SWP Research Paper
Stiftung Wissenschaft und Politik
German Institute for International
and Security Affairs

Marie McGinley / Roderick Parkes

Data Protection in the EU's Internal Security Cooperation

Fundamental Rights vs. Effective Cooperation?

RP 5
May 2007
Berlin

SWP
Stiftung Wissenschaft und
Politik
German Institute for
International
and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Germany
Phone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1863-1053

Table of Contents

Marie McGinley holds a master's degree in European Studies from Humboldt University, Berlin. She is currently working as a trainee at the office of the European Data Protection Supervisor. The views expressed here are her own.
Roderick Parkes is Research Assistant of the EU Integration Research Unit.

Data Protection in the EU's Internal Security Cooperation. Fundamental Rights vs. Effective Cooperation?

European home affairs cooperation amongst the EU member states, as well as between the EU-27 and third countries, has often been characterised by the disinclination of national security officials to submit themselves to robust common rules, institutions and human rights standards. Cooperation has frequently occurred outside the formal framework of the European Community/European Union (EC/EU) at a more informal and ad-hoc level. Even within the EC/EU framework, rights standards as well as judicial and parliamentary oversight remain patchy.

This reluctance to submit to robust rules and oversight is commonly viewed as a legitimate means of overcoming the perceived tension at the heart of efforts to provide security in liberal democratic systems: The aim of achieving effectiveness in internal security activities is perceived to be undermined by the exigencies of parliamentary and judicial oversight, as well as—more specifically—human rights protection. Operating in an institutional environment relatively free from parliamentary, judicial and human rights structures, security officials are thus deemed to be in a better position to cooperate effectively: They thereby overcome traditional obstacles to Executive autonomy rendered irresponsible by the demands of the current threat of transnational crime and terrorism.

The present paper questions this assumed tension, showing that, besides safeguarding the freedoms of individuals, common rules and rights standards backed by sturdy oversight structures can actually have beneficial implications for the effectiveness of internal security cooperation. It suggests that the disinclination of security officials to submit to such frameworks for cooperation may have more to do with their desire to retain their autonomy *vis-à-vis* other actors, and less to do with a desire to engage in effective cooperation.

Officials' predilection for looser and less integrated forms of cooperation can thus subject citizens to a dual security threat: Firstly, the abuse of citizens' freedom and privacy may occur thanks to Executives' efforts to provide security within a framework free from proper judicial and parliamentary oversight;

secondly, internal security may be endangered because cooperation between actors is rendered inefficient.

Although they are often the greatest advocates of this *modus operandi*, government ministers may actually find their position imperilled by their officials' reluctance to submit to more formal or integrated cooperation: Carried out in conditions of weak democratic input and oversight, and potentially lacking in efficacy, this kind of internal security cooperation may lack both the legitimacy that derives from popular participation in policy-making (input legitimacy) and that drawn from the effectiveness of measures (output legitimacy). It is politicians, and not officials, who will pay the political price for the latter's desire to retain autonomy.

The paper begins with an examination of the Europeanisation of home affairs cooperation (pp. 7); it suggests that cooperation occurring within a framework of common rules, and robust, supranational judicial and parliamentary oversight can be more effective than that occurring outside. Yet, domestic security officials have taken scant advantage of these opportunities, sometimes pursuing cooperation instead as a means to boost their factual autonomy.

The paper then goes on to look at data-exchange cooperation for security purposes as well as the human rights framework within which this takes place. Again, it suggests that although the existence of robust common human rights (and specifically of individuals' right to data protection) constrain participating officials' autonomy, they can have a beneficial effect upon the effectiveness of data exchange (pp. 12). A critical analysis of the data protection standards that bind EU data exchange reveals a number of serious lacunae though, indicating that these possibilities to increase effectiveness are not being exploited. There have, of course, been recent efforts to upgrade and make more uniform the data protection rights already in place in the Third Pillar of the EU (i.e., the broadly intergovernmental framework in which police cooperation and judicial affairs in criminal matters are handled) through the adoption of a framework decision on data protection. Yet there has apparently been little appreciation at the national level of the fact that an increase in the uniformity and robustness of standards could be beneficial for the effectiveness of policy, and these proposals have met with considerable resistance in Council (pp. 14).

These deficiencies are made pressing by recent developments. A case study of the data-exchange arrangements set out in the EU's recent Passenger Name Records (PNR) Agreement with the United States highlights the disadvantages arising from the absence of strong and uniform data protection standards (pp. 19).

Against this background, a framework decision on data protection should be promptly adopted in order to simplify cooperation between the various EU and non-EU agencies involved in data exchange and to bolster the protection of individuals' rights. This should set out a coherent framework of data protection standards throughout the Third Pillar and cover a wide range of national data-collection and -processing activities.

Furthermore, beyond creating a harmonised framework of data protection, the Framework Decision should set out high and robust standards, particularly in those areas of data protection that are central both to individuals' human rights and to effective internal security cooperation:

- Individuals must be afforded strong rights to be informed about what data are held on them as well as to challenge their veracity. Such rights provide a useful mechanism for ensuring that data exchanged are accurate. In addition, transparency regarding what data are processed helps ensure the proportionality of the measures, and thus that unnecessary activities are avoided.
- Data exchange must be bound by sturdy "purpose limitation" rules to prevent data from being used for purposes other than those for which they were gathered. This will help create a sense of assurance and certainty between those authorities exchanging data.
- The rules on the transfer of EU data to third states must be equally tough, allowing EU authorities to impose high standards on the use of their data by third countries, and again facilitating certainty.
- All these elements must be subject to independent advice and scrutiny provided by a data protection supervisor with wide-ranging powers.

Executive Autonomy and the Europeanisation of Home Affairs Cooperation

Naturally enough, internal security cooperation between the EU member states has not always occurred within the framework of the European Union (EU). The early EU scarcely provided a suitable framework for such work, characterised as it was by a strong focus on economic cooperation and other issues of "low politics". However, the EU's structure and powers have considerably altered since this early period, and it has gained increasing competencies in the area of home affairs. Despite these changes, much of the relevant cooperation between the member states continues to occur outside the framework of the EU's Community- or First Pillar, and even of the more intergovernmental Third Pillar of the EU which was purpose-built to house such cooperation and in which the European Parliament, Court and Commission are relatively marginalised.

If the participating governments' arguments are to be believed, deviations from the Community and Third Pillar frameworks are not merely to be traced to their reluctance to cede and pool responsibility for a policy area of central importance to national electorates; nor do these deviations apparently derive from less defensible concerns on the part of the relevant sections of national governments about giving up their own autonomy and potentially relegating themselves to a secondary position in the national and European political system: These deviations have been (often tacitly) justified by reference to the idea that oversight by—and rule-making which involves—the European Commission, Parliament (EP) and Court (ECJ) as well as the full number of interested EU states would be detrimental to the efficiency and effectiveness of their internal security cooperation.

The Parliament, Court and Commission are, for example, seen as being too cumbersome to meet the immediate challenges of transnational security threats, as well as promoting rights and interests out of step with the realities of these challenges. Given the important role usually associated with these bodies (democratically representing citizens' interests; protecting individuals' legal rights; identifying a common European interest) it is salient to ask whether such reasoning is well-founded. Has the influence of the European Commission, Parliament or Court in home affairs cooperation between the member states really been detrimental to its efficiency and effectiveness? Similarly, are efforts to involve all EU member states in cooperation detrimental to effective policy or efficient policy-making?

This chapter sketches out the driving factors behind European cooperation in the area of internal security and home affairs. It looks at cooperation at an EU level, both within the formal structures of the intergovernmental Third Pillar established by the Maastricht Treaty, and that drawn into the First Pillar framework of the European Community especially from 1999. It also seeks to identify the forces driving internal security cooperation between small groupings of EU member states "below" the level of the EU—a marked phenomenon in the 1970s which continues to this day. The chapter addresses the question whether the development of *ad hoc*, informal and transgovernmental forms of cooperation below the EU level has been the result of efforts to match rational, effective measures and modes of cooperation to emerging problems. Can it instead be traced to the narrow interests of the relevant sections of member-state governments—and specifically national security officials' desire to retain the autonomy that they enjoy under looser forms of cooperation?

Europeanisation as a Result of National Bureaucratic Activism

An increase in terrorism at the beginning of the 1970s in Europe led to the recognition that the fundamental freedoms which the European Communities sought to realise—namely the free movement of persons, goods and capital—were susceptible to abuse. Particularly from the mid-1980s, as efforts to facilitate the movement of persons between the member states extended beyond workers to include ordinary travellers, it became clear that sovereign states could not tackle terrorism and other forms of criminality solely within their domestic contexts. Although the causes and effects of terrorism were still largely internal to individual member states (notably Germany, Spain and

the United Kingdom), the greater opportunities for individuals to travel and communicate between states afforded terrorists increased channels to perpetrate attacks, and meant that internal security cooperation within a European framework was necessary. The end of the Cold War—and the subsequent emergence of more complex forms of transnational criminality and terrorism—compounded this fact, even if the origins and/or causes of this terrorism were increasingly located *outside* the EU.

