Privacy and Law Enforcement in the European Union: The Data Retention Directive

Francesca Bignami*

This Article examines a recent twist in European Union ("EU") data protection law. In the 1990s, the European Union was a market-creating organization and the law of data protection was designed to prevent rights abuses by market actors. Since the terrorist attacks in New York, Madrid, and London, however, cooperation in law enforcement has accelerated. Now the challenge for the European Union is to protect privacy in its emerging system of criminal justice. This Article analyzes the first EU law to address data privacy in law enforcement—the Data Retention Directive (or "Directive"). Based on a detailed examination of the Directive's legislative history, this Article finds that privacy—as guaranteed under Article 8 of the European Convention on Human Rights and the Council of Europe's Convention on Data Protection—is adequately protected in the Directive. This positive experience can serve as guidance for guaranteeing other fundamental rights in the rapidly expanding area of EU cooperation on criminal matters.

I. INTRODUCTION

Data privacy is one of the oldest human rights policies in the European Union. The European Union was born as an international organization dedicated to the creation of a common market. Rights emerged only gradually, as it became apparent that market liberalization could come into conflict with rights and that the safeguards available under national constitutional law were inadequate. At first, the European Court of Justice took the lead in establishing rights. By the mid-1990s, however, the European legislature had also become active. One of its first forays into the human rights realm was the Data Protection Directive.

---

* Professor, Duke University School of Law. Many thanks to Xavier Lewis and Joan Magat for their valuable comments.

The Data Protection Directive, proposed in 1990 and passed in 1995, set up a complex regulatory scheme at the national level to protect individual rights.[1] At that time, as was to be expected in a European Union still focused on the common market, data protection was aimed at preventing rights abuses by market actors and by government agencies operating as service providers. Recently, however, EU data protection has taken a new turn. Now, the challenge is to safeguard privacy when governments exercise their core sovereign powers of national security and law enforcement.

This Article examines the European Union's new turn toward protecting privacy in law enforcement activities. The first part explores the developments that have given rise to these policies, namely the growing importance of digital technologies in police investigations and the intensification of police cooperation in the European Union following the terrorist attacks in New York, Madrid, and London. The second part analyzes the Data Retention Directive, the legislation with the most significant data protection ramifications to be enacted at the time of this writing.[2] The Article concludes with some thoughts on how the largely positive experience of the Data Retention Directive can inform the protection of other classic liberal rights in the rapidly growing domain of European cooperation on fighting crime.

II. LAW ENFORCEMENT IN THE DIGITAL EUROPEAN AGE

To understand the challenges of data protection today, a bit of history is necessary. The first European data protection laws date to the early 1970s.[3] Their focus was large-scale data collection by the government and by the few private actors with the resources and technology to engage in such data processing—mostly banks and telecommunications providers. On the public side, these early laws largely affected those parts of government administration that routinely collected large amounts of information from citizens for purposes of providing services such as health care, education, and welfare.

For the most part, intelligence and law enforcement officials were untouched by these early data protection regulations. Under their respective

---

1 European Parliament and Council Directive 1995/46/EC, 1995 OJ (L 281) 31 (hereinafter "Data Protection Directive"). See generally Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 Mich J Intl L 807, 813–19, 837–45 (2005).

2 Council Directive 2006/24/EC, 2006 OJ (L 105) 54. At the time of this writing, two other initiatives with far-reaching consequences for data protection were being negotiated in the 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*, COM(05) 475 final (hereinafter "Proposal for Protection of Personal Data in Criminal Matters"); and *Proposal for a Council Framework Decision on the Exchange of Information under the Principle of Availability*, COM(05) 490 final.

3 Colin J. Bennett and Charles D. Raab, *The Governance of Privacy* 102–03 (Ashgate 2003).

national laws, intelligence and law enforcement officers were generally prohibited from accessing without cause the records of other government agencies. These officers had to answer petitions from individuals seeking to verify that their personal data in police and security files was accurate. Otherwise, their information-gathering activities—eavesdropping on phone calls, bugging of homes, and other forms of surveillance—were covered by a more specific set of laws. The police had to apply for warrants from judicial authorities before they could undertake surveillance. In contrast, intelligence officers, responsible for security-related surveillance, were subject to less rigorous standards enforced not by courts but by independent government officials or parliamentary committees.[4]

Since the 1970s, one development has radically altered the nature of law enforcement and the relationship between law enforcement and data protection laws—technology. Increasingly, we live our lives in digital space. We run errands, conduct business, and socialize with friends in the virtual world of the Internet. When not connected to the Web, we are on our cell phones. And, unbeknownst to us, our images and personal details are constantly recorded by surveillance cameras, security systems, and a great number of other devices. With this new, technology-rich lifestyle, we routinely generate millions of pieces of data. This data can be stored and searched with great ease. It is a treasure trove of information for many different types of actors: direct marketers, credit agencies, and especially law enforcement officers. By monitoring our Internet traffic, the police can easily learn where we shop, what we do in our spare time, and how we make a living. This is but a sampling of what can now be done with our electronic data, and a suggestion of what might be done in the future with that data.

In this information-rich environment, the danger of government fishing expeditions is extreme. On a fishing expedition, investigators review correspondence, bills, and other personal records without any clear expectation of what type of evidence or what type of crime might be found. This is one of the most obnoxious, oppressive forms of intrusion by a government into the lives of its citizens. The vast quantity of data generated in today's electronic world—combined with the technology available to process that data—increases exponentially the risk of legitimate police searches degenerating into the aimless perusal of our private lives.

