Security, privacy and surveillance in European policy documents

David Barnard-Wills*

Abstract

- Through an examination of security and privacy policy documents from the EU, selected European states and the USA, this article examines problem construction and policy making in the interrelated fields of security, privacy, and surveillance.
- This horizontal analysis, across a set of documents, provides insights into the way these topics are viewed within the policy-making process.
- The analysis also shows the development of EU governmentality around security and privacy, and indicates that whilst the policy discourse of security and privacy is not homogeneous, the influence of European-level governance on security and privacy practices is significant.
- The study aims to make a contribution to the literature on security and privacy and on the international context for policy making.

Introduction

'Security' and 'privacy' have multiple meanings across contexts. What becomes defined as a privacy or security 'problem' (and what is excluded from this) is a political process, conducted at least in part through policy texts and documents.[1] By assessing a relevant set of policy documents referring to the security and privacy policies of the European Union (EU), selected Member States and the USA, it is possible to understand the manner in which concepts of security, privacy or data protection, and surveillance are framed in a European policy context, and the differences between countries. Although this investigation and conclusions drawn from it are limited by the nature of the sample and the purely documentary basis of the research, the 'horizontal' analysis across documents and places nonetheless gives important insights into the way these topics and themes are viewed within the policy-making process in these countries or jurisdictions. This study may thus pave the way for further research in greater depth and breadth, using additional research tools to gain greater understanding of policy making in these important inter-related fields. This analysis does not look 'behind the text' to the motives and intentions of the texts' authors, but can be seen as specific examples of deliberate attempts to engage in a political process of claim-making,[2] framing issues of privacy and security in particular ways. Policy documents are part of the way that government, broadly conceived and including intergovernmental actors, reflects upon, co-ordinates and seeks justification and legitimation for its activity.[3] The presentation of reasons for action is a critical part of how social actors construct the world.[4] This analysis provides an examination of the ways in which problems of security and privacy are constituted, and of the policy responses that are put forward. The study hopes to make a contribution to literatures on security and privacy and on the international context for policy making in these domains.

* Trilateral Research and Consulting LLP, London, United Kingdom. The research for this paper comprised part of the PRIvacy and Security MirrorS: Towards a European framework for integrated decision making (PRISMS) project, funded under the EU Security programme (Grant agreement no: 285399). The research emerges from work package three, which was conducted by researchers from Trilateral Research & Consulting, the University of Edinburgh, and the Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO). Particular acknowledgements go to Charles Raab, David Wright, Rachel Finn, Fanny Mazella, Gabriela Bodea, Merel Ooms, and Noor Huijboom. The views expressed in this article are those of the author alone and are in no way to be interpreted to be those of the European Commission. More information about PRISMS can be found at http://www.prismsproject.eu.

[1] Mitchell Dean, *Governmentality: Power and Rule in Modern Society* (2nd edn, Sage 2010) 38.

[2] Malcolm Spector and John L. Kitsuse, *Constructing Social Problems* (Cummings Publishing, Menlo Park, CA 1977).

[3] Nicholas Rose, *The Powers of Freedom* (Cambridge University Press, Cambridge 1999); James Tully, 'Political Philosophy as a Critical Activity' (2002) 30 Political Theory 533; David Barnard-Wills, *Surveillance and Identity: Discourse, Subjectivity and the State* (Ashgate, Farnham 2012).

[4] Karen M Fierke, *Critical Approaches to International Security* (Polity, Cambridge 2007) 70.

The article first provides a description of the text selection method used in the study. It then addresses security, privacy, data protection, and surveillance in the policy documents in turn, followed by their international dimension, before concluding with the insights that this analysis provides. The analysis finds that the meaning of the main concepts in focus in this research varies across contexts. Security varies as a concept across different countries and across actors within different countries, and is expanding to include issues such as information security, cyber security, and critical infrastructure protection. Privacy is also understood as being under threat from a variety of different sources that appear to diverge across contexts. While some countries may construct the private sector as the primary privacy invader, others focus on the policies and actions of public authorities. Furthermore, there is some evidence that different technologies emerge as privacy threats in different countries. Finally, while many countries use the 'balance' metaphor to explain the inter-relationship between privacy and security, EU policy documents frequently construct privacy and security as complementary rights that must be 'respected', thus exerting some pressure on Member State governments to adopt similar principles. Beyond the empirical descriptions of clusters of shared and contested meanings across countries, the analysis shows that policy discourses of security and privacy are not homogeneous across Europe, lending support to the idea that approaches are contingent and contextual. However, there are strong areas of consensus for both security and privacy problems, with security perhaps the more established and entrenched problem. There are current attempts actively to integrate and link the two sets of problems, as in the current EU representation of security and rights as complementary. The analysis also shows the development of EU governmentality around security and privacy, and indicates that the current influence of European-level governance on security and privacy practices is significant.[5]

Methods

To tease out how policy-makers regard privacy and security, we first identified more than 900 policy documents that addressed privacy and/or security; these have been published by selected EU Member States, third countries, international organizations, and EU institutions, including legislative bodies, executive bodies, departments of defence, immigration agencies, data protection authorities, and other relevant institutions as appropriate for each country, from 2000 onwards. The documents are publicly available and free to access. Document titles were relied upon to determine material that focused upon privacy or security and that was worth exploring further. From this list, several researchers independently selected those documents that seemed most relevant for this research. Selections were then compared, and an agreed 'short list' of 54 were chosen for more in-depth analysis. Documents that discussed both privacy and security, and to a lesser extent surveillance and data protection, were given priority, as well as major policy documents (e.g. the Stockholm programme), key policy changes after September 2001 and national defence strategies in Europe, Member States and the USA.

