, April 2014, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509979/IPOL-LIBE_ET%282014%29509979_EN.pdf

Wesseling, Maria, Evaluation of EU measures to combat terrorism financing, European Parliament, Brussels, April 2014, http://www.europarl.europa.eu/RegData/etudes/note/join/2014/509978/IPOL-LIBE_NT%282014%29509978_EN.pdf

Davoli, Alessandro, Fact Sheets on the European Union: Personal Data Protection, European Parliament, April 2014, http://www.europarl.europa.eu/RegData/etudes/fiches_techniques/2013/051208/04A_FT%282013%29051208_EN.pdf

Hartman, Andrea-Renatus, Fact Sheets on the European Union: Management of the external borders, European Parliament, April 2014, http://www.europarl.europa.eu/RegData/etudes/fiches_techniques/2013/051204/04A_FT%282013%29051204_EN.pdf

European Parliamentary Research Service, At a glance: The EU approach to cyber-security, European Parliament, 31 March 2014, http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140775/LDM_BRI%282014%29140775_REV1_EN.pdf

European Parliamentary Research Service, At a glance: Big data: opportunities and privacy concerns, http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140771/LDM_BRI%282014%29140771_REV1_EN.pdf

European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)) http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2014/03-12/0212/P7_TA-PROV(2014)0212_EN.pdf

European Parliament legislative resolution of 12 March 2014 on the 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)0010 – C7-0024/2012 – 2012/0010(COD)) http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2014/03-12/0219/P7_TA-PROV(2014)0219_EN.pdf

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)),

http://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/provisoire/2014/03-12/0230/P7_TA-PROV(2014)0230_EN.pdf

European Parliament, Q&A on Parliament's inquiry into mass surveillance of EU citizens, Background, 10 March 2014, http://www.europarl.europa.eu/sides/getDoc.do?type=IM-PRESS&reference=20140310BKG38512&secondRef=0&language=EN

European Parliament, LIBE Committee inquiry: Electronic surveillance of EU citizens. 2013-2014. http://www.polcms.europarl.europa.eu/cmsdata/upload/7d8972f0-e532-4b12-89a5-e97b39eec3be/att_20141016ATT91322-206135629551064330.pdf

European Parliament, Report on the proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (COM(2013)0045) – C7 0032/2013 – 2013/0025(COD)), 28 February 2014. www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2014/0150/P7_A(2014)0150_EN.doc

2013

European Parliament, REPORT on the 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)0010 – C7 0024/2012 – 2012/0010(COD)), www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2013/0403/P7_A(2013)0403_EN.doc

European Parliament, Report on the 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), 22 November 2013. http://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2013/0402/P7_A(2013)0402_EN.doc

Bigo, Didier., Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi & Armandine Scherrer, *National Programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, European Parliament, October 2013. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

European Parliament, Report on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, 19 June 2013, http://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2013/0224/P7_A(2013)0224_EN.doc

European Parliament, Report 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, 25 April 2013,

http://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2013/0150/P7_A(2013)0150_EN.doc

European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), 28 February 2013, http://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2013/0056/P7_A(2013)0056_EN.doc

Moreas, Claude (23 December 2013). "DRAFT REPORT on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. (2013/2188(INI))". European Parliament Committee on Civil Liberties, Justice and Home Affairs.

2012

European Parliament, Report on critical infrastructure protection – achievements and next steps: towards global cyber security, 16 May 2012, http://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2012/0167/P7_A(2012)0167_EN.doc

European Parliament, Report on cyber security and defence, 17 October 2012, http://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2012/0335/P7_A(2012)0335_EN.doc

European Parliament, Report on the situation of fundamental rights in the European Union (2010-2011), 22 November 2012, http://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2012/0383/P7_A(2012)0383_EN.doc

Fighting cyber crime and protecting privacy in the cloud, 2012 http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET%282012%29462509_EN.pdf