Old-fashioned criminal procedure cannot address the privacy challenges of new technologies. Under the rules of criminal procedure, before an individual's

---

4 For a description of the German and US systems, see Paul M. Schwartz, *German and US Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 Hastings L J 751 (2003).

records may be reviewed, government investigators must demonstrate to an independent judicial officer that they have good reason to believe that a crime has been committed and that a search of the individual's records will produce evidence of the crime. But when the records are electronic, many believe that the police should not always be required to make such a showing. Even in Europe, where personal information such as traffic data—information on when and to whom emails and phone calls are sent or made—is protected under the fundamental right to privacy, the privacy interest in such data is perceived as less substantial than the privacy interest in the *content* of that data—an email or a phone conversation. What is revealed by the first type of data is thought to be far less significant than what is revealed by the second type. This set of beliefs is reflected in Europe's legal framework. The law of data protection, not the more rigorous law of criminal procedure, governs police access to personal information such as traffic data.

Much like criminal procedure, the law of data protection seeks to limit the amount of personal information available to the police in the interest of stopping oppressive government surveillance. But compared to criminal procedure the legal standards and enforcement mechanisms of European data protection law are more flexible. As will be explained in detail in the next section, under the basic principles of data protection law, personal information may be obtained by the police only if a number of conditions are satisfied. These conditions include the requirement that such information be relevant to an investigation, that it not be used for purposes unrelated to the investigation, and that it be erased or made anonymous once it no longer serves the purposes of the investigation. In the interests of compliance, oversight powers are vested in an independent privacy authority and individuals have a right to apply to government agencies to check on their personal information. These features of data protection law are geared towards many of the same liberal purposes of criminal procedure but without rigid legal standards such as probable cause—as is required for a search of a home under American criminal procedure—and without the courts as the principal enforcers of such standards. Of course, under European law, special categories of personal data are afforded additional protection from the police. These more demanding standards, however, do not apply across-the-board to all information of interest to the police.

Before the terrorist attacks in New York, Madrid, and London, data protection would have been the responsibility of national legislators and the Council of Europe (or "Council"). Jurisdiction over police matters was still primarily national, with a limited oversight role for the Council of Europe.[5] The

---

5 The Council of Europe's oversight comes in two varieties. The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), 20

EU's data protection rules were designed to regulate market actors, not the police. As was observed by Advocate General Léger in a recent opinion, the Data Protection Directive expressly does *not* apply to data processing for purposes of public security and law enforcement.[6]

In the past few years, however, cooperation on criminal matters under the legal umbrella of the European Union has intensified. In theory, the terrorist attacks might have provoked no more than closer pan-European cooperation on fighting terrorism. Instead, these attacks have triggered cooperation on a wide range of law enforcement matters.[7] The exchange of personal data to prevent and prosecute criminal acts is a critical form of such collaboration.[8]

The corollary to cross-border data-sharing in the interests of EU law enforcement is the EU right to privacy, specifically the right to be free of unwarranted police surveillance. Before handing over data, evidence, or suspects, the police and judiciary of one state must be convinced that the police and judiciary of the requesting state will respect the rights of its nationals. By transferring such information, the police and judiciary of one state put their citizens at risk of being investigated, tried, and imprisoned in another state. This requires a great deal of confidence in the fairness of the requesting state's criminal justice system. In recent years, therefore, a number of attempts have

---

ILM 317, contains rules applicable to private and public actors, including the police. The Convention establishes a committee of representatives of the signatory parties, whose mission is to oversee implementation. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms has been interpreted to include the right to protection of personal data; individuals can seek a remedy before the European Court of Human Rights if they believe that their data protection rights have been breached. See *Rotaru v Romania*, App No 28341/95, 8 BHRC 449 (May 4, 2000) (holding that storage and use of personal information in police files, together with refusal of right of correction, amounts to interference with private life under Article 8); *Leander v Sweden*, App No 9248/81, 9 Eur HR Rep 433, 450 ¶ 48 (Mar 26, 1987) (holding that recording of personal details in police files constitutes interference with private life under Article 8); *Malone v The United Kingdom*, App No 8691/79, 7 Eur HR Rep 14, 49 ¶ 84 (Aug 2, 1984) (holding that pen registers constitute an interference with private life under Article 8); European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), art 8, 213 UN Treaty Ser 221 (1955) ("ECHR").

6 Opinion of Advocate General Léger, *European Parliament v Council and v Commission*, Cases 317/04 and 318/04, ¶ 96 (2006), available online at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004C0317:EN:HTML> (visited Apr 21, 2007).

7 See Jörg Monar, *The Problems of Balance in EU Justice and Home Affairs and the Impact of 11 September*, in Malcolm Anderson and Joanna Apap, eds, *Police and Justice Co-operation and the New European Borders* 165, 177–80 (Kluwer 2002).

8 See *Communication from the Commission to the Council and the European Parliament: Towards Enhancing Access to Information by Law Enforcement Agencies*, COM(04) 429 final.

been made to set down a common rights framework for the European Union's criminal justice system.[9] Data protection is one piece of that rights package.

III. THE DATA RETENTION DIRECTIVE

On March 15, 2006, the European Parliament (or "Parliament") and the Council of the European Union passed the Data Retention Directive.[10] Its aim was to facilitate European cooperation in criminal investigations. Under the Directive, providers of electronic communications services and networks are required to keep traffic data related to phone calls and emails for a period of six months to two years, depending on the Member State.[11] This traffic data includes the information necessary to identify the originator and the recipient of phone calls (including Internet telephony) and emails, together with information on the time, date, and duration of these phone calls and emails.[12] Such data must be made available to the national police and through the national police, as well as to police officers in other Member States in accordance with the requirements of their respective national laws.[13]

Such a directive was necessary because unlike the United States, where communications providers routinely store such information for marketing purposes,[14] communications providers in many European countries have been legally required for decades to erase such information as soon as it is no longer useful for billing purposes.[15] In the wake of the terrorist attacks, police authorities became convinced that such information was indispensable to fighting crime. A law, therefore, was needed to reverse the presumption in favor of information destruction.