As mentioned, the analysis is based upon this sample of selected documents only, and although it may draw some limited generalizations from patterns and trends in these documents, other perspectives might be present in documents not included, and indeed on research materials that might be gathered through other means. Therefore, assertions made here cannot be taken as definite conclusions about the policies or policy-making processes of particular countries or regions as a whole. Moreover, the documents are constrained by the limitations of politics itself and may not reflect the priorities and concerns of individual policy-makers, committees, or government agencies or departments. Instead, the documents must be understood as contextualised within particular political, national, and regional constraints.

France, Germany, Italy, the Netherlands, Romania, the United Kingdom, the USA, and the EU were selected to provide a geographical and political mix of perspectives. For example, the UK has often been described as prioritizing security over privacy, particularly in relation to the introduction of surveillance technologies and a close relationship with the USA.[6] In contrast, recent debates around the introduction of the Data Retention Directive in Germany suggest that the German government focuses heavily on the data protection and privacy considerations of proposed security policies.[7] Romania, as a former totalitarian state, provides another unique

[5] For more detail on the EU as a site of governmentality, see Ann Zimmerman and Adrian Farell, 'Governmentality, Political field, or Public Sphere?: Theoretical alternatives in the political sociology of the EU' (2011) 14 European Journal of Social Theory 489; William Walters and Jens Henrik Haahr, *Governing Europe: Discourse, Governmentality and European Integration* (Routledge, London 2005).

[6] David Lyon, *Surveillance after 9/11* (Polity Press, Cambridge 2003).

[7] Christian DeSimone, 'Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive' (2010) 11 German Law Journal 291–318. <http://www.germanlawjournal.com/index.php?pageID=11&artID=1240> accessed 27 April 2013.

perspective on privacy and security issues. Finally, despite a focus on Europe, the USA is included as a non-European example because of its prominent role in shaping security discourse internationally, particularly after the events of September 2001.

Security

Understanding the framing of security (and insecurity) within security policy documents is important as these documents contribute towards processes of making different phenomena intelligible as insecurities, and therefore as appropriate objects of security policy.[8] These documents therefore give us a better understanding of the extent of the concept of security and the issues that are brought under its aegis. Particularly important documents in this process are the several national security strategies that have been included.

Concepts of security are heterogeneous across the governments of different countries, and across different policy actors within countries, with multiple, divergent framings of security. However, many of these concepts are more expansive than *national* security, and there is an indication that the scope of security has expanded across all countries in the analysis as more areas of social life are represented as contributing towards security.[9] All concepts include national security, but some countries, such as Romania, make specific mention of fundamental rights and 'democratic security' as component parts of security. Security is seen as necessary for the protection and defence of democracy, fundamental rights and freedoms of citizens, and to assert national identity. The Romanian security strategy defines 'national security' as 'a state of normality to which the citizens, the communities and the state aspire'.[10] It represents security as including economic prosperity and development, full observance of domestic and international law, and socio-political 'balance and stability'. It sees a democratic framework and the exercise of civic rights and freedoms as necessary for achieving national security; this can be understood as aligning with concepts of human security.[11] The French strategy depicts a new approach of considering defence, foreign, and economic policy as part of a whole, whilst still considering their distinctive characteristics.[12] The Italian and French security documents also suggest that concepts of homeland defence are insufficient for security, and that there is a blurring of the division between internal and external security.[13] Several texts also represent the public, European, and national citizens as a collective agent 'calling for security' or having 'security questions' to be addressed by various actors.

Characterizations of the international security environment are more homogeneous across countries, and there are large areas of overlap. This supports the findings of the FORESEC project that observed an increasing overlap of threat assessments in different EU member states.[14] The security documents present a consistent picture of a *new security environment*, often positioned as the motivating factor behind the development of a new security strategy, or prompting reflection upon existing security practices. The 2002 Italian armed forces review identifies a changed international security environment since the end of the Cold War, with the rise of ethnic and nationalist tensions, 9/11 signalling a rise in international terrorism, and a greater public sympathy for overseas military interventions. Threats to security are seen as complex and transnational, and irreducible to static homeland defence.[15] In highlighting the continuity between internal and external security, the French white paper on defence and national security sees the traditional distinction as no longer relevant in the new strategic environment. The document suggests the need to define overarching security strategies and to integrate all dimensions of security. It emphasises the possibility of sudden strategic upsets (uncertainty, sudden breaks, new weapons, technological developments in biotech, nanotech, and space), and of changes affecting the nature of military operations, for example, increasing urban settings for conflict.[16] Against the background of the National Security Strategy[17] and the Strategic

[8] Barry Buzan, *People States and Fear: An Agenda for International Security Studies in the post Cold War Era* (2nd edn, Lynne Rienner, Boulder, CO 1991); Jef Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU* (Routledge, London 2006).

[9] See Giacomo Luciani, 'The Economic Content of Security' (1989) 8 Journal of Public Policy 151; Ian Bellamy, 'Towards a Theory of International Security' (1981) 29 Political Studies 102; and Fierke (n 4), at 42.

[10] Presedintele Romaniei, Strategia de securitate nationala a Romaniei [Romanian national security strategy], (Bucharest, 2007).

[11] Neil MacFarlane and Yuen Foong Khong, *Human Security and the UN: A Critical History* (Indiana University Press, Bloomington 2006).

[12] Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, Le livre blanc sur la défense et la sécurité nationale [White paper on defence and national security] (Paris, 17 June 2008).

[13] Italian Defence Ministry, Libro Bianco, 2002 [The White Paper, 2002] (Centro Studi per la Pace, Rome, 2002).