5.1.2 European Commission

2014

European Group on Ethics in Science and New Technologies to the European Commission, Ethics of Security and Surveillance Technologies, Opinion No.28, European Commission, Brussels, 20 May 2014, http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_security_surveillance_technologies.pdf

Fovino, Igor Nai, Ricardo Neisse, Dimitris Geneiatakis, Mobile application privacy: towards a methodology to identify over-privileged applications, European Commission Joint Research Centre, 2014, http://bookshop.europa.eu/en/mobile-applications-privacy-pbLBNA26484/downloads/LB-NA-26484-EN-N/LBNA26484ENN_002.pdf?FileName=LBNA26484ENN_002.pdf&SKU=LBNA26484ENN_PDF&CatalogueNumber=LB-NA-26484-EN-N

2013

Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM (2013) 847, 27 November 2013. http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

European Commission, Communication from the Commission to the European Parliament and the Council Rebuilding Trust in the EU-US Data Flows, COM (2013) 846 final, 27 November 2013, http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country national crossing the external borders of the Member States of the European Union COM (2013) 95, 28 February 2013, http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf

Guimarães Pereira, Ângela, Alice Benessia, and Paula Curvelo, Agency in the Internet of Things, European Commission Joint Research Centre, 2013, http://bookshop.europa.eu/en/agency-in-the-Internet-of-things-pbLBNA26459/downloads/LB-NA-26459-EN-N/LBNA26459ENN_002.pdf?FileName=LBNA26459ENN_002.pdf&SKU=LBNA26459ENN_PDF&CatalogueNumber=LB-NA-26459-EN-N

European Commission, Europe's Policy options for a dynamic and trustworthy development of the Internet of things, 2013, http://bookshop.europa.eu/en/europe-s-policy-options-for-a-dynamic-and-trustworthy-development-of-the-Internet-of-things-pbKK0113297/downloads/KK-01-13-297-EN-N/KK0113297ENN_002.pdf?FileName=KK0113297ENN_002.pdf&SKU=KK0113297ENN_PDF&CatalogueNumber=KK-01-13-297-EN-N

2012

European Commission, Special Eurobarometer 390 — 'Cyber Security', July 2012 http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

Loschner, Jan, Pasquale Stirparo, Vincent Mahieu, David Shaw, Stefan Scheer & Ionnis Kounellis, Digital Footprint in a mobile environment, European Commission, 2012, http://bookshop.europa.eu/en/digital-footprint-in-a-mobile-environment-pbLBNA26051/?AllPersonalAuthorNames=true

5.1.3 Council of the European Union / European Council

2014

The European Council, The European Council in 2013, Luxembourg, Publications Office of the European Union, 2014. www.consilium.europa.eu/en/workarea/downloadAsset.aspx?id=1014

2013

European Council, Statement of Heads of State or Governments, Annex to the conclusions of the European Council, 24/25 October 2014, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

The European Council, The European Council in 2012, Luxembourg, Publications Office of the European Union, 2013. http://www.consilium.europa.eu/en/workarea/downloadAsset.aspx?id=960

5.1.4 European Network and Information Security Agency (ENISA)

2014
(primarily technical guidance for information security methods and best practices)

2013

ENISA, Recommendations for a methodology for the assessment of the severity of personal data breaches, 20 December 2013. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity/at_download/fullReport
ENISA, On the security, privacy and usability of online seals, 16 December 2013, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/on-the-security-privacy-and-usability-of-online-seals
ENISA, Roadmap for European Cyber Security Month, 16 December 2013, https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2013/ecsm-roadmap
ENISA, securing personal data in the context of data retention, 10 December 2013, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/securing-personal-data-in-the-context-of-data-retention
ENSIA, A Good Practice Collection for CERTS on the Directive on attacks against information systems, 28 November 2013, https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems
ENISA, Proposal for One Security Framework for Articles 4 and 13a, 20 December 2013, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/proposal-for-one-security-framework-for-articles-4-and-13a
ENISA, National-level Risk Assessments: an analysis report, 18 November 2013, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report
ENISA, ENISA Threat Landscape, 8 January 2013, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