A. THE LAW-MAKING PROCESS

The Data Retention Directive's procedural history was rocky. The first complication stemmed from confusion over whether the law should be passed pursuant to the European Union's single-market powers, known as the First Pillar, or pursuant to its crime-fighting powers, known as the Third Pillar. As

---

9 See, for example, *Proposal for a Council Framework Decision on Certain Procedural Rights in Criminal Proceedings throughout the European Union*, COM (04) 328 final.

10 Council Directive at 54 (cited in note 2).

11 Id, arts 3, 6.

12 Id, art 5.

13 Id, arts 1, 4, 8.

14 Mark Hosenball and Evan Thomas, *Hold the Phone; Big Brother Knows Whom You Call. Is that Legal, and Will it Help Catch the Bad Guys?*, Newsweek 22 (May 22, 2006).

15 See, for example, Council Directive 2002/58/EC, art 6, 2002 OJ (L 201) 37.

mentioned earlier, the European Union was originally conceived as a market-creating organization. Only in 1992 did it obtain the power to pursue a common foreign and security policy and to act on matters of criminal law. At that time, the powers relating to the single market became known as the First Pillar, those relating to common foreign and security policy as the Second Pillar, and those relating to criminal law as the Third Pillar. Defense policy and criminal law, however, go to the core of national sovereignty and therefore the powers conferred by the Second and Third Pillars were far more limited than those of the First Pillar.

The Directive could have plausibly been passed under either the First or the Third Pillar. Its principal aim was to promote cooperation among law enforcement communities by improving the information available to the police. Yet the initiative also had a single-market effect. By standardizing the data retention requirements imposed by police authorities on electronic communications providers, it would be easier for providers to do business in multiple jurisdictions. Rather than having to comply with the laws of twenty-seven different EU Member States ("Member States"), communications providers would be able to rely on a single data retention standard for all of their European operations.

The choice of the Directive's legal basis mattered because of the less supranational character of the Third Pillar as compared to the First Pillar. A Third Pillar measure could be proposed by single Member States, whereas a First Pillar measure could only be proposed by the European Commission (or "Commission"). To pass a Third Pillar measure, unanimity in the Council would be necessary, whereas to pass a First Pillar measure, only a qualified majority would be required. For a Third Pillar measure, the European Parliament would only be consulted, but under the First Pillar, the European Parliament would enjoy full legislative prerogatives in accordance with the co-decision procedure. Moreover, the European Court of Justice's jurisdiction over a Third Pillar measure is narrower than over a First Pillar measure.[16]

Initially, the measure was proposed by France, Ireland, Sweden, and the United Kingdom as a framework decision under the Third Pillar.[17] A year later,

---

16 See Treaty on European Union, art 35, 2002 OJ (C 325) 5 (Feb 7, 1992) (hereinafter "Treaty on European Union"). For the Court of Justice to have jurisdiction over preliminary rulings from national courts concerning Third Pillar measures, the Member State must enter a declaration. By 2005, fourteen out of twenty-five Member States had acceded to the Court of Justice's jurisdiction. See *Information Concerning the Declarations by the French Republic and the Republic of Hungary on their Acceptance of the Jurisdiction of the Court of Justice to Give Preliminary Rulings on the Acts Referred to in Article 35 of the Treaty on European Union*, 2005 OJ (L 327) 19.

17 *Draft Framework Decision on the Retention of Data Processed and Stored in Connection with the Provision of Publicly Available Electronic Communications Services or Data on Public Communications Networks for the*

however, the Council and the Commission reversed course, and the measure was proposed by the Commission as a First Pillar directive.[18] The Directive was finally passed in March 2006 on that same legal basis.[19] Ultimately, the more democratic co-decision procedure under the First Pillar appeared better suited to deal with an issue with implications for a fundamental right—the right to personal data protection.

A second complication was the variety of data protection institutions with a right of consultation. Two separate data protection authorities gave opinions on the proposed directive. While the opinion of the first was expected,[20] the other came as somewhat of a surprise.[21] The first authority, the Data Protection Working Party ("Working Party"), is composed of national data protection officials. It was established in 1995 to advise on implementation of the Data Protection Directive and on new data protection initiatives proposed for the European Community.[22] Since then it has routinely issued opinions, sometimes at the request of the Commission, on legislative initiatives with data protection ramifications.

Purpose of Prevention, Investigation, Detection and Prosecution of Crime and Criminal Offences Including Terrorism, Council Doc 8958/04 (Apr 28, 2004) ("Draft Framework Decision"), available online at <http://www.statewatch.org/news/2004/apr/8958-04-dataret.pdf> (visited Apr 21, 2007).

18 *Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*, COM(05) 438 final ("Commission Proposal"). The legal basis for the proposed and the final versions of the directive was the Treaty Establishing the European Community, art 95, 1997 OJ (C340) 3 (Nov 10, 1997).

19 On July 6, 2006, Ireland brought a legal challenge to the Data Retention Directive on the grounds that it should have been passed under the Third Pillar, not the First Pillar. See *Ireland v Council of the European Union*, European Parliament, Case C-301/06, 2006 OJ (C 237) 5 (case pending).

20 See Article 29 Data Protection Working Party, *Opinion 9/2004*, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf> (visited Apr 21, 2007) ("Working Party"); Working Party, *Opinion 4/2005*, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf> (visited Apr 21, 2007); Working Party, *Opinion 3/2006*, available online at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf> (visited Apr 21, 2007).