Starting in the mid-1970s, EC member states began to cooperate informally in an effort to meet these emergent problems through the TREVI Working Group, which dealt with matters of terrorism and policing. Within the overarching framework of this group, various specialist formations developed over the years, the principal sub-groups dealing with terrorism, organised crime and the facilitation of the police cooperation. The main aim of the—now defunct—TREVI Group was the exchange of information and best practice relating to the fight against terrorism, as well as the development of common strategies between member states.[1]

Home affairs cooperation between the member-state authorities therefore occurred within an Executive-dominated institutional framework, relatively free from judicial, parliamentary and popular oversight. The TREVI Group had no basis in Community law and was thus not part of the institutional framework of the EC. This left the European Parliament and European Court of Justice without formal rights of control. The Group's working reports were not published and it was not accountable to national parliaments—a particularly crucial point considering that not only security issues were at stake, but also civil liberties.

By pooling their autonomy in a limited way with like-minded actors in other states, national home-affairs officials were able to use the institutional framework of the TREVI meetings to extend their autonomy *de facto vis-à-vis* other national actors. As a result, European home affairs cooperation occurred not only as a rational response to the problems generated by the increase in free movement between European states: control-oriented political, administrative and operative sections of national Executives were able to realise policies through European cooperation which would have been impossible to achieve in a purely domestic setting, thanks to precisely the parliamentary and judicial oversight that was lacking at the European level.[2] Thus the German Interior Ministry's recent attempts within the framework of the Executive-dominated G6 meetings (the six-monthly gatherings of the interior ministers of the six largest EU member states) to see domestic secret services gain broad access to data held within the EU's Schengen Information System (SIS-II)—despite domestic opposition to the liberalisation of German rules strictly regulating access to equivalent data—have a long pedigree.[3]

Analysis elsewhere has suggested that national bureaucrats and agencies were, at the very least, selective in the information that they released to politicians and the public, leading to misperceptions of the security threat likely to "spill over" as a result of free movement, and thereby legitimating their activities. A number of reports released—in the main, prior to the removal of the EU's internal borders—created an unwarranted fear of a phenomenon termed "Euro-crime".[4] Thus, policies and issues that were sometimes only loosely connected with core transnational security threats were reconceived as such and uploaded to the European level for treatment.

1 Gunter Warg, *Terrorismusbekämpfung in der Europäischen Union*, Speyerer Arbeitsheft Nr. 145 (Deutsche Hochschule für Verwaltungswissenschaften Speyer, 2002), p. 53.

2 For an analysis of this early cooperation and the motives underpinning it: Didier Bigo, "The European Internal Security Field: Stakes and Rivalries in a Newly Developing Area of Police Intervention," in *Policing across National Boundaries,* Malcolm Anderson and Monica Den Boer eds. (Pinter publications, 1994); Virginie Guiraudon, "The Constitution of a European Immigration Policy Domain: A Political Sociology Approach," *Journal of European Policy* 10, no. 2 (April 2003). Monika Bösche, "Trapped inside Fortress Europe: Germany and the European Union Asylum and Refugee Policy," paper presented at the 44th Annual Convention of the International Studies Association in Portland, February 25–March 1, 2003.

3 On the question of access to SIS-II see the Motion of the Left Party, "Zugriff von Geheimdiensten auf das Schengener Informationssystem der zweiten Generation verhindern," 16/3619, November 29, 2006.

4 For analysis of the political effect of these reports see: Andrew Geddes, *Immigration and European Integration: Towards Fortress Europe?* (Manchester: MUP, 2000), pp. 22–26; Simon Hix, *The Political System of the European Union* (Basingstoke: Macmillan, 1999), p. 325; Andreas Maurer/ Roderick Parkes, "The Prospects for Policy Change in European Asylum Policy," paper presented at the Workshop on Migration and Security, Berlin, March 2006, http://www.midas.bham.ac.uk/Maurer-Parkes-Workshop.pdf. For analysis of more recent events: Ian Loader, "Policing, Securitization and Democratization in Europe," in: *Criminology and Criminal Justice*, Vol. 2 No.2, (2002): pp. 125–153.

This was, for example, the case with issues of immigration and asylum, which became conceptually linked to hard, internal security threats such as terrorism.[5]

The Benefits of Formal EU Structures for Efficient Policy-Making and Effective Policy

Many home affairs issues initially dealt with outside the EU framework as issues of transnational criminality and terrorism have been increasingly drawn into the mainstream process of European integration, with the Community institutions gaining more formal as well as informal influence over them. The participation of the Parliament, Court and Commission in such policy areas does, however, remain uneven.

Asylum and immigration policies are now legislated for within the EC framework, employing almost all facets of the "Community method" of policy-making. The European Commission thus enjoys a sole right of initiative and the Parliament has accrued co-decision rights over all major areas of asylum and immigration policy apart from legal immigration. Only the considerably restricted powers of the European Court over asylum and immigration remain an anomaly. Issues of police and judicial cooperation in criminal matters are, meanwhile, still largely dealt with outside the EC structure, in the Third Pillar of the EU. The powers of the EP and ECJ are extremely narrow in this area: While the EP only has the right to be consulted in Third Pillar matters[6] and can thus merely delay but not veto nor directly influence proposed measures and legislation, the ECJ's powers are granted at the member states' discretion. Under Article 35 (2) of the Treaty on European Union (TEU), member states can grant the ECJ jurisdiction over referrals from national courts on the validity and interpretation of EC laws. However, only 14 member states have done so: of the EU-15, Ireland, Denmark and the United Kingdom have not; of the post-2004 member states, only the Czech Republic and Hungary have.[7]

What explains the gradual integration of home affairs cooperation into EU and particularly into EC structures? This may not always have been the product of efforts to match rational, effective solutions to the member states' mutual security problems. In part, it has been the result of the Community actors mobilising allies outside the policy process, and creating political pressure on member-state governments to involve them in policy-making. The EP has, for example, sought to form alliances with NGOs, highlighting the need for greater democratic participation in justice and home affairs cooperation. Thus just as the pursuit of institutional interests can be found in the national bureaucratic activism that drove early cooperation, it finds parallels in the subsequent efforts of the supranational institutions to expand their role in policy-making.[8]

EP-induced political pressure does not, however, entirely explain the increasing role of supranational rule-making in home affairs policy-making: The communitarisation of policy-making offers benefits for the efficiency of policy-making and effectiveness of policies. The Commission has successfully increased its formal role in policy-making by offering a means to "neutralise" agenda-setting in this area of high political salience for national governments; it thus helps prevent ideas and proposals from merely reflecting the priorities of a certain member state, and promotes instead what it views as the common interest. Moreover, it has also played a strong—if unbidden—role, putting forward ideas for the better regulation of European home affairs which make fuller use of the range of policy tools available at the European level. Supranational judicial, parliamentary and executive oversight also reduces the likelihood that member states will fail to properly implement common policies.[9] Given the interdependencies between the EU-27, the most effective policies in this area are often those that involve all the member

5 Bigo, "The European Internal Security Field" [see n. 2]; Virginie Guiraudon, "European Integration and Migration Policy: Vertical Policy-making as Venue Shopping," *Journal of Common Market Studies* 38, no. 2 (June 2000): pp. 251–271; Eiko Thielemann, "The Soft Europeanisation of Migration Policy," paper presented at ECPR Joint Sessions of Workshops, Turin, March 22–27, 2002.

6 Article 39 TEU.

7 Steve Peers, *Transferring the Third Pillar*, Statewatch Analysis, May 2006, p. 7.

8 Jörg Monar, "Democratic Control of Justice and Home Affairs: The European Parliament and National Parliaments," in *Justice and Home Affairs in the European Union: The Development of the Third Pillar,* Roland Bieber and Jörg Monar, eds., (Brussels: Interuniversity Press, 1995).

9 See James Walsh, "Intelligence-sharing in the European Union: When Institutions Are Not Enough," *Journal of Common Market Studies*, Vol. 44, No. 3, (2006): pp. 625–643, p. 630.

states, whether these be the largest states, the best equipped to provide security or those most adversely affected by the problem at hand. This is indicated by the way in which the UK in particular has been cajoled into opting in to asylum policy measures and punished for its pick-and-choose attitude to migration policy. The communitarisation of policy-making facilitates efficient decision-taking between the member states by abandoning the principle of unanimity.

The Prüm Convention: A Product of the Search for Effectiveness or for Autonomy?

Despite these benefits for efficient policy-making and effective policy, commentators have recently noted the tendency of national home-affairs officials and agencies to seek out modes of operational and policy-making cooperation outside the EC/EU structure, even shifting those areas of policy receiving formal EU treatment to decision-making fora below the EU level.[10] Typical of this trend is the conclusion of the Prüm Convention in May 2005 between a small number of EU member states (Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria) outside the EU framework.