[14] Bastian Gregerich and Raffaello Pantucci, FORESEC Deliverable D2.2 Synthesis Report (2008). <http://www.foresec.eu/wp2_docs/Synthesis_Report_150808.pdf> accessed 27 April 2013.

[15] Italian Defence Ministry (n 13).

[16] Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration (n 12).

[17] HM Government, 'A Strong Britain in an Age of Uncertainty: The National Security Strategy' (Cm 7952, 2010).

Defence Review,[18] the 2012 report from the UK Ministry of Defence identifies the UK's security context as a dangerous and uncertain world, with continued threats from Al Qaeda and groups in Northern Ireland, and with constrained government budgets.[19] Many texts represent the international security environment as more complex, fast-paced, and uncertain. This environment is portrayed as featuring greater involvement by non-state actors and blurred lines between internal and external security. It is argued to be vulnerable to rapid strategic upset, affected by technological developments, and requiring international cooperation to respond to these new dangers. It is represented as a combination of positive trends with the potential for significant strategic upset.

There is a relatively stable core of what are considered security threats, although with some variations in priority and interests specific to individual states. The European countries see the likelihood of outright, involuntary war as low. International terrorism and related 'asymmetric threats' sit high on explicit security agendas as well as in what can be interpreted from other texts. Information threats, including espionage, major cyber attacks, technological risks, and strategies of influence are also given a high profile. A third source of shared threat for the European countries are areas of instability outside Europe or on the European periphery. 9/11 is the most significant terrorist event in the United States, but is mentioned in subsequent security documents across all countries. The apparent frequency and prominence of these mentions reduces over time, and they become part of a cluster of other security events (e.g. Madrid train bombings in 2004, London 7/7 2005, etc.). The Madrid and London bombings have greater significance in EU security texts than in US texts. In regard to counter-terrorism, there is no mention in these documents of the lead role played by the 'Group of Six' (UK, France, Germany, Spain, Italy, and Portugal).[20] Security documents diverge regarding particular national security priorities beyond international stability and security, and responding to the new security environment, to the concrete security ambitions of particular countries. An example of these specific, context-dependent concerns is Romania's ambition to bridge the divide it perceives between itself and the rest of the EU. France identifies a shift in power towards Asia, whilst the UK government identifies a continued terrorist risk in Northern Ireland.[21] Fundamentally, several countries represent the security context as less predictable and more uncertain than previous contexts.

Several security documents emphasize the importance of knowledge and pre-emption in security practice, relating this to the complexity of the contemporary security context.[22] The Romanian security strategy states: 'In such a tense and complex environment, the security of each individual country, as well as that of the international community as a whole, depends on the ability to anticipate and to undertake predictive action, rather than reacting to events or adjusting to them.'[23] Similarly, the French Defence and Security white paper argues that France's ambition is 'to not submit to this uncertainty, and to harness the knowledge and information revolutions to be able to anticipate, respond to and influence international developments'[24] and that anticipation is a key strategic principle. In relation to surveillance, the paper advocates improved technological development, and additional programmes in relation to intelligence and preparation for the future, including 'knowledge based security, observation, early warning, development of surveillance and armed drones as well as both offensive and defensive cyber war capabilities'. The response to the complex global security situation is to ensure that France harnesses the 'information revolution' to manage increased uncertainty.[25] This identification of the necessity of pre-emption and better security provides ready rhetorical support for surveillance practices in the domain of national and international security.

The texts generally value information exchange between security agencies as an important contributor to security, but there are noticeable differences between countries. The USA's 9/11 Commission report sees an absence of information sharing as contributory to 9/11 and argues for a paradigm shift to the sharing of security information from the previously dominant paradigm of the protection of information.[26] Factors contributing

[18] HM Government, 'Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review' (Cm 7948, 2010).

[19] Ministry of Defence, 'National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security' (The Stationery Office, London 2012).

[20] Wyn Rees, 'Inside Out: The External Face of EU Internal Security Policy' (2008) 30 Journal of European Integration 97.

[21] Ministry of Defence (n 19).

[22] Claudia Aradau and Rens Van Munster, 'Governing Terrorism through Risk: Taking precautions, (un)knowing the future' (2007) 13 European Journal of International Relations 89.

[23] Presedintele Romaniei (n 10).

[24] Ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration (n 12).

[25] Ibid.

[26] 9/11 Commission, The 9/11 Commission Report (Government Printing Office, Washington DC 2004). This paradigm should be understood as protection in terms of protection of intelligence sources and national security, rather than protection of personal information or privacy.

towards the insecurity of the USA in this context include restrictions in communications between security agencies (and with actors such as airlines and airports) and the difficulty of sharing information. The narrative that a lack of shared intelligence or information contributed to 9/11 appears to have taken hold fairly rapidly and to have been pervasive. It can also be seen in documents from the Netherlands.[27] In contrast, German and Romanian documents contain concerns about information sharing between police and intelligence agencies based upon historical experience, and constitutional frameworks.[28] German documents highlight the constitutional separation between police and intelligence functions, linked to the concept of proportionality in some state constitutions.[29] They do not want police acting upon 'soft' intelligence or a blurring of the roles, despite several measures to increase cooperation. These documents do not deny the potential of information sharing to contribute to security and counter-terrorism, but are sceptical of the extent of its effectiveness and attempt to refocus attention upon the motives behind such limitations.