21 See *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*, 2005 OJ (C 298) 1 ("Opinion of European Data Protection Supervisor").

22 See Data Protection Directive, art 29 (cited in note 1). Formally, the Working Party's jurisdiction extends only as far as that of the Directive, namely initiatives for the European Community (the First Pillar). Id, art 30. However, the Working Party also gives opinions on initiatives in the Third Pillar. This practice appears to have been ratified and codified in the proposed Framework Decision on data protection in the Third Pillar, with the creation of a working party with a nearly identical composition and set of powers. See Proposal for Protection of Personal Data in Criminal Matters, art 31 (cited in note 2).

The other authority—the European Data Protection Supervisor ("Data Protection Supervisor")—is a more recent body, created in 2001 to oversee the use of personal data by European Community institutions.[23] For the most part, the Data Protection Supervisor was conceived as a functional equivalent to the data protection authorities responsible for government oversight at the national level. It was to be responsible, *inter alia*, for: receiving notifications of data processing by European Community institutions like the European Commission; checking that such data processing was lawful; enforcing, with sanctions if necessary, the data protection rules; hearing individual complaints of wrongful data processing; and advising European Community bodies on their more specific data protection administrative rules.[24] Strictly speaking, the Data Protection Supervisor did not have jurisdiction over data processing at the national level nor did he have a right of consultation on directives regulating national data processing. Nevertheless, at the same time the Data Retention Directive was proposed, the European Commission requested an opinion from the Data Protection Supervisor.[25] Therefore, two sets of opinions informed the debate on the Directive.

Was data privacy adequately protected under the Data Retention Directive? As we shall see, the views of the different institutional actors were radically opposed on this question. While the Working Party and the Data Protection Supervisor unequivocally condemned the initial version of the Directive and remained skeptical of the final version, the Council, the Commission, and the European Parliament judged the privacy guarantees in the final version satisfactory.

B. THE RIGHTS ANALYSIS

The best place to begin the analysis of the Data Retention Directive for compliance with the right to data privacy—and where European policymakers began their analysis—is the European Convention on Human Rights ("ECHR").[26] Although the European Union is not a party to the ECHR, it is well-established under treaty law and case law that ECHR rights are guaranteed in the European Union.[27] Article 8 of the ECHR protects the right to private life. An additional set of guarantees, specific to data privacy and critical to this analysis, are contained in Council of Europe Convention 108 ("Convention

---

23 Council Regulation 45/2001, 2001 OJ (L 8) 1.

24 Id, art 46.

25 See Opinion of European Data Protection Supervisor, recitals, ¶ 5 (cited in note 21).

26 See note 5.

27 Treaty on European Union, art 6(2) (cited in note 16).

108").[28] Again, although the European Union is not a party to Convention 108, all the EU Member States are parties. Moreover, Convention 108 served as the main point of reference for the Data Protection Directive.

These legal standards are complex and allow for significant variation in national data protection regimes. For purposes of this analysis, however, the standards can be summarized as follows. Under the case law of the European Court of Human Rights and the European Court of Justice, the storing and processing of personal data for purposes of fighting crime constitutes an interference with the right to private life under Article 8 of the ECHR.[29] Nevertheless, this data processing is permissible if it satisfies three conditions. First, if the processing is done by a public authority or for a public purpose, it must be authorized by a law, accessible to the public, with precise enough provisions to curb arbitrary government action and to put citizens on notice of possible incursions into their private sphere.[30] Second, the purpose of the interference must be legitimate. Namely, the purpose must be related to one of the categories recognized under Article 8. It must be "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[31] Third, the interference with private life must be proportional. Proportionality is comprised of two elements: a search for alternative, less rights-burdensome government means of accomplishing the public purpose and an assessment, not always explicit, of the importance of the right as compared to the public purpose.[32] If the right is sufficiently important and there are alternative means of accomplishing the public purpose, proportionality is breached.

1. Authorization by Law

These steps in the privacy rights analysis were debated by the many institutional players involved in drafting the Data Retention Directive. The entire

---

28 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe Treaties No 108 (Jan 28, 1981), available online at <http://conventions.coe.int/Treaty/en/Treaties/html/108.htm> (visited Apr 21, 2007) (hereinafter "Convention 108").

29 See Opinion of European Data Protection Supervisor at 2, ¶ 9 (cited in note 21).

30 See, for example, *Amann v Switzerland*, App No 27798/95, 30 Eur HR Rep 843, 858 ¶ 50 (2000), available online at <http://cmiskp.echr.coe.int////tkp197/viewhbkm.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=1078&sessionId=10122313&skin=hudoc-en&attachment=true> (visited Apr 21, 2007).

31 ECHR, art 8 (cited in note 5).

32 See, for example, Donald P. Kommers, *The Constitutional Jurisprudence of the Federal Republic of Germany* 46 (Duke 2d ed 1997).

initiative turned on the need to provide a legal basis for the retention of traffic data by private telecommunications providers. Without this, there would be no law authorizing the interference with private life and, as a result, all those involved—communications providers, national police, Member States, and the European Union—would be in breach of their duties under Article 8 of the ECHR. The legal basis contained in the Data Retention Directive would replace divergent national laws specifying the circumstances under which communication providers were required to retain data for law enforcement purposes.[33] On this, all of the institutional actors—Council, Commission, Parliament, Working Party, and Data Protection Supervisor—were in agreement.