The Prüm protagonists have loudly protested their allegiance to the EU and the Convention is touted as an innovative means to facilitate EU integration[11]: Despite the fact that they relied upon modes of co-operation below the EU level, their apparent intention was to drive on EU integration in a way currently impossible given the reluctance of some EU member states to introduce qualified-majority voting in Council. The initial signatories of the Convention thus declared themselves eager to agree on rules for cooperation in three policy areas (cross-border crime, terrorism and illegal immigration), in which they feared consensus would prove elusive if they went through the regular EU channels.

At the heart of the Prüm Convention lie efforts to improve data exchange between the participating states for the purposes of combating crime and terrorism. According to the Convention, authorities seeking data must engage in a two-step process: They first go online, comparing the DNA and fingerprint data of the suspect with the equivalent information on the databases of contracting states. Although they may "make a hit", that is match their DNA data with data held elsewhere, they do not gain automatic access to the details on the data subject's identity held by the other state. In the case of a hit, any additional information requested in a second step is thus subject to the national legislation and procedures of the state holding the data. In this, the participating agencies maintain a high degree of discretion in the decision over whether to hand over data. By contrast, the "principle of availability", which was endorsed by the heads of state and government of the then EU-25 in 2004 and is already the subject of a Commission proposal, was to be realised by setting out common criteria about which data on a suspect's identity are to be released. Although the Commission proposal is rather modest, it could thereby go some way in overcoming the divergences in national law that have proved so disruptive to effective cooperation in the past, but which are maintained under Prüm.[12]

Given the Convention's substantive content and mode of adoption, it is questionable whether the Prüm signatories' predilection for policy-making below the EU level derives exclusively from the fact that EU decision-making still occurs under unanimity in most of the areas dealt with by the Convention. The Convention's *apologia*, which implies that it marks some kind of pragmatic response to the disinclination of *other* EU governments to give up autonomy in this area, is thus thrown into doubt. Instead, it should be asked whether the Convention is not, instead, a counter-reaction on the part of its signatories to the growing constraints on their autonomy at the European level: Negotiations began on the cusp of the 2004 enlargement, an event heralding the advent of a large number of states whose standards of, and capacity for, data collection and exchange are often seen as inferior

10 See Daniela Kietz and Andreas Maurer, *From Schengen to Prüm. Deeper Integration through Enhanced Cooperation or Signs of Fragmentation in the EU?* (Berlin: Stiftung Wissenschaft und Politik [SWP], German Institute for International and Security Affairs, May 2006), SWP Comments no. 15; Daniela Kietz and Andreas Maurer, Folgen der Prümer Vertragsavantgarde: Fragmentierung und Entdemokratisierung der europäischen Justiz- und Innenpolitik? (Berlin: SWP, January 2007); Thierry Balzacq et al., *Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats* (Brussels: Centre for European Policy Studies [CEPS], January 2006), CEPS Working Document, no. 234, pp. 1–23; Andreas Maurer and Roderick Parkes, "The Prospects for Policy Change in European Asylum Policy," paper presented at the Workshop on Migration and Security, Berlin, March 2006, http://www.midas.bham.ac.uk/Maurer-Parkes-Workshop.pdf.

11 Article 1 (4), Basic Principles of the Convention.

12 Kietz and Maurer, *From Schengen to Prüm* [see n. 10].

to those enjoyed by the Prüm signatories. Moreover, in the form of the principle of availability, the Commission began driving a data-exchange agenda that could have seen participating national agencies give up a broad degree of control over data-exchange processes. The "Prümers" may be seen to have disrupted that agenda. Finally, at the time of negotiation, the powers of the European Parliament and Court in this area looked set to grow thanks to the changes foreseen in the European Constitutional Treaty. By adopting the Prüm Convention, far removed from supranational parliamentary oversight, its signatories have factually reduced the EP's already limited capacity to alter the version uploaded to the EU level, as well as preempting any possible increase in its powers.

Autonomy vs. Effectiveness?

In sum, then, the fuller integration of home affairs cooperation between EU member states offers certain functional benefits that can improve the efficiency of policy-making and the effectiveness of policy. Yet, whilst the Prüm signatories have, for example, recognised that the communitarisation of policy-making might boost the efficiency of decision-taking in Council, they appear more sceptical about the benefits of bolstering the role of the European Commission, Parliament and Court. All the same, the Community bodies can be instrumental in neutralising agenda-setting and reducing defection from common policies. Of course, officials' and ministers' disinclination to involve these bodies too heavily in policy-making may derive from a perfectly defensible desire to retain responsibility for a highly sensitive policy area of core importance for national voters. Nevertheless, it should be recognised that these actors have a certain self-interest to ensure that only those actors that most closely share their preferences are involved in policy-making, not least because this can facilitate agreements that would have proved impossible in a purely national context.

Home affairs policy-making below the level of the EU has, meanwhile, tended to reproduce forms of cooperation with a comparatively low degree of integration, sometimes failing to make full use of collective action and the full range of policy tools open to the EU. The Prüm Convention and its provisions for data exchange conform to this trend. Of course, officials' predilection for less integrated forms of data exchange as set out in the Prüm Convention may derive from a perfectly justifiable unease at the centralised mechanisms that are employed in the more integrated data-exchange models. Officials' preference for regulating the transfer of data themselves on a case-by-case basis can, for example, derive from the fact that they fear being held politically accountable for the abuse of data which they themselves gathered and transferred. Yet by pooling autonomy on this matter, national governments may actually enjoy better chances of ensuring the responsible use of data *after* it leaves the national domain: Whilst exchange rules under the Prüm system seek to ensure the responsible use of data by third countries primarily by imposing strong *a priori* checks on their transfer, those rules ideally accompanying the principle of availability would also be *ex posteriori* in nature, providing mechanisms to regulate the use of data after they have left the jurisdiction of the state that collected them.

Against this background, it should be acknowledged that, since security officials' political clout *vis-à-vis* actors in their own countries and other member states (including their supposed cooperation partners) broadly correlates with the degree of information that only they enjoy, these security officials may also be seen to have a strong self-interest in regulating data exchange on their own terms. The retention of control over the conditions under which data are transferred allows them to "err on the side of caution": By citing concerns about how data will be used by another country, officials and politicians can disguise a desire to retain information for themselves.[13]

13 For a brief overview of the current state of affairs: Marie McGinley and Roderick Parkes, *Data Protection at the European Level: A Stocktaking of the Current State of Affairs*, SWP Working Paper, 4/2007, p. 7.

Effective Data Exchange and Fundamental Rights: A Zero-Sum Relationship?

Even if supranational rules and institutions do not appear generally detrimental to the efficiency and effectiveness of member states' internal security cooperation, what of the specific influence of supranational human rights standards? The implications for data-exchange arising from robust (or deficient) data protection rights are what principally concern us. The implementation of robust rules can certainly impede on the autonomy of participating authorities, but does this come at the detriment of effective cooperation?

The international exchange of information (both raw data and intelligence) has become a cornerstone of efforts to combat internal security threats faced by EU member states. Data- and intelligence-sharing between states is, for example, key to preventive counterterrorist measures as well as to efforts to bring the perpetrators of terrorist attacks to justice. The effectiveness of exchange is therefore imperative, and, insofar as it might be supposed to undermine this effectiveness, the maintenance of human rights standards formulated before the onset proper of transnational terrorism may legitimately become the subject of public and political debate.[14]

Safeguarding Privacy: The Accepted Rationale behind Data Protection Rules

The collection of data about individuals on the part of Executives is undoubtedly an indispensable part of states' efforts to provide internal security. It is, however, open to error and abuse. Governments may, for example, be tempted to collect and circulate information about individuals amongst various national agencies that is in reality superfluous to internal security measures but useful for other purposes.

In order to circumscribe error and "Executive abuse", liberal democracies have developed safeguards to protect individuals' freedom from state interference and to ensure a degree of "data protection" (i.e., rules governing what personal data can be collected and what use can be made of it) for reasons of privacy as well as of freedom of expression, movement, association, conscience and religion.

Yet, international data exchange for the purposes of combating terrorism opens new avenues for the abuse of information about national citizens—this time *outside* the national jurisdiction: Intelligence and data collected and stored under the highest standards in one state may be complacently circulated once transferred to another.

A desire to avoid the complacent treatment of data outside the national jurisdiction might lead to the improvement of data protection standards in the transmitting states and to their developing restrictions on the kinds of data to be released. Similarly, it might give rise to an international "race to the top" in data protection. Third states would thus receive data only on condition that they improve their data protection standards.

In reality though, and given the importance to them regarding security concerns, states may put considerable diplomatic pressure on each other to hand over information held on certain categories of individuals, whilst refusing to upgrade the protection they afford to those data. The United States, which by European standards offers a relatively low level of data protection, is, for example, in a position to exert substantial pressure on the EU member states to hand over data. In order to ensure that agreements are reciprocated and that they receive the data necessary for their own internal security efforts, and with an eye to avoiding sanctions in other areas, EU member states may prove susceptible to such pressures.

All this would point to a clear need for robust data protection standards in the EU, not only detailing criteria for intra-EU exchange but also for the release of data to third countries. Yet, the imposition of high protection standards might be deemed irresponsible, and the desire to protect individuals' privacy relativised, insofar as these standards undermine efforts to provide security. To what degree is this the case?