Information security

The concept of national security is expanding in security policy documents across many countries to include *information* security, often under the rhetoric of cyber security, critical information infrastructure or cybercrime. In a German document on the Internet and digital society, data security is discussed more frequently than data *protection* across many topic areas.[30] Italian Guidance on CCTV requires that data controllers provide adequate information security, including measures that minimize destruction, loss, and unauthorized access.[31] This raises the profile of information security to a national level security issue. Many practices of information security are similar to practices of data protection, and good data protection measures contribute towards good information security. Reflecting upon this increasing inclusion of data protection-type activities within security politics, the overlap between information security practices and privacy and data protection practices may allow for the reduction of a perception of a fundamental conflict between security and privacy. On the other hand, the frequently made but erroneous equation of data security with data protection in the fuller sense does a disservice to the latter.

In 2002, the European Parliament underlined the increasing social and economic importance of electronic communications networks, but argued that this requires an adequate legal and policy framework at the EU level to guarantee the protection of network and information security, primarily in order to allow the smooth operation of the internal market.[32] The level of information security, including critical infrastructure and coordination of Computer Emergency Response Teams (CERTs), was seen as inadequate at that time; the context was said to require a specifically European approach, based around the formulation of common definitions and standards, and a European strategy. The Stockholm Programme sees network and information security as compatible with protecting citizen's rights, and talks about establishing a European legal framework for cyberspace.[33] The European Network and Information Security Agency (ENISA) continues this theme, arguing for a cohesive pan-European approach to cyber security. Cyber threats include cybercrime and cyber espionage, and increased dependency upon ICT makes critical infrastructure protection an issue of economic competitiveness and prosperity as well as security.[34] The ENISA report identifies areas where

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

[28] Romanian government. Stenograma audierii publice din ziua de 27 iunie 2006 «Libertate individuală versus securitate naţională. Echilibrul între transparenţă şi secretizare» [Minutes of the public debate organized by the Romanian Government on the subject: 'Individual freedom vs. national security—balancing transparency and secrecy'] (27 June 2006). <http://www.cdep.ro/pls/dic/site.page?den=ap200606_8> accessed 27 April 2013.

[29] Peter Schaar, Wie nachrichtendienstliche Erkenntnisse und polizeiliche Daten zukünftig verschmelzen werden—neue Herausforderungen für die Aufsichtsbehörden? Vortrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen der Conference of DPA's of Federal and Plurinational States [How intelligence data and police data will merge in the future—new challenges for supervision? Speech by Federal Data Protection Commissioner at a Conference of DPAs of federal and plurinational states] Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, (19 March 2009). <http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/2009/PlurinationaleKonferenzMaerz.html>.

[30] Enquete-Kommission 'Internet und digitale Gesellschaft' Datenschutz, Persönlichkeitsrechte, Fünfter Zwischenbericht der Enquete-Kommission 'Internet und digitale Gesellschaft' Datenschutz, Persönlichkeitsrecht [Report of the project group 'Data protection and personal rights' of the Committee of inquiry 'Internet and digital society' (fifth report)] (Bundestag, Berlin 15 March 2012). In data protection discourse and regulation, data security is seen as only one component of data protection.

[31] Garante per la Protezione dei Dati Personali, Decision on Video Surveillance (8 April 2010).

[32] European Parliament, 'Resolution of 22 Oct 2002on the Commission Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security: Proposal for a European policy approach', COM (2001) 298 final.

[33] European Commission, 'Delivering an area of freedom, security and justice for Europe's citizens, Action Plan Implementing the Stockholm Programme, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions' (Communication) COM (2010) 171 final, 20 April 2010.

[34] European Network and Information Security Agency (ENISA), Cyber security: Future challenges and opportunities (Heraklion, 2 December 2011).

current EU approaches to cyber security could be extended.[35] However, in several documents related to data protection, information security is reduced to technical measures.

Privacy, surveillance, and data protection

In a manner similar to the framing of security, these documents provide ways of framing the problematic of privacy, data protection, and surveillance and the appropriate policy and legal responses to these issues.[36] The texts show how these issues are represented as problems. The combination of privacy and security documents in this analysis also permits reflection upon the way the relationship between the related concepts and practices is presented in public texts.

The current EU position on the conflict between privacy and security appears to be that security and fundamental rights (including privacy) are complementary, not in contradiction. Fundamental rights and freedoms are to be 'respected' more than 'balanced'.[37] The language of the 'balancing' of privacy and security is, however, still used at national levels, and can be found in texts from Romania, the Netherlands, Germany, and the UK. The House of Commons Home Affairs Committee asked contributors to comment on the processes they use to conduct 'balancing' between privacy and security.[38] Many scholars have taken issue with the notion of balancing privacy and security, as in a zero-sum game, where the reduction in one is at the expense of the other.[39]

There is broad agreement across these texts on the broad principles involved in privacy, data protection and surveillance, including proportionality, accountability, transparency, trust, consent, and the rights of the data subject. Texts from each EU country include those that are actively advocating greater privacy protection or identifying activities that can infringe upon privacy. Support for fundamental rights and freedoms are explicit in many EU texts. Data protection, privacy and security are all represented as fundamental rights, and the European Parliament asserts that citizens should not have to choose between being free and being safe.[40] Several texts also advocate strict harmonization and equivalence of fundamental rights, including rights to privacy and data protection across the EU, and urge that EU institutions should themselves be compliant with fundamental rights and freedoms.[41]

There are variations across the analysed documents in the representation and use of the concept of surveillance. The term appears to be less frequently mentioned than data protection or privacy across all of these texts apart from those from the UK.[42] The most limited use of surveillance is in the documents from the Netherlands, where surveillance is not a core topic in any document. The French and Italian documents directly refer to surveillance only in terms of video surveillance. In this context, the term is used as a description of a particular visual technology. Documents from the respective data protection agencies reiterate that video surveillance is covered by general data protection legislation.[43] German documents also do not make significant use of the concept of surveillance, but identify Internet surveillance and video surveillance as issues within the broader law and politics of data protection. Romanian documents associate 'surveillance' closely with intelligence activities, and discuss it in the context of counter-terrorism and the adoption of intelligence service practices by the police, with increased potential for unwarranted surveillance arising from proposed intelligence reforms.[44] In the US texts, 'surveillance' is externally directed, with the term being mainly used in relation to foreign intelligence gathering[45] and inadequate surveillance of borders prior

[35] Ibid. These areas include cross-border collection of data relating to cyber security, improved dialogue between information security communities, a proactive approach to building new cross-border communities, modernisation and further development of ENISA.