They strongly disagreed, however, on whether the Data Retention Directive should also serve as the basis, in law, for police access to traffic data. In other words, should the Directive set down the conditions under which the police would be able to request the retained data from communications providers? This difference turned on the seemingly technical issue of whether data retention should be categorized as a Third Pillar or a First Pillar policy. Once the choice was made to go ahead with the Directive as a First Pillar initiative, the Commission and the Council took the position that, legally speaking, the Directive could not regulate police access to communications data. Anything having to do with the police was strictly Third Pillar. The Working Party, the Data Protection Supervisor, and the European Parliament took the opposite position.[34] This was unsurprising because their institutional clout on the question of police access depended on it. If the issue were regulated nationally, or under the Third Pillar, the power of these supranational institutions would be minimal. Ultimately, a provision on police access was included.[35] The substance of this provision, however, is skeletal compared to what the Parliament, following the lead of the two advisory bodies, had requested.

Related to the choice between the First and the Third Pillar was the debate over the appropriate institutional process for bringing the Directive into line, in

---

33 Since a directive must be implemented at the national level, there are still national laws. However, the room for variation among those national laws has been reduced considerably.

34 See Working Party, *Opinion 4/2005* at 8 (cited in note 20); Opinion of Data Protection Supervisor at 3 ¶ 14, 11 ¶ 80 (cited in note 21). The Parliament, in agreement with these two data protection advisory bodies, proposed a series of amendments giving effect to their recommendations. See Parliament Legislative Resolution, Eur Parl Doc (P6_TA (2005) 0512) 1 (Dec 14, 2005) (approving amended version of the Retention Directive), available online at <http://www.europarl.europa.eu/sides/getDoc.do?objRefId=105467&language=MT> (visited Apr 21, 2007); *Report on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*, Eur Parl Doc (A6-0365/2005) 14, 15–16, 33–34 (2005) ("Parliament Report").

35 Council Directive, art 4 (cited in note 2).

the future, with changing technological and social realities. In the Commission proposal, revisions to the types of traffic data to be retained were to be made by an administrative process: a regulatory comitology committee, which in practice meant close supervision of the Commission's rulemaking by the Council.[36] The data protection bodies and the Parliament objected. For an issue with such far-reaching implications for fundamental rights they advocated the full-blown legislative procedure of co-decision, under which the Parliament would have a right to vote. In the view of the Parliament and the data protection bodies, Europe's only directly elected legislative body should be entitled to decide.[37] Ultimately, the position shared by the data protection bodies and the Parliament prevailed.

This division between the Council and the Commission on the one hand, and the Parliament and the data protection bodies on the other, was driven not by the need to enact a law authorizing the interference with the right to privacy, but by different views of which type of law was most legitimate. Under Article 8 of the ECHR, any national or EU law is satisfactory as long as it is precise and accessible to the public.[38] The debate, therefore, was not about rights but about the nature of EU democracy. In the view of the Council and the Commission, national ministries of the interior, sitting on the Council, should alone decide on the privacy safeguards to be respected by the police. The unanimity requirement, which gives each state a veto right, together with the power of national parliaments to supervise their executives, would ensure that the decisions of the Council would respect the will of European electorates. By contrast, the European Parliament and the data protection authorities argued that the Council, together with the Parliament, should decide on the privacy safeguards to be put into place. In their view, as a directly elected, democratic body, the European Parliament would improve the deliberative, rights-abiding quality of the law. But even though this position might have surface appeal, the correct outcome is far from self-evident. Many believe that the European Parliament is more removed from the European people than the national governments that sit on the Council and the national parliaments that hold their governments in check. If this is indeed true, then the Council, not the European Parliament, is the more democratic legislator.

---

36 See Commission Proposal, arts 5, 6 (cited in note 18).

37 See Opinion of European Data Protection Supervisor ¶ 60 (cited in note 21); Working Party, *Opinion 4/2005* at 9 (cited in note 20); Parliament Report at 34 (cited in note 34).

38 Under German constitutional law, by contrast, government action that interferes with certain types of basic rights must be taken pursuant to parliamentary statute. See Sabine Michalowski and Lorna Woods, *German Constitutional Law: The Protection of Civil Liberties* 80–81 (Ashgate 1999).

In sum, the Data Retention Directive was enacted to comply with the first condition of data privacy: any interference, including the retention and use of traffic data to assist with criminal investigations, had to be authorized by law. But the debates that emerged over the form of law to be used were focused on a very different set of concerns. For some, the Council was the repository of legitimacy and for others it was the European Parliament. While the decision to regulate only minimally the terms of police access represented a victory for the Council position, the choice of a co-decision legislative process to revise the list of traffic data represented a victory for the Parliament's position.

2. Legitimate Purpose

The institutions also debated the second step of the rights analysis: legitimate purpose. To satisfy Article 8 of the ECHR, the retention requirement had to advance a legitimate purpose. At the beginning of the legislative debate, the purpose of data retention was quite broad. In the Council's draft, the data was to be used to fight all crimes. Moreover, it was to be used not only to investigate and to prosecute past crime, but to prevent future crimes.[39] In the Commission's proposal, the crimes were paired down to "serious criminal offences, such as terrorism and organised crime."[40] In the final version, the purpose was further narrowed: prevention of crime was stricken from the text. Thus the provision now reads: "The Directive aims to harmonise Member States' provisions . . . for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."[41] The decision to limit the use of traffic data to serious criminal offenses and to exclude crime prevention can be traced to the Working Party and the European Parliament. Both were extremely critical of the nearly unfettered rights of access that such broad purposes would confer upon police authorities.[42]

Notice, however, that the debate did not focus on the legitimacy of the government purpose. Under Article 8 of the ECHR, the use of data to fight any type of crime is considered legitimate. Even the original Council proposal would have satisfied this part of the analysis. Rather, the debate was driven by the logic of the proportionality test: the greater the importance of the government's purpose, the more deference should be afforded government actors in deciding the rights-burdening means by which such a purpose will be accomplished. In the eyes of the data protection advocates, such a massive data retention program

---

39 Draft Framework Decision, art 1 (cited in note 17).

40 Commission Proposal, art 1 (cited in note 18).

41 Council Directive, art 1(1) (cited in note 2).

42 See Working Party, *Opinion 4/2005* at 8 (cited in note 20); Parliament Report at 33 (cited in note 34).

could be justified only by the need to catch the perpetrators of serious crimes and the perpetrators of crimes that were certain, not speculative.