14 For a recent analysis of the debate about human rights and internal security in Britain see: Roderick Parkes and Andreas Maurer, *Britische Anti-Terror-Politik und die Internationalisierung der Inneren Sicherheit: Zur Balance zwischen Freiheit, Sicherheit und Demokratie* (Berlin: Stiftung Wissenschaft und Politik, January 2007), SWP-Studie 3/07.

Increasing the Effectiveness of Intra-EU Data Exchange: The Added Value of Robust Data Protection

The elaboration of EU-wide data protection standards, and their robust enforcement, could actually have a beneficial effect on the effectiveness of data exchange between member states:

- Member states should be happier to hand over data to each other if the receiving state is bound by clear rules about what use it can make of it (for example, purpose limitation rules backed by scrutiny from an independent data protection supervisor).[15]
- A set of standards of data protection common to various states and bodies could facilitate a more efficient exchange of data between agencies otherwise bound by divergent rules.
- Giving individuals robust rights to be informed that data are held on them as well as to challenge the veracity of these data constitutes a useful mechanism to ensure that accurate information is exchanged.[16]
- By according the individual the right to be informed, procedures are rendered more transparent; this provides a means of assessing the proportionality of measures, helping to avoid unnecessary cooperation.

By contrast, the absence of robust, common data protection rules may damage the effectiveness of exchange: Rather than trusting in common data protection rules and institutions to ensure that their data are not misused by receiving states, security officials will use the discretionary non-transfer of information as a safeguard against data abuse—if there is deemed to be a danger of abuse by a third state, it is decided on an *ad hoc* basis not to transfer the data.[17] As noted above, in some cases, security officials may even tend to be overly "cautious" in the transfer of data: Their political influence directly correlates with the informational asymmetries that they enjoy over other actors; by sharing information, they can lose clout.

The absence of strong human rights standards in the area of data exchange can therefore subject individuals to a double security threat: firstly, that arising from the abuse of their privacy and freedoms by security officials, and secondly, that arising from ineffective cooperation.

15 *Second Opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, Brussels, November 29, 2006.
16 House of Lords, *Fortieth Report: Behind Closed Doors: the Meeting of the G6 Interior Ministers at Heiligendamm*, 2006.
17 Again, see: Walsh, "Intelligence-sharing in the European Union" [see n. 9].

Increasing the Effectiveness of Data Exchange with Third States: The Added Value of Robust Data Protection

Should the EU bind itself to high data protection standards, this may also encourage third states to supply it with data:

- A high standard of protection in the EU will encourage external cooperation partners in their belief that their data will be used responsibly by EU authorities.
- Robust, common data protection standards may help individual member states maintain special data-exchange relations with a third country (such as between the United Kingdom and United States): greater transparency of intra-EU data exchange will allay third country's concerns that sharing data with a favoured member state may actually open avenues for the misuse of its information by the rest of the EU-27. By the same token, it may also encourage the favoured member state to engage in data exchange with other EU members, more secure in the knowledge that this will not jeopardise its special data-exchange arrangements with third countries.

All the same, although high intra-EU standards might induce third countries to share information with it, it would have little positive effect upon the EU's readiness to share its data with third countries. Yet its willingness to supply third states with data can be beneficial to its own provision of internal security in two ways: firstly, by ensuring that it is not subject to attacks launched from third states which could have been prevented had it shared data; secondly, by encouraging a reciprocal readiness to supply data on the part of a third state.

How can the EU best foster favourable conditions under which to transfer data? Although the EU's data relations with third countries might well benefit from the kind of strong common rules and oversight capable of being set up for data exchange between the EU-27, such arrangements remain a more distant prospect in practical terms. Thus the best way to ensure that EU data is not abused by third states remains through the implementation of robust *a priori* checks.

The Inconsistencies and Deficiencies of EU Data Protection Standards

Analysis of data protection standards in the EU strongly suggests that their architects were unaware of, or uninterested in, the benefits which robust standards offer for effective internal security cooperation.[18] Data gathered and exchanged within the legal framework of the First Pillar of the EU (principally commercial data) are, it is true, bound by the relatively robust Data Protection Directive of 1995[19] which set up an independent advisory group known as the Article 29 Working Party. Moreover, under the Amsterdam Treaty, an independent supervisory authority was provided for, and realised in 2004 in the form of the European Data Protection Supervisor (EDPS). Yet in the Third Pillar, which provides the framework for the EU's core internal security efforts, standards remain patchy. The various agencies and information systems (Schengen Information System, Europol, Eurojust, Customs Information System) that are housed within this framework employ their own protection standards, some of which show serious lacunae. Meanwhile, data exchange between national agencies remains largely subject to national laws.[20]

Of late there has, however, been an apparent desire amongst decision-takers to tackle the data protection inconsistencies between the different European agencies and information systems found in the Third Pillar. Moreover, from 2004, efforts to facilitate data exchange between *national* authorities, according to the abovementioned principle of availability, increased pressure for harmonised Third Pillar protection standards covering that data. Indeed, in the so-called Hague Programme, the EU's heads of state and government made the development of the principle of availability semi-conditional on the adoption of a data protection measure.

At the Spring 2005 Conference of European Data Protection Authorities (DPAs), in Krakow, the data protection authorities of the member states called for harmonised rules.[21] The issue was taken up by the Commission in October 2005, when it put forward a proposal for a framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (hereafter referred to as DPFD-1).[22]

The Demise of the First Draft Framework Decision on Data Protection in the Third Pillar

In the run-up to the German Presidency (first semester of 2007), which withdrew it, DPFD-1 was extensively debated and modified in the Council. It was also the subject of considerable pressure from the European Parliament, which has little *de jure* influence over the content or adoption of a measure regulating data protection in the Third Pillar, but has sought by means of an "issue-linkage" to increase its real powers over the measure: It made its acquiescence to member states' priorities in a dossier over which it enjoyed greater powers (the recent Directive on the retention of telecommunications data), conditional on their prioritising the adoption of a data protection framework decision.

The main issue of contention in negotiations prior to the German Presidency was the scope of DPFD-1, and in particular, whether or not it should be limited

18 For an overview of the current data protection landscape in the EU see: Marie McGinley and Roderick Parkes, *Data Protection at the European Level* [see n. 13].

19 Directive EC 95/46 of the EP and of the Council of October 24, 1995 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data."

20 For a detailed analysis of the discrepancies between data protection in the First and Third Pillars see: Johanna Kübler, *Die Säulen der Europäischen Union: einheitliche Grundrechte? Zur Grundrechtsdivergenz zwischen der ersten und dritten Säule am Beispiel des Datenschutzes* (Baden-Baden: Nomos Verlag, 2002). In addition, for a discussion on data protection standards in individual Third Pillar bodies and systems, see Spiros Simitis, *Der verkürzte Datenschutz: Versuch einer Korrektur der Defizite und Diskrepanzen im justitiellen und Sicherheitsbereich der Europäischen Union* (Baden-Baden: Nomos Verlag, 2004).

21 Position paper on "Law Enforcement & Information Exchange in the EU," Spring Conference of European Data Protection Authorities, Krakow, April 25–26, 2005, p. 4.

22 MEMO/05/349, Brussels, October 4, 2005.

to cross-border data transfer between the member states or if it should include the transfer of data to third states and even the domestic collation and processing of data which would not necessarily be transferred to other states.

Member states which opposed the inclusion of domestic data processing activities within the DPFD-1's remit had argued that this would be contrary to the principle of subsidiarity and even disproportionate. The United Kingdom, for example, pointed out that only a small amount of police cases have a cross-border dimension and it would therefore be disproportionate to subject this processing to a European data protection regime.[23] Some member states even questioned whether there was a legal basis in the Treaty on European Union which would justify the inclusion of domestic processing within the scope of such a Framework Decision; this challenge came despite the positive findings of the Commission's legal services.[24] In fact, the advantages of the Framework Decision covering all three kinds of data exchange are clear: harmonised standards would afford the individual a consistent level of data protection, as well as offering a greater degree of legal certainty and potentially facilitating exchange.

When negotiations in the Council were eventually deemed to have stalled due *inter alia* to disagreements about the scope of DPFD-1, the proposal was sent back to the Commission for revision in January 2007.[25] However, before this could occur, the German Presidency put forward its own draft proposal (DPFD-2).[26]

Evaluating the Draft Data Protection Framework Decision

As discussed above, a sturdy data protection framework requires the respect of a number of principles key both to the protection of individuals' privacy and to the effectiveness of internal security cooperation. DPFD-2 falls short of these principles on a number of counts:

- The establishment of a consistent set of data protection standards would facilitate data-exchange cooperation that would otherwise be disrupted by the hurdles posed by divergent protection standards. Unlike those set out in the rejected DPFD-1, these standards would ideally stretch not only throughout the Third Pillar, providing a common framework for the various EU bodies (Europol[27], Eurojust) and information systems (Schengen Information System, Customs Information System) housed there, but also to data collation and processing by, as well as data exchange between, national authorities. However, rather than resolving the issues related to scope that plagued DPFD-1, DPFD-2 would further confuse the issue. While Recital 6a states that standards for domestic processing shall match those provided for in the Framework Decision, this is not inserted as an *obligation* into the (legally binding) body of the text. In fact, this is merely something which member states "intend to ensure."[28] Furthermore, it hardly seems conducive to legal certainty or to the provision of con-

23 Council of the European Union, Note from Presidency to Article 36 Committee/Coreper/Council Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters—Scope: application to processing of data in a purely domestic context, document no.: 8175/06, Brussels, April 6, 2006 [hereafter cited as Note from Presidency to Article 36].