2012

ENISA, National Cyber Security Strategies: An Implementation Guide, 19 December 2012, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape
ENISA, Report on Annual Privacy Forum 2012, 12 December 2012, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/report-on-annual-privacy-forum-2012
ENISA, Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime, 28 November 2012, https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime

ENISA, The right to be forgotten – between expectations and practice, 20 November 2012, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten
ENISA, Privacy considerations of online behavioural tracking, 14 November 2012, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking

5.1.5 European Security Research Advisory Board (ESRAB)

Not active during update period

5.1.6 European Security Research and Innovation Forum (ESRIF)

Not active during update period

5.1.7 Frontex

2014

Frontex, Annual Risk Analysis 2014, Warsaw, 2014. http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2014.pdf

2013

Frontex, Annual Risk Analysis 2013, Warsaw, 2014, http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2013.pdf

5.1.8 European Agency for Fundamental Rights

2014

FRA, Fundamental Rights: challenges and achievements 2013: Annual Report, Vienna, 2014, http://fra.europa.eu/sites/default/files/fra-2014-annual-report-2013-0_en.pdf
FRA, Handbook on European data protection law, Vienna, June 2014, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law
FRA, Access to data protection remedies in EU Member States, Vienna, January 2014, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states

2013

FRA, Fundamental Rights, challenges and achievements in 2012, Vienna, June 2013, http://fra.europa.eu/en/publication/2013/fundamental-rights-challenges-and-achievements-2012
FRA, Fundamental rights in the future of the European Union's Justice and Home Affairs, Vienna, 31 December 2013, http://fra.europa.eu/sites/default/files/fra_submission_on_the_future_of_eu_justice.pdf

2012

FRA, Data protection reform package FRA Opinion, Factsheet, Vienna, October 2012, http://fra.europa.eu/en/publication/2012/data-protection-reform-package-fra-opinion-october-2012

FRA, Fundamental Rights: Challenges and achievements in 2012, Vienna, June 2012, http://fra.europa.eu/en/publication/2012/fundamental-rights-key-legal-and-policy-developments-2011

5.1.9 Article 29 Data Protection Working Party

2014

Article 29 Data Protection Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things, WP223, 16 September 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Article 29 Data Protection Working Party, Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, WP221, 16 September 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

Article 29 Data Protection Working Party, Statement on the ruling of the Court of Justice of the European Union which invalidates the Data Retention Directive, WP220, 1 August 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp220_en.pdf

Article 29 Data Protection Working Party, Opinion 7/2014 on the protection of personal data in Quebec, WP219, 4 June 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp219_en.pdf

Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, WP218, 30 May 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

Article 29 Data Protection Working Party Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of the Directive 95/46/EC", WP217, 9 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Article 29 Data Protection Working Party, Opinion 05/2014 on "Anonymisation Techniques", WP216, 10 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Article 29 Data Protection Working Party, Opinion 04/2014 on "Surveillance of electronic communications for intelligence and national security purposes", WP215, 10 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

Article 29 Data Protection Working Party, Opinion 03/2014 on "Personal Data Breach Notification", WP213, 25 March 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

Article 29 Data Protection Working Party, Opinion 02/2014 on "Referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the

EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents", WP212, 27 February 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf

Article 29 Data Protection Working Party, Opinion 01/2013 on the "Application of necessity and proportionality concepts and data protection within the law enforcement sector", WP211, 27 February 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf

2013

Article 29 Data Protection Working Party, Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DIPA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, WP209, 4 December 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

Article 29 Data Protection Working Party, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP208, 2 October 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

Article 29 Data Protection Working Party, Opinion 06/2013 on open data and public sector information ('PSI') reuse, WP207, 5 June 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf

Article 29 Data Protection Working Party, Opinion 05/2013 on Smart Borders, WP206, 6 June 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf

Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, WP205, 22 April 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, WP203, 2 April 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices, WP202, 27 February 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

Article 29 Data Protection Working Party, Opinion 01/2013 providing further input into the discussion on the draft Police and Criminal Justice Data Protection Directive, WP201, 26 February 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf

Article 29 Data Protection Working Party, Working Document 01/2013 Input on the proposed implementing acts, WP200, 22 January 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp200_en.pdf

2012

Article 29 Data Protection Working Party, Opinion 08/2012 providing further input on the data protection reform discussions, WP199, 5 October 2012,

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf
Article 29 Data Protection Working Party, Opinion 07/2012 on the level of protection of personal data in the Principality of Monaco, WP198, 19 July 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp198_en.pdf
Article 29 Data Protection Working Party, Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications, WP197, 12 July 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp197_en.pdf
Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, 1 July 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
Article 29 Data Protection Working Party, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP195, 6 June 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf
Article 29 Data Protection Working Party, Opinion 04/2012 on Cookie Consent Exemption, WP194, 7 June 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf
Article 29 Data Protection Working Party, Opinion 03/2012 on developments in biometric technologies, WP193, 27 April 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

5.1.10 European Data Protection Supervisor

2014

EDPS, The transfer of personal data to third countries and international organisations by EU institutions and bodies, Position paper, Brussels, 14 July 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf
EDPS, The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience, Policy paper, Brussels, 4 June 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/14-06-04_PP_EDPSadvisor_EN.pdf
European Data Protection Supervisor, Annual Report 2013, Publications Office of the European Union, Luzembourg, 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2013/AR2013_EN.pdf

2013

EDPS, Annual Report 2012 – 'Smart, sustainable, inclusive Europe': only with stronger and more effective data protection, Publications Office of the European Union, Luxembourg, 2013, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2012/AR2012_EN.pdf

2012

EDPS, Policy on consultations in the field of Supervision and Enforcement, Brussels, 23 November 2012, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/12-11-23_Policy_on_Consultations_EN.pdf

5.2 INTERNATIONAL ORGANISATIONS

5.2.1 United Nations

2014

Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/3, 30 June 2014, http://www.ohchr.org/en/hrbodies/hrc/regularsessions/session27/documents/a.hrc.27.37_en.pdf

United Nations Security Council, Resolution 2178 (2014) Threats to international peace and security caused by terrorist acts, S/RES/2178 (2014), 24 September 2014. http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2178%20%282014%29

United Nations Security Council, Resolution 2170 (2014) Threats to international peace and security caused by terrorist acts, S/RES/2170 (2014), 15 August 2014. http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2170%20%282014%29

United Nations Security Council, Resolution 2161 (2014) Threats to international peace and security caused by terrorist acts, S/RES/2161 (2014), 17 June 2014. http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2161(2014)

United Nations Security Council, Resolution 2170 (2014) Threats to international peace and security caused by terrorist acts, S/RES/2160 (2014), 17 August 2014. http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2160(2014)

United Nations Security Council, Resolution 2133 (2014) Threats to international peace and security caused by terrorist acts, S/RES/2160 (2014), 27 January 2014. http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2133%282014%29

2013

United Nations General Assembly, Resolution 68/167 on the right to privacy in the digital age, A/RES/68/167, 18 December 2013, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

United Nations Security Council, Resolution 2119 (2013) Threats to international peace and security caused by terrorist acts, S/RES/2119 (2013), 17 December 2013

5.2.2 OECD

2014

OECD, Food and Nutrition (in)security and Social Protection, in OECD Development Co-operation Working Papers, 12 May 2014, http://www.oecd-

ilibrary.org/deliver/fulltext?contentType=%2fns%2fWorkingPaper&itemId=%2fcontent%2fworkingpaper%2f5jz44w9ltszt-en&mimeType=freepreview&containerItemId=%2fcontent%2fworkingpaperseries%2f22220518&accessItemIds=&redirecturl=http%3a%2f%2fwww.keepeek.com%2fDigital-Asset-Management%2foecd%2fdevelopment%2ffood-and-nutrition-in-security-and-social-protection_5jz44w9ltszt-en&isPreview=true