3. Proportionality

Proportionality proved to be the thorniest issue of all. The proportionality test has many different formulations, depending on the court and the commentator.[43] Even in the same court and on the same panel, the test can be articulated differently.[44] At the very least, however, the following questions must be addressed: Is there evidence that government action can achieve the stated purpose? Is the government action necessary for accomplishing the stated purpose or would alternative means accomplish the same purpose with a lesser burden on the privacy right?[45] The burden of justification under the proportionality test lies with the government and varies tremendously, depending on the right at stake and the public interest being pursued: the more important the right, the higher the burden on the government; and the more important the public purpose, the lower the burden on the government.[46]

When the privacy right at stake is data protection, the proportionality investigation is guided by some of the more specific guarantees of Convention 108.[47] Since every instance in which data traceable to an individual is collected and processed is considered an intrusion into private life, all such data must be "adequate" and "relevant" to accomplishing the government purpose.[48] To ensure that personal data processing can accomplish the government's purpose, such data must be "accurate and, where necessary, kept up to date."[49] The

---

43 See, for example, Catherine Barnard, *The Substantive Law of the EU: The Four Freedoms* 79–82, 243–44 (Oxford 2004); Paul Craig and Gráinne de Búrca, *EU Law: Text, Cases, and Materials* 371–79 (Oxford 3d ed 2002).

44 For instance, compare the different versions of the proportionality test in the majority opinion in *Leyla Şahin v Turkey*, App No 44774/98, 2005-XI Eur Ct HR, ¶ 71 (2005), available online at <http://cmiskp.echr.coe.int////tkp197/viewhbkm.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=11423&sessionId=10122336&skin=hudoc-en&attachment=true> (visited Apr 21, 2007), with the dissent in *Leyla Şahin v Turkey*, App No 44774/98, 2005-XI Eur Ct HR, ¶ A1 (2005) (Tulkens, J dissenting), available online at <http://cmiskp.echr.coe.int////tkp197/viewhbkm.asp?action=open&table=F69A27FD8FB86142BF01C1166DEA398649&key=11423&sessionId=10122336&skin=hudoc-en&attachment=true> (visited Apr 21, 2007).

45 A third common element of the proportionality inquiry—although employed generally only when the burdened right is a non-economic right—is whether, even in the face of the necessity of the measure for accomplishing the purpose, the right trumps the government action. Kommers, *Constitutional Jurisprudence* at 46 (cited in note 32).

46 See Opinion of Advocate General Léger ¶¶ 228–30 (cited in note 6).

47 Convention 108 (cited in note 28).

48 Id, art 5(c).

49 Id, art 5(d).

amount of data processed and the time during which it is stored should be no more than necessary to accomplish this purpose.[50] Moreover, security precautions must be taken to guarantee that the data is used only by those entities and for those purposes for which it was collected originally.[51] Finally, as a special safeguard for the privacy right, individuals should have the right to check their personal data to make sure that it is accurate and that, in all other respects, it is being processed in accordance with the law.

Neither the Working Party nor the Data Protection Supervisor believed that lawmakers had satisfied the proportionality test. On the first question—whether data retention could accomplish the crime-fighting purpose—the two data protection bodies were skeptical. Neither believed that lawmakers had demonstrated with enough certainty that communications data over six months old would be useful in investigating crimes.[52] In other words, they did not believe that the legislature had shown that the government measure could achieve the stated crime-fighting result. The evidence in favor of data retention was drawn largely from figures provided by the United Kingdom on police requests for communications data.[53] According to these figures, traffic data older than six months was often useful in investigating serious crimes. Both data protection bodies dismissed this evidence as inadequate.[54] European legislators, however, were persuaded otherwise, as demonstrated by the enactment of the Data Retention Directive.

The most divisive aspect of the proportionality debate lay elsewhere: the length of the data retention period and the amount of data to be retained. Was it truly necessary to keep so much traffic data for so long to accomplish the crime-fighting purpose? The original Council proposal would have required data retention for a period of one to three years.[55] In other words, in their implementing legislation, Member States could have chosen anything from a one- to a three-year data retention period. For some, this period was disproportionate and excessive in light of the measure's burden on the privacy right. Responding to this criticism, the Commission reduced the data retention period considerably. The proposed directive would have required call data to be

---

50 Id, art 5(c); Id, art 5(e) (referring to storage time).

51 Id, art 7.

52 See Note from Council Presidency to COREPER/JHA Council, Council Doc 15220/05, 2 (Dec 1, 2005) (on limiting purpose to fighting serious crime); Opinion of European Data Protection Supervisor ¶ 27 (cited in note 21) (on eliminating crime prevention); Working Party, *Opinion 4/2005* at 6 (cited in note 20) (on eliminating crime prevention).

53 Opinion of European Data Protection Supervisor ¶ 16 (cited in note 21).

54 Id ¶¶ 16, 61; Working Party, *Opinion 9/2004* at 4 (cited in note 20).

55 See Draft Framework Decision, art 4 (cited in note 17).

retained for one year, and email and voice-over Internet protocol data to be retained for six months.[56] After negotiations in the Council, however, the retention period in the final version was lengthened to between six months to two years for all data. In this political compromise between the security-minded officials in the Council and the data protection advocates in the oversight bodies and the Parliament, the difference was split exactly in two: one year shorter than the Council's initial position, one year longer than the Parliament's position.