24 The position of the Commission throughout negotiations was that having separate data protection regimes could not be justified, as even data collected within the context of an internal investigation could at some stage be exchanged with a foreign authority. There was also apparently a majority of member states who supported this part of the proposal. For a discussion of this see: Note from Presidency to Article 36; Council of the European Union, Note from Presidency to Coreper. Questions on scope, document no.: 13918/1/06, Brussels, October 31, 2006; Council of the European Union, Note from Presidency to Coreper/Council, Questions to the Council, document no.: 15431/1/06, Brussels, November 22, 2006.

25 Note from Presidency to Article 36, document no.: 5435/07, Brussels, January 18, 2007.

26 Note from Presidency to Article 36, document no.: 7315/1/07, Brussels, April 24, 2007. This draft is a slightly amended version of one originally submitted by the German Presidency on March 13, 2007. Unless otherwise stated, in the following discussion, "DPFD-2" refers to the draft submitted in April 2007.

27 The legal status of Europol is due to undergo significant changes. Following discussions at the JHA Council in June 2006 to replace the Europol Convention with a Council decision based on Article 34 (2c) TEU, the Commission presented a proposal on December 20, 2006 (COM (2006) 817 final).This would establish Europol as an agency of the Union.

28 This is one of the provisions which was re-drafted after the proposal submitted on March 13 was discussed in the Council. The draft of March 13 had been slightly more specific in that it stated that "Member States will also apply the rules of the Framework Decision to national data-processing, in order that the conditions for transmitting data may already be met when the data are collected."

sistent data protection standards to exclude "activities *specific to national* intelligence services"[29] [emphasis added] from the scope of the Framework Decision.

- Affording individuals strong rights—including the right to be informed about the data that are held on them as well as the right to have inaccurate or irrelevant data amended or deleted—is essential both for protecting the individual and for ensuring effective cooperation between law enforcement authorities (exchanging data which are inaccurate, irrelevant or obsolete would clearly be counterproductive for internal security efforts). In addition, transparency regarding what data are processed helps ensure the proportionality of the measures, and thus avoids unnecessary activities. DPFD-2 goes further towards realising these benefits than its predecessor, in that it provides for a general obligation for member states to ensure that the competent authority informs the data subject (i.e., the individual upon whom data is held, irrespective of their nationality or place of residence) about both the collection and processing of their personal data.[30] The reasons for refusing access to this data set out in Article 17 (2) are similar to the equivalent provisions in Article 21 (2) in the rejected version of DPFD-1.[31] The terms this article employs are open to broad interpretation, making it easier to refuse a data subject access.

- "Purpose limitation" rules on data exchange are required to prevent data gathered or exchanged for a particular reason from being used for other reasons. This should help create trust and certainty between those authorities exchanging data, imposing safeguards that data exchanged will not be used for other purposes once outside the national jurisdiction. While DPFD-2 enshrines this principle in Article 3, the wording is vague and so it is open to broad interpretation. Similarly, derogation from this set out in Article 12 can be criticised as being too non-specific.[32]

- To ensure consistent protection standards and effective cooperation, robust standards and safeguards must apply to the transfer of EU data to third states. This should help create trust and certainty in data-exchange relations. Recital 12 of DPFD-2 states that data transferred from the EU to an extra-EU body "should, in principle, benefit from an adequate level of protection" outside the EU jurisdiction. Article 14 of DPFD-2 does indeed contain a provision that data may be transferred from competent authorities of member states only if the third state or international body concerned ensures an appropriate level of protection for the intended data processing.[33] However, DPFD-2 does not contain the same specific provisions for assessing adequacy as DPFD-1[34], nor is there any obligation for member states to inform each other in the case of a third party not having adequate data protection standards.[35] There is thus no definition of what shall constitute an adequate level of data protection—this appears to be left to member states' discretion. The grounds for derogating from Article 14 (1d) are also vague and subject to national legislation. Unlike previous drafts, DPFD-2 states that the scope shall extend to future agreements concluded with third parties.[36] This indicates that the provisions of the DPFD will serve as a basis for any agreement the EU concludes with third states on data exchange. Although given the lack of specific provisions on the substance of these rules, the real added value of these new provisions as they stand remains questionable.

- Finally, all these elements must be subject to independent advice and scrutiny provided by a data protection supervisor with wide-ranging powers. This kind of oversight helps to reinforce the benefits for human rights and the effectiveness of cooperation.

29 Article 1 (4).

30 In contrast, the Commission proposal had stipulated that the data subject be provided "on request" with information collected on him with his knowledge, and that in the case of data collected without his knowledge, the information must be provided "as soon as the object of the law enforcement activities is no longer likely to be prejudiced" (Articles 19(1) and (1a), Commission proposal).

31 The language used in the initial draft submitted by the German Presidency—that of March 13—was actually more restrictive. Thus instead of access refusal being allowed to "enable" authorities to perform their duties or "protect" public security, the draft of March 13 had stipulated that access may only be refused if this would "jeopardise" performance of duties, public security, etc. The reason for reverting back to the original formulation was apparently the result of a request from a number of delegations (FR, SE, UK, NL, BU, IT and AT). See DPFD draft proposal of April 24, 2007.

32 See Third Opinion of EDPS on the DPFD, pts. 20–23.

33 Article 14 (1d). The transferring member state must also give its consent and the data must be required for preventing, investigating, detecting or prosecuting criminal offences. This requirement had originally been omitted from the proposal put forward by the German Presidency in March 2007. The decision to insert such a commitment came on the tail of the wish expressed by several delegations (COM, FR, ES, HU, PT, IT, BE, CY). The proposal is based on Article 2 of the Additional Protocol to the Council of Europe's 108 Convention.

34 Article 15 (2) of DPFD-1.

35 As provided for in Article 15 (3) of DPFD-1.

36 Recital 24 and Article 27.

One of the most significant changes proposed in DPFD-2 is the merging of the four existing supervisory bodies in the Third Pillar (the Schengen Information System, Europol, Eurojust and the Customs Information System) into a single joint supervisory authority.[37] This step towards harmonising the monitoring of adherence to data protection in the Third Pillar may in principle have a beneficial effect both on the provision of fundamental rights and on the effectiveness of cooperation, if the joint supervisory authority is accorded true independence as well as strong enforcement powers. Yet, it is detrimental to efforts to provide an adequate data protection framework that an essential element such as supervision has effectively been "postponed" from the draft DPFD to a separate Council Decision, without any indication of when such a decision may be adopted.

Data Protection under the Prüm Convention

Should the DPFD and the Prüm standards for data protection remain distinct, the dual rationale behind the DPFD—namely to regulate the protection of national data exchanged amongst member states under EU rules, and to provide a common framework for data exchange within the Third Pillar—could be undermined. By introducing a new and separate set of standards, the Decision agreed upon in Council, and currently before the European Parliament, integrating relevant Prüm provisions[38] into the EU framework could undo much of the harmonisation effected in the Third Pillar, as well as setting an unhelpful precedent for the development of data protection under the DPFD. The DPFD's scope of application to national data exchange would thus be considerably reduced.

All the same, apart from the apparent advantages in stepping up cooperation between the member states in combating cross-border crime, one of the most important aspects of the Prüm Convention is its claimed "comprehensive range of modern data protection regulations".[39] If it does indeed contain such rules, this might somewhat offset the disadvantages arising from the fragmentation of the emergent Third Pillar data protection regime. It would also mitigate what was said above about national security officials being reluctant to bind themselves to robust and/or common human rights rules.

However, the proposed Prüm Decision fails to establish a framework of clear, common data protection standards by leaving much to the discretion of member states. For example, if data are to be processed for purposes other than those for which they were collected, this may only occur in compliance with the national law of the supplying and the receiving state. Thus two different sets of legislation must be considered before such a decision is made.[40] Article 31 of the proposed Prüm Decision outlines the data subject's right to have inaccurate data corrected and unlawfully processed data deleted. There are also provisions permitting the data subject to seek damages either at an independent court or tribunal, or with the relevant national data protection authority. Again, though, the *member states* are responsible for ensuring this is made possible. Such arrangements can hardly be seen as contributing to more efficiency in data exchange, let alone to the coherent protection of individuals' freedoms.