[36] Kevin Haggerty, 'Surveillance and Political Problems' in Sean P. Hier and Josh Greenberg (eds), *The Surveillance Studies Reader* (Open University Press, Maidenhead 2007).

[37] Other terms that are used in discussing the interaction of privacy and security in other texts include: be 'respected', be 'consistent with', be 'reconciled with', 'balanced with', 'balanced against', 'not interfere with', 'protect', 'support', and 'allow the exercise of'.

[38] Home Affairs Select Committee, 'A Surveillance Society?' HC (2007–08), 58-I; Select Committee on the Constitution, 'Surveillance: Citizens and the State' HL (2008–09) 18–1.

[39] See, for example, Lucia Zedner, *Security* (Routledge, London 2009), 134–137, and for a critique of the concept of 'balance' in the data protection context, see Charles Raab, 'From Balancing to Steering: New directions for data protection' in Colin Bennett and Rebecca Grant (eds), *Visions of Privacy: Policy approaches for the digital age* (University of Toronto Press, Toronto, 1999) 68–93.

[40] European Parliament Resolution 2025/2011 of 6 July 2011 on a comprehensive approach on personal data protection in the European Union,OJ C 291 E.

[41] European Parliament Recommendation 2175/2004 of 14 Oct 2004 to the Council and to the European Council on the future of the area of freedom, security and justice as well as on the measures required to enhance the legitimacy and effectiveness thereof, OJ C 166 E.

[42] This may be an effect of the selection of the UK documents for analysis.

[43] Commission nationale de l'information et des libertés (CNIL), Vidéosurveillance/vidéoprotection: les bonnes pratiques pour des systèmes plus respectueux de la vie privée [Video surveillance/CCTV: best practices for systems more respectful of privacy], (Press release, June 2012); Garante per la Protezione dei Dati Personali (n 31).

[44] Romanian government (n 28).

[45] Charles Doyle, 'Terrorism Legislation: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct

to 9/11.[46] In contrast to the other countries analysed, many of the UK documents are explicitly and directly examining surveillance, including its social consequences and constitutional implications. Several of these documents were produced in response to concerns that the UK was becoming a 'surveillance society'[47] due to increased surveillance infrastructure introduced in pursuit of safety and security since 9/11, with consequences for public trust and the relationship between citizen and state. Given that several of the selected sources focused upon surveillance, the way surveillance is represented in UK documents is accordingly richer. These texts depict surveillance as increasing, both in terms of the surveillance capacity exercised by government and other actors, and the amount of public concern this creates.[48] UK documents also express the need to examine whether current regulation is sufficient to respond to these increases.

In the EU documents, there are several direct mentions of surveillance, but as part of a range of associated privacy and data protection issues. Increased surveillance is one factor (alongside globalization, new technologies, and law enforcement practices) that prompts reconsideration of EU data protection regulation. EU documents state that surveillance measures should be consistent with (or respect) human rights, freedoms, and data protection law. Real-time surveillance is identified as a specific type of intrusive measure, alongside biometrics, telephone tapping, telecommunications data retention, and data-sharing. This use of 'surveillance' is much narrower than that used in the UK documents, essentially referring to a practice rather than to a category. Further, there is little mention in any documents of EU-led surveillance activities and capacities, such as Passenger Name Records, Europol intelligence files, the Schengen information systems, EURODAC, or directives on money laundering.[49]

There are somewhat fewer representations of public calls for privacy present across these documents than there are representations of public calls for security. There are also representations of pressures from the public for more surveillance.[50] The UK Home Affairs Select Committee identifies these as arising from raised expectations on security and policing actors due to technological developments. If security practices are legitimized by articulating a public demand for security, then an absence of such readily articulated public calls for privacy or for data protection may reduce the weight of privacy in any 'balance' against security.

Privacy threats

Different countries have different sets of privacy 'threats'—those risks to privacy that are considered to be the most threatening in a particular context. In the UK, this appeared to be attributed to 'the state' most broadly, and the Home Office and law enforcement agencies in particular. In Germany, this appeared to be the police, intelligence agencies, and the risks of sharing data with the United States. In Italy, the biggest apparent threat to privacy in the analysed documents comes from the private sector. There is a wide and diverse range of privacy problems identified through the documents. These are often common across countries, but particular issues appear to have more salience in some countries than in others. Examples of this include body scanners in Germany[51] and information-sharing between banks in Italy.[52] Several documents are explicitly 'triggered' in response to particular privacy breakdowns or failures that are often taken as emblematic of broader problems either requiring some kind of intervention in response or further evaluation to determine the nature of potential responses.