As for the amount of data to be retained, it was clear from the very beginning that the Data Retention Directive would *not* cover content data.[57] Communications providers would not be given a mandate to create vast databases of telephone conversations and email correspondence that could then be tapped by law enforcement officials. Also, at the very beginning, legislators settled on six categories of traffic data to be gathered: (1) data on the source of the communication, such as the telephone number originating the call; (2) data on the destination of the communication, such as the telephone number receiving the call; (3) data on the date, time, and duration of the communication; (4) data on the type of communication—namely whether it was a phone call, a voicemail message, a text message, an email, or a voice-over Internet protocol; (5) data necessary to identify the equipment used by the parties to the communication; and (6) data necessary to identify the location of mobile equipment such as cell phones for the duration of the communication.[58]

Later, however, two points of contention over data content emerged. Some of those involved in the legislative debate argued that a call that was made, but not answered, should be considered a "communication" and therefore be retained. Some of the institutions also pushed for location data on mobile equipment such as cell phones to be collected for the entire call, enabling the police not only to monitor calls, but also to track the movements of individuals. The Working Party, on the other hand, recommended retention only for successful calls and only for the location of mobile devices at the beginning of the call.[59] The European Parliament in essence adopted the Working Party's recommendation.[60] The Council and the Commission, however, successfully resisted this recommendation. In the final version of the Directive, data on

---

56 Commission Proposal, art 7 (cited in note 18). The Commission's position was largely satisfactory to the data protection bodies and the European Parliament. See Opinion of European Data Protection Supervisor at 11, ¶ 83 (cited in note 21); Working Party, *Opinion 4/2005* at 6–7 (cited in note 20); Parliament Report at 22, 35 (cited in note 34).

57 See Draft Framework Decision, art 1(2) (cited in note 17).

58 See id, art 2(2); Commission Proposal at Annex (cited in note 18).

59 Working Party, *Opinion 4/2005* at 10 (cited in note 20).

60 Parliament Report at 35 (cited in note 34).

unsuccessful calls and on the location of mobile equipment throughout the call must be retained.[61]

As explained earlier, the proportionality inquiry can turn on the existence of an equally feasible and equally effective government measure with a lower burden on the privacy right. According to the data protection watchdogs, retaining less data for a shorter time was one such government measure. But they also had in mind another, less privacy-burdening means of getting the traffic data necessary to catch criminals: a "quick-freeze procedure."[62] Under this procedure, when the police have a suspect in mind, yet still do not have evidence that would satisfy the standard for obtaining a court warrant, they can ask communications providers to store that person's communications data. If at a later point the police do have the evidence necessary for a court warrant, they can obtain access to the data. This alternative, however, did not surface in any other parts of the legislative history, and it does not appear to have been taken seriously by the other institutional players.

C. IS PRIVACY ADEQUATELY PROTECTED?

With this understanding of the legislative debates underpinning the Data Retention Directive, the question posed earlier can now be addressed: Will the Data Retention Directive adequately protect privacy? Overall, the answer is yes. Two critical aspects of the Directive support this conclusion: the type of law that serves as the basis for the interference with the right to privacy, and the measure's proportionality.

1. Type of Law

With the Data Retention Directive, an accessible, detailed, and democratically enacted law serves as the basis for personal data processing by communications providers. Police access to communications data is also based on accessible, detailed, and democratically enacted laws, albeit laws that are scattered among various sources—the Data Retention Directive, national laws regulating police surveillance of electronic communications, and, once agreement is reached in the Council, an EU law protecting personal data in police cooperation on criminal matters.[63] In addition, any future changes to data retention duties, even those changes that appear merely technical and administrative, will have to be made through the democratic process.

---

61 See Council Directive, arts 3(2) (retention of unsuccessful call attempts), 5(f)(2) (location data) (cited in note 2).

62 See Opinion of European Data Protection Supervisor ¶ 20 (cited in note 21); Working Party, *Opinion 4/2005* at 6 (cited in note 20).

63 Proposal for Protection of Personal Data in Criminal Matters (cited in note 2).

The decision to go forward under the First Pillar was salutary. Of course, this was not strictly necessary under the European right to privacy. Any rule that is detailed and available to the public satisfies the requirements of the ECHR. Yet the involvement of a directly elected legislature improves the transparency of rights-burdening rules, thus promoting the goals underlying the requirement of authorization by law. Indeed, under German constitutional law, only the German Parliament may enact laws that intrude upon basic rights. Giving the European Parliament co-decision powers meant that the decision to amass huge amounts of personal data concerning ordinary citizens was more visible and was debated more vigorously than it otherwise would have been. Additionally, the Council's burden of justification for this data-gathering initiative was more substantial once the matter had to be decided by the Parliament. In other words, involving the European Parliament had the great merit of putting data retention and its privacy implications in the public eye. Furthermore, even though it is difficult to prove with any degree of certainty, some of the changes in the final version seem to have been the product of this higher burden of explanation. It appears that once the Council was forced to explain the more intrusive aspects of the proposed directive, it backed down. The Council concluded that routine law enforcement methods, as opposed to privacy-invading retention of communications data, would suffice for ordinary crimes like theft. The Council also decided that communications data over two years old would not be particularly useful to the police because those plotting a serious crime like a terrorist attack could be expected to communicate at some time within the two years leading up to the attack.