Data transfer to third countries is not covered under the proposed Prüm Decision and indeed multilateral agreements are excluded from its scope.[41] The data protection rules in the proposed Decision are limited to data collected and processed for the pur-

37 Recital 18 and Article 26.

38 First Pillar issues (such as asylum and immigration, as well as the provisions relating to sky marshals) will not be part of the EU legal framework, but will apparently remain part of Prüm in its capacity as an international treaty. The EP has criticised this for its lack of legal certainty, in that two different sets of legislation will exist parallel to each other. It has also suggested that the fact that these areas are Community competences, meaning that this could actually constitute a violation of the EC Treaty. See European Parliament, Working Document, Committee on Civil Liberties, Justice and Home Affairs, April 10, 2007, p. 3. In addition, one Third Pillar provision (cooperation on request) was not included in the draft Council decision—this was deemed to be Schengen related and is dealt with in the separate Framework Decision on improving cooperation on request, (960/2006/JHA of December 18, 2006). See also: Background note, Justice and Home Affairs Council, Brussels, February 15, 2007. For the text of the proposed Prüm Decision, see Council of the European Union, document no.: 7273/1/07, Brussels, April 17, 2007. This is a slightly amended draft from the one which was submitted by the German Presidency at the end of February 2007.

39 Council of the European Union, press release, "2781st Council Meeting, Justice and Home Affairs."

40 Article 26 (1). There are other examples of two sets of legislation having to be applied for data exchange to take place, as pointed out by the EDPS; see EDPS Opinion on the Prüm Initiative, pt. 68.

41 Article 36 (6).

poses, and within the scope, of this Decision. In other words, these rules will exist parallel to the other Third Pillar instruments and, as discussed above, it does not appear that data collected within the scope of the Prüm Decision will be subject to a DPFD.

In terms of independent supervision, the national data protection authorities are accorded a role in monitoring the admissibility of data processing under the proposed Prüm Decision. This is actually to occur *ex post* in that both automated and non-automated searches are logged or recorded[42] and can be made available to the national data protection authorities upon request. The request must be granted within four weeks. The data protection authorities can make these requests as part of random checks to monitor the lawfulness of data supply, as well as in response to requests by data subjects to monitor the compliance of data processing with national data protection legislation. There is, however, no general review mechanism of compliance with data provisions at the European level.

42 For non-automated searches this information is: the reason for the supply; the data supplied; the date of the supply; the name or reference code of the searching body and of the body administering the file. For automated searches information recorded is: the data supplied; the date and exact time of the supply; the name or reference code of the searching body and of the body administering the file, as well as whether or not a hit exists. In addition, the receiving authority is obliged to record the reason for the supply of data, an identifier for the official who carried out the search and the official who requested the search or supply (Article 30, proposed Prüm Decision).

The Passenger Name Record Agreement: A Case Study of Data Protection Failure

US authorities' access to data held by European airlines—as regulated by the Passenger Name Record (PNR) Agreement of 2004 and its 2006 successor—is perhaps not representative of the mainstream data-exchange activities the EU is involved in: The Agreement concerns the one-way transfer of information held by private actors (airlines) to security agencies in the United States. By contrast, most data exchange is two-way, between security agencies in one state and their counterparts in another. Since it regulates the use of data held by private actors in the EU, the PNR Agreement does not therefore directly affect the autonomy of the EU's authorities nor their monopoly over certain forms of data. The tension between their retention of autonomy and their engagement in effective cooperation is perhaps less pronounced than elsewhere.

All the same, a desire to increase their autonomy would give EU authorities an incentive to introduce lax protection conditions regulating the transfer of this data to the United States: As will be shown below, a future reciprocal agreement for regulating the transfer of data held by *US* transport firms to *EU* authorities or future standards for the transfer of data held by *EU*-transport firms to *EU* authorities, might well be based on the standards set out in the PNR Agreement. In order to ensure that they would receive such data in the future under amenable conditions and without the perceived impediment of human rights constraints restricting their autonomy, the EU authorities had a certain interest in formulating lax data protection provisions for the United States to gain access to data held in the EU.

The United States' threat to fine airlines not granting access to data created an added sense of urgency to negotiations above and beyond that arising from the rather more diffuse terrorist threat. Under such conditions, efforts to introduce human rights concerns into the Agreement could be portrayed by negotiators as a troublesome impediment to efficient negotiation.

US Access to European PNR Data

Passenger name records (PNR) are sets of data elements held on passengers and contained in airlines' automated control systems.[43] Although ostensibly banal, these data allow authorities to create a profile of passengers which might in turn be useful for counterterrorist purposes. In the aftermath of the 2001 terrorist attacks on the United States, for example, information about passengers' dietary requirements has become even more significant, since it gives clues as to the passengers' religious persuasion and practices. Other elements usually found in a passenger name record include passport details, further contact details and age details.[44]

The history of the PNR Agreement between the United States and EU is somewhat convoluted. Following the 2001 attacks, the United States passed a law obliging airlines operating incoming flights to pass certain data held on their passengers to the then Customs Service (now the Bureau of Customs and Border Protection [CBP] under the Department of Homeland Security [DHS]). These US measures, which came into force in March 2003, thus bound private actors to grant access to data collected and stored outside the jurisdiction of the United States. Should they have failed to release PNR data, airline companies were liable for a withdrawal of landing rights or a fine of $5000 per passenger whose data were not released.

Given that the PNR data were collected under the conditions laid down by the Data Protection Directive regulating data protection in the First Pillar of the EU,

43 According to the Undertakings of the Department of Homeland Security, PNR encompasses 34 fields of data, including name, date of birth, telephone numbers, email address, credit card numbers and travel insurance details. Data are kept on file for at least three and a half years and can be held for eight and a half years if it is of particular interest to the investigators. Europol is to monitor the recording and deletion of data. See Wolfgang S. Heinz and Jan-Michael Arend, *The International Fight against Terrorism and the Protection of Human Rights. With Recommendations to the German Government and Parliament* (Berlin: German Institute for Human Rights, 2005), p. 17.

44 A full list of the 34 data elements to be passed on is given in the CBP Undertakings of May 11, 2004, Attachment A.

European airlines were thus placed between a rock and a hard place, risking a breach of the EU's Data Protection Directive if they granted access to data, and a fine in the United States if they failed to. In order to facilitate the transfer of data, and remove airlines from their quandary, the EU took steps towards a PNR agreement with the United States.[45]

On the basis of the 1995 Data Protection Directive, negotiations between the United States and the Commission's Directorate General for the Internal Market[46] were held throughout 2003, with a consensus between both negotiating parties apparently being reached in December of that year.[47] The Council then adopted an agreement on the transfer of PNR data by air carriers in the EU to the US Department of Homeland Security on May 17, 2004.[48]

The negotiations were not without controversy. While the Commission had initially expressed concern regarding both the amount (34 fields) of PNR data to be collected, as well as its use for purposes other than fighting terrorism, it modified its position within the space of two weeks, deeming the United States' provisions sufficiently adequate to justify transferring the data.[49] The reasoning was that such reservations—and the resulting restrictions on the transfer of data—could hamper the EU in developing a similar policy of its own. In its Communication of December 2003 on the transfer of PNR data, the Commission regarded "the 'purpose limitation' language" agreed with the United States as a "sound" basis for developing an EU policy along these lines, covering both the fight against terrorism and international organised crime. Furthermore, it considered that "the list of data elements also seems broad enough to accommodate law enforcement needs in the EU."[50] The Commission subsequently passed a positive decision concerning the adequacy of the protection of personal data offered by the United States—a precondition for data transfer under the 1995 Data Protection Directive.[51]

All this occurred despite the fact that the United States fell short on a number of counts concerning the recommendations of the Article 29 Working Party (the First Pillar's independent data protection advisory body) for adequate data protection standards.[52] Indeed, data protection remains patchy in the United States: A sectoral approach is taken, and there is a lack of a general regulatory framework. In any event, federal privacy laws do not apply to foreign nationals. Other concerns included the long data-retention periods (the United States originally pushed for a duration of 50 years), the lack of safeguards for the data subject as well as lacunae in the proportionality and purpose limitation of data collection. Originally aimed at preventing terrorist attacks, the Undertakings of the DHS (which form part of the Agreement) extend the purpose of data collection to preventing and combating "other serious crimes ... which are transnational in nature".

The EP had, meanwhile, felt marginalised in the decision-making process.[53] While the EP in principle supported an agreement between the EU and the United States, it repeatedly stated the importance of ensuring data protection safeguards, as well as its concern for the direction negotiations were taking.[54] However, it appears that there were delays in the Com-

45 Council Decision of May 17, 2004, on the conclusion of an Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 2004/496/EC.

46 The DG Internal Market was at this time responsible for data protection. In view of subsequent events, in particular the ECJ judgement (see below), negotiations which came after the ECJ judgement were conducted between the United States and jointly the Council Presidency and the Commission DG Justice, Freedom and Security.

47 As documented by Privacy International, *Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection,* first report on "Towards an International Infrastructure for Surveillance of Movement," February 2004, in particular p. 7.

48 Council Decision [see n. 45].

49 See Privacy International report [see n. 47].

50 Communication from the Commission to the Council and the Parliament: *Transfer of Air Passenger Name Record (PNR) Data: A Global/EU Approach,* Brussels, European Union, 2003, COM (2003) 826 final, p. 8.