Technological determinism runs through these texts. Developments in technology are considered to bring about both increased insecurity, but also risks to privacy and data protection. When threats to data protection or privacy arise, they are often portrayed as coming from information technology (such as 'databases') or from information sharing practices, more than from 'surveillance' as a phenomenon. Some documents engage with particular new technological developments, as in the parliamentary debate on body scanners in Germany, or the Article 29 Data Protection Working Party's response to increasing use of facial recognition technology.[53] There is little discussion about the commercial or security origins of technologies, with technological development being presented as a naturalistic *fait accompli*. However, technology use is almost universally positively valued throughout these texts: there are no expressions of 'luddism'. In general, the representation of information systems and technology

Terrorism (USA PATRIOT) Act of 2001' (Washington, Congressional Research Service, Washington DC 26 Oct 2001).

[46] 9/11 Commission (n 26).

[47] Surveillance Studies Network, A Report on the Surveillance Society for the Information Commissioner, (Information Commissioner's Office, 2006).

[48] Home Affairs Select Committee (n 38); Select Committee on the Constitution (n 38).

[49] Joe McNamee, Kristen Fielder, Marie Humeau and Daniel Dimov, EU Surveillance: A Summary of current EU Surveillance and Security Measures (EDRI 2012). <http://www.edri.org/files/2012EDRiPapers/eusurveillance.pdf> accessed 27 April 2013.

[50] Home Affairs Select Committee (n 39).

[51] Bundestag, Plenarprotokoll der 14. Sitzung vom 19.01.2010 [Report of plenary session of the German National Parliament] (Berlin 19 Jan 2010).

[52] Garante per la Protezione dei Dati Personali, 'Data Sharing and Tracking of Transactions in the Banking Sector' (3 June 2011) 127 Official Journal.

[53] Article 29 Data Protection Working Party, 'Opinion 02/2012 on facial recognition in online and mobile services' (WP 192, 22 March 2012).

was as functional unless attacked by a hostile actor, and there is only one discussion about data leaking.[54]

Privacy protecting measures and policy responses

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

Some French and EU texts suggest that increased individual responsibility for, and control over, personal data would be an appropriate response to current data protection, privacy, and surveillance issues. Such increased control is to be achieved through education and awareness campaigns, greater transparency of data processing, and enforced legal rights. The Council of Europe recommends that everyone must be able to control the use by others of their personal data. This requires consent for data collection and processing to be given in advance, and the ability to withdraw consent.[55] Commenting on the proposals for reform of Directive 95/46, the Article 29 Working Party highlights the need for a stronger position for the data subject in the data protection framework, based upon consent, notification of data breaches, and greater transparency.[56] The Council appears also to be moving in this direction, advocating strengthening rights, clarifying the concept of consent, introducing strong rights to object to profiling, greater transparency, rights to data portability, procedures for exercising rights, and the deletion of unnecessary data.[57]

The strongest form of the idea of individual control over data is found in the German texts. These texts are the only ones that explicitly mention rights to informational self-determination. Arising from opposition to the 1983 census, informational self-determination is the legal anchor for data protection in the German constitution.[58] Distinguished from privacy (as the right to be left alone), the data subject is to maintain control of his or her own personal data as part of a general right of personality. Self-determination protects information from one context proliferating into another, and German documents see this as necessary for the development of the individual and as a precondition of free and democratic communities. UK parliamentary documents are actively sceptical of increasing individual control over their personal data as an effective response to privacy and surveillance issues, as it potentially places too great an obligation upon individuals. There is little mention of the 'right to be forgotten' in documents other than in those from France[59] and from the European Commission.[60] The Commission sees the right, understood as the deletion of unnecessary data, as one measure that contributes towards greater individual control of personal data.

Few documents are highly supportive or reliant upon technological responses to privacy problems. There were occasional mentions of privacy enhancing technologies (PETs) and privacy by design (PbD), but across all countries, these are presented as solutions much less frequently than legal, regulatory, and compliance responses. The EDPS sees PbD as a guiding principle for technology and process design.[61] Several of these texts should themselves be understood as a form of response to problems raised by privacy and data protection. EU documents, specifically from the Parliament and Council, suggest various ways in which security and surveillance practices might be themselves subject to monitoring as a way of ensuring that they do not negatively impact upon privacy and data rights. The European Parliament encouraged an independent benchmarking tool for crime prevention, whilst the Council identifies evaluation and impact assessments for responsible organizations.[62]

[54] Bundestag (n 51).

[55] Council of Europe Parliamentary Assembly, Resolution 1843 of 7 October 2011 'The protection of privacy and personal data on the Internet and online media'.

[56] Article 29 Data Protection Working Party, 'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (WP 168, 1 December 2009).

[57] Council of the European Union (10/5731) of 3 March 2010 The Stockholm Programme—An open and secure Europe serving and protecting citizens. OJ C 115/1.

[58] Gerrit Hornung and Christoph Schrabel, 'Data Protection in Germany I: the population census decision and the right to informational self determination' (2009) 25 Computer Law & Society Report 84.

[59] Senat, Proposition de loi, visant à mieux garantir le droit à la vie privée à l'heure du numérique [Proposed legislation to better protect the right to privacy in the digital age] (Paris 23 March 2010).

[60] Commission (EC) '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' COM(2012) 11/4 draft, 25 Jan 2012.

[61] European Data Protection Supervisor (EDPS), Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 18 March 2010.

[62] Parliament (EC), Legislative resolution 14 Dec 2006 on the proposal for a Council decision establishing the Specific Programme 'Prevention of and Fight against Crime' for the period 2007–2013, General Programme 'Security and Safeguarding Liberties', COM(2005)0124; Council of the European Union (n 57).