2013

OECD, Building a smarter health and wellness future: Privacy and security challenges, 3 October 2013, http://www.oecd-ilibrary.org/building-a-smarter-health-and-wellness-future-privacy-and-security-challenges_5k3z2f2kj6r1.pdf?contentType=%2fns%2fChapter&itemId=%2fcontent%2fchapter%2f9789264202863-11-en&mimeType=application%2fpdf&containerItemId=%2fcontent%2fbook%2f9789264202863-en&accessItemIds=

OECD, Empowering and Protecting Consumers in the Internet Economy, OECD Digital Economy Papers, 5 February 2013, http://www.oecd-ilibrary.org/science-and-technology/empowering-and-protecting-consumers-in-the-Internet-economy_5k4c6tbcvvq2-en

OECD, Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities, and Data Privacy Protection Challenges, OECD Health Policy Studies, OECD Publishing, 2013, http://www.keepeek.com/Digital-Asset-Management/oecd/social-issues-migration-health/strengthening-health-information-infrastructure-for-health-care-quality-governance_9789264193505-en#page3

OECD, Global Environmental Change and Human Security, in World Social Science Report 2013: Changing Global Environments, http://www.keepeek.com/Digital-Asset-Management/oecd/social-issues-migration-health/world-social-science-report-2013/global-environmental-change-and-human-security_9789264203419-103-en#page1

OECD, Gender gaps in feelings of insecurity: Percentage of people declaring feeling safe when walking alone at night in the city or area where they live, by gender, 2012 or latest available year, in How's Life? 2013: Measuring Well-Being, 05 November 2013. http://www.oecd-ilibrary.org/deliver/fulltext?contentType=%2fns%2fOECDBook%2c%2fns%2fBook%2c%2fns%2fStatisticalPublication&itemId=%2fcontent%2fbook%2f9789264201392-en&mimeType=freepreview&containerItemId=%2fcontent%2fserial%2f23089679&accessItemIds=&redirecturl=http%3a%2f%2fwww.keepeek.com%2fDigital-Asset-Management%2foecd%2feconomics%2fhow-s-life-2013_9789264201392-en&isPreview=true

OECD, Water Security for Better Lives, OECD Publishing, 2 September 2013. http://www.oecd-ilibrary.org/deliver/fulltext?contentType=%2fns%2fChapter&itemId=%2fcontent%2fchapter%2f9789264202405-3-en&mimeType=freepreview&containerItemId=%2fcontent%2fserial%2f22245081&accessItemIds=&redirecturl=http%3a%2f%2fwww.keepeek.com%2fDigital-Asset-Management%2foecd%2fenvironment%2fwater-security-for-better-lives%2fexecutive-summary_9789264202405-3-en&isPreview=true

OECD, Global Food Security: Challenges for the Food and Agricultural System, OECD Publishing, 19 June 2013. http://www.oecd-ilibrary.org/deliver/fulltext?contentType=%2fns%2fChapter&itemId=%2fcontent%2fchapter%2f9789264195363-5-en&mimeType=freepreview&containerItemId=%2fcontent%2fbook%2f9789264195363-en&accessItemIds=&redirecturl=http%3a%2f%2fwww.keepeek.com%2fDigital-Asset-Management%2foecd%2fagriculture-and-food%2fglobal-food-security%2fensuring-global-food-availability_9789264195363-5-en&isPreview=true

OECD, Settlement, Market and Food Security, OECD Publishing, 21 May 2013, http://www.oecd-ilibrary.org/deliver/fulltext?contentType=%2fns%2fChapter&itemId=%2fcontent%2fchapter%2f9789264187443-4-en&mimeType=freepreview&containerItemId=%2fcontent%2fserial%2f2074353x&accessItemIds=&redirecturl=http%3a%2f%2fwww.keepeek.com%2fDigital-Asset-Management%2foecd%2fagriculture-and-food%2fsettlement-market-and-food-security%2fexecutive-summary_9789264187443-4-en&isPreview=true