51 Commission Decision of May 14, 2004, on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States' Bureau of Customs and Border Protection C (2004) 1914.

52 Article 29 Working Party, First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy. Brussels, European Commission, XV D/5020/96-EN final WP4, June 26, 1997, in particular pp. 6–7.

53 The EP had questioned the legality of the PNR Agreement in its resolution of March 2004 and on April 21, 2004, voted to ask the ECJ for an opinion on the compatibility of the PNR Agreement with the Treaties. See European Parliament Resolution of March 31, 2004, and "European Parliament votes to go to court on EU-US PNR deal," *Statewatch News Online*, April 21, 2004.

54 European Parliament, Resolution on the Transmission of Personal Data by Airlines in Case of Transatlantic Flights: State of Negotiations with USA. P5_TA-PROV (2003) 0429.

mission submitting proposals both to the EP and Council.[55] The EP's concerns and recommendations were along the lines of those put forward by the Article 29 Working Party.[56] The long data-retention period was seen as disproportionate to the aim of combating terrorism, as were the kinds of data transmitted. As mentioned above, the United States was keen to retain data for up to 50 years. During negotiations, the Commission brought the period of retention down to 3.5 years (for no other reason than because this was to be the lifetime of the initial Agreement). The Article 29 Working Party deemed this disproportionate. It recommended a period not longer than "some weeks or even months"[57] in view of the fact that the stated purpose of data collection is to control entry to US territory in order to prevent terrorist attacks.

In addition, there was concern that the rules on the further transfer of PNR data to other authorities, including foreign authorities, remained vague. This deficiency was aggravated by institutional rearrangements in the United States which saw agencies that were previously privy to or excluded from the Agreement restructured, and thus subject to new relations with one another. The Department of Homeland Security committed itself not to engage in bulk sharing of data with other agencies. However, the DHS is made up of a multitude of departments which had—until shortly before these negotiations—been separate agencies, making the further processing of data extremely opaque.[58] The EP raised its concern that its reservations regarding the Agreement were not being given due consideration by the Commission and expressed its intention to take the matter before the ECJ if the Commission did not withdraw its decision on adequacy. It also stressed that the outcome of the negotiations with the United States should not serve as a model for EU policy in this area.[59]

Some of the EP's concerns appear to have been borne out in practice: The United States' wished to use European passenger data to test and implement its then Computer Assisted Passenger Pre-Screening System (CAPPS II), which was considered so controversial that US airlines refused to participate. Due to the number of open questions on the System, including data-retention periods, further processing of data and even the accuracy of the system itself, an agreement was reached that European passenger data would not be included in computer assisted screening until further negotiations had taken place.[60] However, there are indications that the DHS did in fact use PNR data from EU passengers to test CAPPS II.[61]

Similarly, at the end of 2006, there were reports that PNR data were among those included in the United States' Automated Targeting System (ATS).[62] This system is the object of no little criticism in the United States, and American civil-liberties organisations have warned that it stands in violation of US privacy legislation, in particular the Privacy Act of 1974.[63] Originally designed to collect data relating to cargo, ATS has in the last years been used to profile

55 European Parliament, Resolution on Transfer of Personal Data by Airlines in the Case of Transatlantic Flights, P5_TA(2003)0097, p. 2.

56 Article 29 Working Party Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, adopted June 13, 2003, as well as Article 29 Working Party Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), adopted January 29, 2004.

57 Article 29 Working Party Opinion 4/2003, p. 8.

58 Privacy International report [see n. 47], p. 5.

59 European Parliament, Motion for a Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection (C5-0124/2004), March 19, 2004.

60 According to the Commission Communication [see n. 50], p. 7.

61 Privacy International report [see n. 47], p. 10. Due to the controversy of the CAPPS II project, it was eventually dropped by the government and replaced by a more simplified watch list system. However, the accuracy and hence the value of these lists is also highly questionable given the exponential rise in persons included on the watch lists (as many as 435,000 in March 2007), and the number of cases of innocent people being included on the watch lists. One of the main concerns is that once a person has been included on the watch list, it is virtually impossible to have their name removed and it is not possible to find out for what reasons their name was included in the first place. See "Terror Database Has Quadrupled in Four Years. U.S. Watch Lists Are Drawn from Massive Clearinghouse," *Washington Post*, March 25, 2007.

62 See "Address to the European Parliament by Minister for European Affairs Paula Lehtomäki," *Statewatch News Online*, December 13, 2006. Retrieved at: http://www.statewatch.org/news/2006/dec/ats-eu-coun-statement-12-dec-06.pdf.

63 "Comments of 30 Organizations and 16 experts in Privacy and Technology urging the Department of Homeland Security to a) suspend the 'Automated Targeting System' as applied to individuals, or in the alternative, b) fully apply all privacy act safeguards to any person subject to the automatic targeting system," docket no.: DH6-2006-0060 Notice of Privacy Act System of Records. Source: http://www.statewatch.org/news/2006/dec/ats-ngo-comments.pdf.

data relating to persons "seeking to enter or exit the United States" (this includes US citizens). Such profiles provide the DHS with a "risk assessment" of the individual's potential to pose a terrorist threat, which in turn determines whether persons concerned will be subjected to invasive searches or indeed be allowed to enter or exit the country. ATS can be criticised for its lack of transparency: Redress procedures for individuals are extremely complicated and can also be costly.

On the basis of its concerns, the EP resolved to take the matter before the ECJ in order to ask for the annulment of the PNR Agreement and to appeal against the Commission's decision on adequacy.[64] The ECJ eventually reached a ruling on 30 May 2006[65] in which it held that the Agreement was illegal, and overturned the Commission's decision on the adequacy of data protection provisions in the United States.[66] In order to avoid legal uncertainty, the ECJ ruled that the then valid PNR Agreement should remain in place until September 30, 2006, to give the Council time to renegotiate a substitute agreement.

The Court ruled that both the PNR Agreement and the Commission's adequacy decision had actually been carried out under the wrong legal basis: The stated purpose of the Agreement was to enhance security, prevent and fight terrorism and other serious crime. These aims placed it outside the scope of the legal basis that the Commission had used (transport policy—a First Pillar issue) and thus beyond the scope of the Data Protection Directive in Article 3 (2). These aims belong instead to the realm of Third Pillar activities, meaning the Commission did not have a competence to negotiate such an agreement.[67] This in turn meant that the ECJ felt unable to examine the actual content of the PNR Agreement and the Commission's adequacy decision—which was the EP's principal reason for disputing the Agreement and Decision.

64 "European Parliament to Go to Court over Council and Commission Decisions on PNR Data Agreement with USA," *Statewatch News Online*, June 25, 2004.

65 The ECJ had rejected a request by the EP in 2004 for the accelerated procedure. See Court Judgement Case on the accelerated procedure in C-317/04 *European Parliament v Council of the European Union* of September 21, 2004.

66 Judgement of the Court of Justice in Joined Cases C-317/04 and C-318/04 *European Parliament v Council of the European Union* and *European Parliament v Commission of the European Communities*, press release no. 46/06.

67 Elspeth Guild and Evelien Brouwer, *The Political Life of Data. The ECJ Decision on the PNR Agreement between the EU and the US* (Brussels: Centre for European Policy Studies [CEPS], August 2006), policy brief no. 109, p. 3.

On June 27, 2006, the Council authorised the EU Presidency—assisted by the Commission—to open negotiations with the DHS on a new agreement on the transfer and processing of PNR data. By the ECJ deadline of September 30, 2006, an agreement had not been reached, indicating that it was not simply a case of changing the legal basis, but that the negotiations had led to arguments about the substantive content of the new Agreement which were stalling progress. The problem appeared to revolve around the United States' demands for the transfer of kinds of information not foreseen in the original agreement.[68]

Nevertheless, an agreement was announced a week after the deadline and the Council adopted a decision on the signing of this on October 16, 2006.[69] This Interim Agreement is due to run until July 31, 2007, as the previous Agreement was, unless extended by mutual written agreement, by which time a more permanent agreement is to be reached.

The Interim PNR Agreement and its Implications for Data Protection

The October 2006 Agreement is a temporary one and is regarded as unsatisfactory by many actors in the contracting parties, albeit for different reasons:

- The United States appears to view the data protection standards it contains as a hindrance to counterterrorism efforts. Given that data collection is seen as imperative for the prevention of further terrorist attacks, the United States negotiated to retain data for a longer period than that foreseen in the 2006 Interim Agreement. The United States has subsequently expressed the intention of extending the purpose of data collection to serious crime in general and even to include sensitive data, such as that pertaining to health.
- The 2006 Agreement has raised serious concerns on the part of the EU's oversight structures (EP, EDPS, Article 29 Working Party) which, even if only indirectly involved in Third Pillar issues, consistently called for a different, more rights-based approach to the negotiations.

Many of the European Parliament's, EDPS' and Article 29 Working Party's concerns appear well-

68 Stephen Mulvey, "What the US Knows about Visitors," *BBC News Online*, October 1, 2006. Source: http://news.bbc.co.uk/1/hi/world/europe/5390074.stm.