Privacy impact assessment (PIA) is directly mentioned in UK and EU texts, where they are represented as having considerable merit, as part of self-regulation for individuals and organizations. PIA, and the expanded surveillance impact assessment, is shown as a step beyond legal compliance and a way of determining if surveillance activity conforms with ethical principles. PIA should be built into information processes as a form of risk assessment, and the identification of ways that privacy protection can be included whilst contributing towards socially valuable objectives should be part of the PIA process.[63] The Commission also suggests that greater obligations should be placed upon responsible organizations with regard to good data management and security practices, greater accountability, the burden of proof for legality, data protection impact assessments, and the introduction of security breach notification.[64]

International and national interactions

These documents also feature representations of the interactions between countries, and between countries and international organizations. For the EU Member States, the EU is a significant actor in privacy and data protection. Several texts provide representations of these relationships and what can be understood as strategic policy transfer.[65] The EU exerts pressure upon both sides of the privacy/security 'balance' experienced in national European contexts. This may be due to contradictory policy, an artefact of the scale of the EU or pressures in particular directions arising from the EU policy-making process. Pressures for both privacy and security are mediated at a national level by (at least) two processes: the representation of the role of the EU in the local context and the implementation of EU rulings or measures at the local level.

On the side of privacy, the EU exerts pressure through its normative commitment to fundamental rights and post-communist transition, and through data protection regulations. Dutch documents suggest that the EU could contribute to promoting trust in national government. The EU expresses a strong desire for harmonization and coherence across both security and privacy/data protection policy areas. In 2004, the European Parliament recommended the adoption of joint data protection standards, and the formation of a joint data protection authority, as part of a systematic evaluation of fundamental rights policies in relation to the Area of Freedom, Security and Justice.[66] In 2011, it reiterated the necessity for 'a comprehensive, coherent, modern, high-level framework able to protect effectively individuals' fundamental rights, in particular privacy, with regard to any processing of personal data of individuals within and beyond the EU in all circumstances'.[67] This concept of internationally uniform standards is also present in the Council of Ministers' Declaration on human rights and the rule of law in the information society.[68] It also suggests that the EU should be a driver of international data protection standards and that these should be included in bilateral and multilateral agreements. Proposals for reform also contain an international dimension in which data protection rights are asserted against third-country entities delivering services in the EU or against monitoring the behaviour of Europeans.[69] This necessity of coherence and harmonization is less frequently articulated in texts at the national level, which tend to elevate local contexts and local variations upon privacy and security issues above European harmonization. Harmonization is rarely present as an actual policy goal, and the assumption that harmonized privacy and data protection law across the EU will be economically beneficial is absent (but not contested) elsewhere.

Across most of the documents, the representation of the EU is nuanced. It is both a (necessary) source of security and a support for privacy and data protection rights, but also brings with it membership costs, and its measures can have impacts upon both security and the exercise of rights. Romanian references to the EU include the necessity of transposing the Data Retention Directive despite it being found unconstitutional. They also hold that joining the EU has impacts upon security and privacy, but argue that membership is necessary for security activity (including international action) and that Romanian national security must be aligned with that of the EU and with NATO, even though these may not align with each other. Italian texts also present the EU, alongside NATO, as a reference point for international security. The Italian White Paper states that

[63] Surveillance Studies Network (n 47); Home Affairs Select Committee (n 38); Select Committee on the Constitution (n 38); 31st International Conference of Data Protection and Privacy Commissioners 'Joint Proposal on International Standards for the Protection of Privacy with Regard to the Processing of Personal Data' (5 Nov 2009).

[64] European Commission (n 60).

[65] Irina Gheorghe and Richard Common, 'The Impact of EU Accession on public administration in Romania: the role of strategic policy transfer', 33rd Annual EGPA Conference, Bucharest September 2011.

[66] European Parliament (n 41).

[67] European Parliament (n 40) 2. This reflects the ending of the 'third pillar' as a result of the Lisbon Treaty.

[68] Committee of Ministers Declaration of 13 May 2005 on human rights and the rule of law in the Information Society, CM(2005)56 final.

[69] European Commission (n 60).

Italian military transformations must be aligned with the EU for collective defence.[70] An early Dutch document includes calls from the national level for adjustments to EU privacy policies to increase security.[71] It envisages the EU as contributing towards public trust by its emphasis on the importance of basic rights, and through collaboration and the provision of information. This document actively reflects upon the process of the representation of the EU and is concerned that EU measures may be misrepresented by other political actors.[72]

The French documents broadly positively represent the EU in relation to legal alignment. The general security regulatory framework portrays EU standards on electronic communication as something with which to be harmonized,[73] whilst the Senate proposals for a law to protect privacy in the digital age mirror and potentially pre-empt the implementation of Directive 2009/136/EC.[74] German texts comment upon the unconstitutional nature of the Data Retention Directive,[75] but also imply that the EU has significantly better data protection law than the USA. As might be expected, the US documents in this analysis make no mention of the EU in regard to privacy. Despite being an EU Member State, the UK texts also make no direct link between security, privacy, data protection, surveillance, and EU membership.[76] There are mentions of global influences, but not of the regional context, or of any particular measures or reforms at the EU level, either contributing towards or acting as a barrier to increasing surveillance. In general, external influences upon policy process are downplayed. The non-US documents do not describe any post-9/11 security or surveillance measures as being driven by US expectations regarding speedy security cooperation,[77] but rather frame these measures as a required response to the revealed security problematic of terrorism or global instability. Recent concerns about industry lobbying around data protection reforms are not reflected in these documents.[78]