OECD, Conflict over Resources and Terrorism: Two Facets of Insecurity, OECD Publishing, 02 April 2013, http://www.oecd-ilibrary.org/development/conflict-over-resources-and-terrorism_9789264190283-en

2012

OECD, Security and Privacy, in OECD Internet Economy Outlook 2012, OECD Publishing, 2012, http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-Internet-economy-outlook-2012/security-and-privacy_9789264086463-10-en#page1

OECD, Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security Privacy and the Protection of Children Online, OECD Publishing, 20 December 2012. http://www.oecd-ilibrary.org/science-and-technology/improving-the-evidence-base-for-information-security-and-privacy-policies_5k4dq3rkb19n-en

OECD, The Role of the 2002 Security Guidelines, Towards Cybersecurity for an Open and Interconnected Economy, Digital Economy Papers, OECD Publishing, 16 November 2012, http://www.oecd-ilibrary.org/science-and-technology/the-role-of-the-2002-security-guidelines-towards-cybersecurity-for-an-open-and-interconnected-economy_5k8zq930xr5j-en

5.2.3 NATO

2014

Progress report on the implementation of the NATO/EPAC Policy and Action Plan on Women, Peace and Security – Report to the Heads of State and Government, 5 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112846.htm?selectedLocale=en

NATO/EPAC Policy for the implementation of UNSCR 1325 on Women, Peace and Security and related resolutions, 1 April 2014, http://www.nato.int/cps/en/natohq/official_texts_109830.htm?selectedLocale=en

2013

NATO, NATO's policy guidelines on counter-terrorism, 21 May 2013, http://www.nato.int/cps/en/natohq/official_texts_87905.htm?selectedLocale=en

5.2.4 International Conference of Data Protection and Privacy Commissioners

2014

36th International Conference of Data Protection and Privacy Commissioners, Declaration on the Internet of Things, Balaclava Fort, October 2014. http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf

36th International Conference of Data Protection and Privacy Commissioners, Resolution Big Data, Balaclava Fort, October 2014. http://www.privacyconference2014.org/media/16602/Resolution-Big-Data.pdf

36th International Conference of Data Protection and Privacy Commissioners, Resolution Privacy in the digital age, Balaclava Fort, October 2014. http://www.privacyconference2014.org/media/16608/Resolution-Privacy-in-the-digital-age.pdf

2013

35th International Conference of Data Protection and Privacy Commissioners, Declaration on the appification of society, Warsaw, 2013. https://privacyconference2013.org/web/pageFiles/kcfinder/files/ATT29312.pdf

35th International Conference of Data Protection and Privacy Commissioners, Profiling resolution, Warsaw, 2013. https://privacyconference2013.org/web/pageFiles/kcfinder/files/2.%20Profiling%20resolution%20EN%281%29.pdf

35th International Conference of Data Protection and Privacy Commissioners, Webtracking resolution, Warsaw, 2013. https://privacyconference2013.org/web/pageFiles/kcfinder/files/8.%20Webtracking%20Resolution%20EN%281%29.pdf

35th International Conference of Data Protection and Privacy Commissioners, International Law resolution, Warsaw, 2013. https://privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf

2012

34th International Conference of Data Protection and Privacy Commissioners, Resolution on Cloud Computing, Punta Del Este, October 2012. http://privacyconference2012.org/wps/wcm/connect/92d083804d5dbb9ab90dfbfd6066fd91/Resolutionon_Cloud_Computing.pdf?MOD=AJPERES

34th International Conference of Data Protection and Privacy Commissioners, Resolution on the future of privacy, Punta Del Este, October 2012. http://privacyconference2012.org/wps/wcm/connect/ae021f804d5dbfeeb937fbfd6066fd91/aResolution_on_the_Future_of_Privacy.pdf?MOD=AJPERES

34th International Conference of Data Protection and Privacy Commissioners, Urugauy Declaration on profiling, Punta Del Este, October 2012. http://privacyconference2012.org/wps/wcm/connect/7b10b0804d5dc38db944fbfd6066fd91/Uruguay_Declaration_final.pdf?MOD=AJPERES