69 Council decision 2006/729/CFSP/JHA of October 16, 2006 [hereafter referred to as the "Interim Agreement"].

founded: Both the 2004 and 2006 PNR Agreements state that data shall be processed and the data subject treated in accordance with "applicable US law". This means that any changes in US legislation impose unforeseen changes *de facto* in the way that data are processed and held. Despite the fact that US privacy laws offer a considerably lower standard of data protection than Europe[70], the EU agreed to continue to offer access to passenger data on this basis. In fact, the original CBP Undertakings of 2004 continue to form part of the Agreement.[71] In a letter to the DHS following the conclusion of the Interim Agreement, the Council Presidency and the Commission stated: "The commitments of DHS to continue to implement the Undertakings allow the EU to deem that, for purposes of the implementation of the Agreement, it ensures an adequate level of data protection."[72] This statement is preceded by a reaffirmation of the EU's commitment to the respect of fundamental rights and in particular the protection of personal data. A similar affirmation can be found in the Preamble of the Interim Agreement, however there is no indication of how the parties intend to realise these standards.

The DHS intends to extend the purpose of data transfer and processing beyond the scope of counter-terrorism to include information on data subjects who "may carry or have been exposed to a dangerous communicable disease" so that they "can be readily identified, located and informed without delay".[73] This is an issue for concern with regard to data protection, as it goes against the principle of purpose limitation. Concern was voiced on this issue by the Dutch Liberal MEP, Sophie in 't Veld, during the plenary session in the EP on October 11, 2006.

70 For a comparative study of US and European data protection legislation, see Francesca Bignami, "European versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data Mining," forthcoming, *Boston College Law Review*, May 2007.

71 Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) of May 11, 2004. On the interpretation of these and their application under the new agreement see Letter from Assistant Secretary for Policy, DHS, to the European Commission of October 6, 2006.

72 Council of the European Union, Reply by the Council Presidency and the Commission to the Letter from the USA's Department of Homeland Security, document no.: 13835/06, Brussels, October 13, 2006.

73 Letter from the DHS to the European Commission [see n. 71].

In a letter to the Commission, the DHS also expressed the wish to extend the data-retention period (3.5 years under the Interim Agreement) in order to identify potential terrorists. No definite period of retention is put forward at this point and this is likely to be an issue for the negotiations for a future agreement. Although the DHS letter to the European Commission is not part of the formal Agreement and therefore not legally binding, it does reflect the intentions and interests of the United States, and indicates the line most likely to be taken in any future negotiations on the PNR Agreement.

The October 2006 Agreement has been presented as the result of difficult negotiations, which were held under conditions of urgency. To avoid carriers being subjected to fines or loss of landing rights, the only alternative for the member states would have been bilateral agreements between themselves and the United States, something which was seen as a last resort by all parties and would have made consistent data protection standards even more difficult. At the same time, one of the main criticisms levelled at internal security measures and legislation is the fact that they are often decided on within a very short period of time, without sufficient participation of civil society and particularly of parliament, and by reference to a sense of emergency which is often spurious. While it is necessary to act quickly and adapt laws to changing circumstances and threats, bypassing the usual checks and balances of the democratic system can have serious implications for fundamental rights, in particular when it comes to providing safeguards for innocent individuals when the system fails.

The PNR Agreement as a Case Study of Data Protection Failure

The PNR Agreement may be understood as a case study of data protection failure, highlighting many of the dangers identified in the above section (p. 12):

Firstly, the standards of data protection in the European states where the data are stored have been called into question: although the passenger data in the EU are collected under a First Pillar transport policy measure, and are thus subject to the relatively high standards afforded by the 1995 Data Protection Directive, in its judgement on the initial Agreement the ECJ deemed the transfer of the data to occur on the basis of Third Pillar security aims. The Interim Agreement thus falls outside the scope of the First

Pillar data protection standards. Given that private actors and Executives are capable of error and abuse when it comes to the processing and transmission of data, the lack of clarity in the EU's data protection standards presents dangers to the data subject.

Secondly, the standards of data protection in the receiving state are highly questionable, with limited safeguards on the use and circulation of the data beyond the jurisdiction of the EU. The potential for Executive abuse beyond the EU's jurisdiction is high: Although the data could be useful to the United States' counterterrorist efforts, they might for example also be misused for broader efforts to control immigration from the EU. Meanwhile, recent institutional changes made to the Department of Homeland Security make the question of how broadly the data can and will be circulated, even within the United States, difficult to answer. Under considerable pressure from the United States, the EU is generally agreed to have failed to make the transfer of data conditional on the United States upgrading the standards of protection afforded them.

Thirdly, the European Executive branch which dominated the negotiations had an incentive *not* to push for high data protection standards: The "exchange" of data in this case was one-way, from the EU to the United States; subsequent agreements would regulate data transfers from the United States to the EU. If the EU set high protection levels for the United States, it would itself in all likelihood be reciprocally bound by similar standards in future. These might restrict their autonomy.

Recommendations

It is in line with citizens' interests to establish a clear legal framework which provides consistent data protection standards within which data exchange can take place. Firstly, this hinders the abuse of their privacy by the authorities; secondly, this facilitates more effective cooperation in data exchange for counterterrorist purposes. Whilst it may not appear to be in the narrow institutional interests of the participating authorities to give up a degree of autonomy and submit to such rules, such a move provides a degree of legal certainty—fostering conditions for effective cooperation.

As the PNR case clearly illustrates, the risks that transnational data transferrals pose for the individual are significant, since the manner in which their data will be further processed and the rules establishing which authorities will have access to it are often lacking in transparency. Under current circumstances, there is no way to ascertain the proportionality of the measures. At present, the DHS is granted access to data on all passengers travelling to or transiting through the United States. In other words, the data transfer is not based on a specific threat but amounts to a general surveillance of all passengers, which would seem to be disproportionate. Specific rules are therefore required on what kind of data is transferred.

Against this background, the DPFD should be seen as a prerequisite and not as an obstacle to developing further ways of deepening cross-border cooperation. The original sticking point in negotiations—namely the scope of application to national data collection—must be overcome: Considering the increasing importance of data exchange in international counterterrorism efforts, any data which are processed for law enforcement purposes within a member state could potentially be requested as part of an EU or an international investigation. It is therefore virtually impossible to speak of data processed "purely" in a domestic context. In order to be effective—in terms of protecting the individual and improving counterterrorism efforts—such a DPFD needs to be applicable to three kinds of data exchange: within the EU itself, within individual member states and between EU member states and third countries. Further, the Prüm Convention must be brought into line with the DPFD on data protection. It is also vital that any legal framework for data protection standards in the EU covers data which leaves the Community's jurisdiction.

Such a framework should not only establish consistent data protection rules for these areas of activity, but specifically contain the following as elements essential for the twin aims of safeguarding privacy and internal security:

- *Purpose Limitation:* Currently, much of the data processed for security reasons was originally collected for other purposes. Such a state of affairs lacks certainty and requires clarification. Relevant purpose limitation rules restricting the use of data for reasons other than those for which they were collected are urgently needed.
- *Further Processing of Data:* For legal certainty, transparent conditions need to be set out under which further processing is permitted, for example by compiling a list of the specific authorities and agencies which are allowed access to the data, rather than descriptions such as "counterterrorism authorities", which are open to interpretation. On no occasion should this decision be left to the discretion of the authority holding the data.
- *Period of Data Retention:* Similarly, the period for which data can be retained must be bound by specific rules and should be reviewed on a regular basis. In the case of the PNR Agreement, it should be borne in mind that the purpose of data collection is to prevent terrorists entering the country and carrying out attacks. Therefore, extensive periods of data retention are difficult to justify.
- *Rights of the Individual:* An individual must be granted the right to know if data are being held, to have false data corrected or deleted, as well as the right of redress in cases of data being abused. The circumstances under which exceptions to this rule apply within the context of combating and preventing terrorism must be clearly specified and applied restrictively, on a case by case basis.
- *Oversight:* To increase legitimacy and ensure that the resulting legislation is not one-sided, data protection experts should be included in the decision-making process. Here, the EU can draw on existing structures in the member states (data protection

authorities), as well as within the European institutions themselves (EDPS, Article 29 Working Party). To increase democratic legitimacy, the EP must also be included in the decision-making process. Implementation reports on data-exchange agreements should also focus on data protection compliance, as well as review changes in the state of play, in terms of technological advances and their implications for data protection. Again, parliament and the other mentioned oversight mechanisms should be included in this process.

In order to ensure the security of its citizens in the long term, the EU must recognise that effective internal security cooperation and the respect of fundamental rights are inextricably linked.

Abbreviations

ATS	Automated Targeting System
CAPPS	Computer Assisted Passenger Pre-Screening System
CBP	Customs and Border Protection
DHS	Department of Homeland Security (U.S.)
DPA	Data Protection Authority
DPFD	Data Protection Framework Decision (Framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters)
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EP	European Parliament
JHA	Justice and Home Affairs
NGO	Non Governmental Organisation
PNR	Passenger Name Records
SIS	Schengen Information System
TEU	Treaty on European Union
VIS	Visa Information System