Countries can also interpret EU directives as they pass into national law, and the documents provide some reflections upon the representation of this process in relation to privacy, security, and surveillance. There are several ways the implementation processes might be represented. A text might downplay the agency of the nation state in comparison to the EU, which might be a sign of either 'policy-laundering' or a genuine feeling of disempowerment; it might present an account of implementation as business as usual, or highlight the agency of the nation state. The processes might be represented as consensual or antagonistic, and the particular choices of implementation might be highlighted or covered over. In relation to the Data Retention Directive, Romanian texts identify elements that can be varied in national implementations, including the time of retention (between six and 24 months), the organizations that can request retained data, and the penalties for non-compliance. More politically powerful, confident, or influential states appear more ready to question EU regulations, and to expect these questions to be taken seriously. This is not to say that other countries do not challenge privacy or security policies emerging from the EU, as the Romanian Constitutional Court challenged the Data Retention Directive. The difference in the texts is somewhat rhetorical. This challenge can be seen in resistance to measures perceived as increasing surveillance, as in German opposition to the Data Retention Directive, but also in national-level opposition to data protection measures originating at the European level. Germany and Romania have currently not implemented this directive, whilst the Netherlands and Italy were previously infringing, but proceedings have since been closed. The UK and France have had no infringement proceedings against them in relation to this directive.

Conclusion

This analysis of policy documents from the seven countries and the EU presents a perspective upon the constitution of the interrelated problems of security and privacy within policy discourse. Both security and privacy can be seen as mature and developed policy issues that have attracted substantial policy attention from a wide range of policy actors. There is diversity in the way that security and privacy are understood and

[70] Italian Defence Ministry (n 13).

[71] Tweede Kamer (n 27).

[72] Raad voor het openbaar bestuur 'Rob-advies Veiligheid en vertrouwen' [Advice to Parliament re security and trust] (The Hague, Nov 2010).

[73] Secrétariat générale de la défense et de la sécurité nationale, Référentiel Général de Sécurité [The General Security Regulatory Framework] (Agence nationale de la sécurité des systèmes d'information, Paris 6 May 2010).

[74] Senat (n 59).

[75] Bundesregierung, Vorratsdatenspeicherung und Sicherheitslücken [Data Retention and Security Vulnerabilities] (Berlin 22 April 2010).

[76] In these texts, we also observed no mention of the UK's role in developing and pushing forward the Data Retention Directive 2006/24 EC under the UK presidency of the Council in the second half of 2005.

[77] Hans G. Nilsson, 'The EU Action Plan on combating terrorism: assessment and perspectives' in Dieter Mahncke and Jörg Monar (eds), *International Terrorism: A European Response to a Global Threat?* (PIE Peter Lang, Brussels 2006).

[78] Liat Clark, 'MEPs copied US lobbyists' Data Protection Regulation amendments verbatim' (14 February 2013) WIRED <http://www.wired.co.uk/news/archive/2013-02/14/lobbyplag-eu-plagiarises-us-lobbyists?page=all> accessed 27 April 2013.

represented, but there is also a strong shared set of norms and assumptions about the nature of political problems in these policy areas that require some form of governmental intervention. Arguably, security has the greater cross-context coherence and there is greater variation in the proposed responses to problems of privacy, data protection, and surveillance.

However, the limited nature of the evidence and the methods used to collect it means that conclusions must be drawn with caution. Nevertheless, there is value in taking the present study as a scoping exercise for a subsequent, fuller analysis that can probe beyond, and further into, documentary sources. The preceding analysis suggests a number of findings for further examination. Among these are the following:

- The core of national security is consistent across countries, but the particular focus of security and threats varies from one country to another.
- Individual national security priorities remain despite shared interests.
- Security is not limited to national defence.
- The international security environment is generally framed as insecure, vulnerable, interconnected, affected by technology, interdependent, and involving non-state actors.
- It is seen as a new security environment, but one in which collective security methods are valued.
- The rhetoric of 9/11 is waning: local, historical, or more recent security events are more salient than 9/11.
- Information exchange for security is often represented as a good thing, except where there are constitutional limitations or negative historical experience.
- Knowledge and pre-emption are seen as important for security, providing rhetorical support for surveillance.
- Information and cyber security are increasingly part of security, which may reduce the imbalance or opposition between the concepts of privacy and security.
- The EU advocates a position in which security and privacy are not fundamentally opposed, that they support each other, and any conflicts can be resolved through appropriate processes; surveillance is less commonly discussed than privacy.
- The UK has the highest level of discussion of surveillance using the terminology of surveillance.
- There is broad agreement across EU policy documents on the core principles of privacy and data protection, although these principles will be open to interpretation. There is broad agreement for increased individual control (or determination) of their own data and strengthened rights for the data subject, but this support varies somewhat across Member States.
- Technological determinism is strongly dominant in policy discourse, although technology is less privileged than law and regulation as a protection for privacy. PETs and PbD are not common solutions, but monitoring and evaluation of the privacy impact is seen as part of a potential solution to privacy and surveillance problems. Countries have 'traditional' sources of threats to privacy, and this will attract (potentially disproportionate) public and policy attention. The 'public' is more commonly represented as calling for or demanding security than it is as calling for privacy, but it is also represented as being in need of privacy and data protection.
- The most common response to problems of privacy or data protection from policy-makers across the EU is policy (law or regulation). Data protection regimes, including data protection authorities, are represented as being at different levels of maturity, and this will affect the next steps or perceived needs. The EU exerts pressure on both security policy and policy regarding privacy, data protection, and surveillance in member states. Different countries experience this pressure differently. In addition, different policy actors represent this pressure differently, and these pressures interact with the perceived maturity of the regulatory regime. More established data protection regimes are able to put up more resistance to non-desirable pressure, while those that are new or that are re-evaluating their regimes may be more open to EU influence than those that are considered mature, stable, and 'generally acceptable'.

doi:10.1093/idpl/ipt014