5.2.5 ITU

nothing relevant found

5.2.6 Council of Europe

2015

Committee on Legal Affairs and Human Rights, Parliamentary Assembly, Council of Europe, Mass Surveillance: Report, Provisional version, 26 January 2015, http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2

2014

European Audiovisual Observatory, "How Private is Personal Data?", IRIS Plus 2013-6, 2014. https://book.CoE.int/eur/en/european-audiovisual-observatory/5824-iris-plus-2013-6-how-private-is-personal-data.html [paid content]

Council of Europe, Protection of Whistleblowers – Recommendation CM/REC(2017)7 and explanatory memorandum, 2014. https://book.CoE.int/eur/en/legal-instruments/6162-protectionof-whistleblowers-recommendation-cmrec20177-and-explanatory-memorandum.html

Consultative committee of the convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Opinion on the implications for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes, Strasbourg, 4 June 2014, http://www.CoE.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%282014%2905_En_Opinion%20tax%20%28final%29.pdf

2013

Committee of Ministers, Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, 11 June 2013. https://wcd.CoE.int/ViewDoc.jsp?id=2074317&Site=CM

Council of Europe, Council of Europe and Internet: Maximising Rights, Minimising Restrictions, 2013, https://edoc.CoE.int/en/Internet/5990-council-of-europe-maximising-rights-minimising-restrictions.html

Ana Salinas de Frias, Counter-Terrorism and human rights in the case law of the European Court of Human Rights, Council of Europe, 2013. https://book.CoE.int/eur/en/european-court-of-human-rights/5716-pdf-counter-terrorism-and-human-rights-in-the-case-law-of-the-european-court-of-human-rights.html (paid content) http://www.CoE.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD%282013%2907%20KORFF%20-%20Trends%20report%20-%20March2013%20%28new%29.pdf

6 OTHER CITED LITERATURE

Barnard-Wills, David, "Security, Privacy and Surveillance in European policy documents", International Data Privacy Law, Vol. 3, No. 3, 2013, pp. 170-180.

Barnard-Wills, David, Surveillance and Identity; Discourse, Subjectivity and the State, Ashgate, Farnham, 2012.

Bodea, Gabriela, Noor Huijboom, Sander van Oort, Merel Ooms, Bas van Schoonhoven, Tom Bakker, Livia Teernstra, Rachel L. Finn, David Barnard-Wills, David Wright, and Charles D. Raab, "Draft analysis of privacy and security policy documents in the EU and US", PRISMS Deliverable 3.1, 2013.

Chouliaraki, Lilie, and Norman Fairclough, Discourse in Late Modernity: Rethinking Critical Discourse Analysis, Edinburgh University Press, Edinburgh, 1999.

European Council, "The Stockholm Programme – An open and secure Europe serving and protecting the citizens", Official Journal of the European Union C 115, 4.5.2010, pp. 1-38

González Fuster, Gloria, Serge Gutwirth, Bernadette Somody, and Ivan Székely, "Consolidated legal report on the relationship between security, privacy and personal data protection in EU law", PRISMS Deliverable 5.2, 2014.

Hajer, Maarten A., "Coalitions, practices and meanings in environmental politics: from acid rain to BSE", in D. Howard, and J. Torfing (eds.), Discourse theory in European Politics: Identity, policy and governance, Palgrave-Macmillan, Basingstoke, 2005.

Heilbroner, Robert, L., "Do Machines Make History?", in Robert C. Scharff, and Val Dusek (eds.), The Philosophy of Technology: The Technological Condition, Blackwell, Oxford, 2003.

Huijboom, Noor, and Gabriela Bodea, "Understanding the Political PNR-debate in Europe: A Discourse Analytical Perspective", Perspectives on European Politics and Society, 2015.

Lyon, David, Surveillance Studies: An Overview, Polity Press, Cambridge, 2007.

Philips, Louise, and Marianne W. Jørgensen, Discourse Analysis as Theory and Method, Sage, London, 2004.