It certainly is true that even when the Council alone enacts legislation under the Third Pillar, it is subject to democratic checks: the European Parliament is consulted and national governments that sit in the Council must answer to their national parliaments, some of which can be very exacting. Moreover, under the Third Pillar, the voting rule is unanimity, meaning that each government must consent to every measure. Yet, the actual experience with democracy via national parliaments' control of their governments has been disappointing. The basic difficulty is that as an issue is being negotiated among governments, those governments demand secrecy, and after the issue has been decided, the intergovernmental bargains can be unraveled only at considerable cost. Giving the European Parliament real powers is one of the easiest ways of overcoming the shortcomings of national parliamentary control in the supranational, European context.

The Working Party and the Data Protection Supervisor also improved the quality of the deliberative process. This was because of their expertise on privacy issues, as well as their experience with comparable national legislation on data retention. Based on this background knowledge, the two data protection bodies could easily spot the shortcomings of the data retention initiative. Their

familiarity with the policy area also enabled them to suggest policy alternatives to the proposals of the Council and the Commission. It is not surprising that most of their recommendations made their way into the Parliament's amendments. Few parliamentarians can be expected to have experience with data protection; to protect privacy rights, the Parliament naturally looked to these two independent data protection watchdogs for guidance.

2. Proportionality

The data retention scheme also satisfied the demands of proportionality. A maximum retention period of two years appears reasonable. It takes time to plan certain types of crimes, and it is not unthinkable that, even two years before the event, the conspiracy might have begun to take shape and leave communications traces. In this respect, the data protection watchdogs were overly severe. As recounted earlier, they wanted solid, social scientific proof of the usefulness of communications data over six months old. This, however, was unrealistic. Such certainty is hard to give in the face of rapidly changing technologies—changes that affect both how electronic communications can be used to commit crimes and how the police can use communications records to combat crime. In a similar vein, it was impractical for the watchdogs to insist on proof that their favorite policy alternative—the quick-freeze procedure—would be less effective in fighting crime than data retention. Certainly, this discussion of alternative law enforcement techniques was extremely valuable. But, again, in light of the technological uncertainties and the importance of protecting public security, the expectations of the data protection watchdogs were set too high.

Like the maximum retention period of two years, the amount of personal data to be retained also appears reasonable. The main dispute in this regard was over data relating to unsuccessful calls. In the final text, data on such calls must be retained. It is difficult for the layperson to know the value of information on calls made, but not answered, by a suspected criminal. Perhaps, since only calls involving at least two parties can count as evidence of a conspiracy, only completed calls are helpful in investigating crimes. Yet an unsuccessful call might indicate to the police that the two parties conspired in the real, non-digital world. And with caller identification, even a call that goes unanswered is capable of communicating information to a co-conspirator. Although certainly not foolproof, these arguments in favor of retention are at least plausible.

The Data Retention Directive's provisions on record-keeping contribute to the proportionality of the measure. Under the Directive, the Member States must provide yearly figures on the number of times that traffic data is transferred to the police, the age of the transferred data, and the number of

instances in which police requests for data could not be satisfied.[64] Good documentation on police use of communications data enables future legislators to determine whether the data in fact contributes to fighting crime. It gives legislators the tools to assess, over time and in light of national experience, whether such information does indeed improve public security. This provision could have required national police to collect more detailed information—for instance to break down data by the type of electronic communications involved. However, in light of the limits on the bureaucratic resources that can be devoted to such information-gathering initiatives, the record-keeping provision is a valuable first step. If it were to emerge that communications data over a year old are hardly ever used, then it would be appropriate to consider the data retention program disproportionate and to amend the Directive.

Critical to this assessment of the Data Retention Directive's proportionality are the different privacy safeguards contained in the Directive. The investigation of ordinary crimes and crime prevention were eliminated as acceptable uses of personal data. Moreover, the duties of communications providers are laid down in some detail: they must adopt various measures to keep personal data safe from theft and fraud; they are strictly forbidden from using the data for their own commercial purposes; and they are specifically directed to erase the data after the retention period.[65] Most importantly, national police are allowed to access the data only "in specific cases."[66] This provision is designed to prohibit data mining—hi-tech fishing expeditions. This falls into line with the emerging European trend to prohibit data mining, whether done by the police for imperative security reasons or by market actors for less important profit motives. The police cannot make blanket requests for calling information. Rather, they must compile detailed requests for information on specific telephone numbers. The requirement of specificity is a means of guaranteeing that the police have at least some grounds for suspecting those telephone numbers of being involved in a criminal conspiracy.

If specificity is combined with other legal checks on national authorities, the threat to privacy will be diminished considerably. For instance, the draft legislation on Third Pillar data protection might be amended to contain a warrant requirement for access to personal data.[67] A new measure guaranteeing

---

64 Council Directive, art 10 (cited in note 2).

65 Id, art 7.

66 Id, art 4.

67 See Note from Council Presidency to Multidisciplinary Group on Organised Crime, Council Doc 6450/1/06 (Mar 23, 2006), available online at <http://www.statewatch.org/news/2006/mar/eu-dp-coun-draft-pos-6450-rev1-06.pdf> (visited Apr 21, 2007). As the proposal currently stands, the police would have to provide a "factual indication" that personal data will help investigate or

data protection in the work of intelligence agencies—not covered by the Third Pillar legislation—would also be welcome.

IV. FINAL THOUGHTS: PROTECTING RIGHTS IN CRIME-FIGHTING INITIATIVES

The sharing of personal data among national police authorities—and the countervailing need for data protection—is but one of many examples of the rapidly growing field of European cooperation on criminal matters.[68] What light can the experience with data privacy in the Data Retention Directive shed on the protection of fundamental rights more generally in the European Union's emerging system of criminal justice?

One of the most impressive aspects of the Council's bid to mandate a massive system of data collection was the publicity and the quality of the legislative debate. But that debate was achieved largely in spite of, not because of, EU law. The decision to go forward under the First Pillar was disputed. A plausible argument could be made that having different police regulations on data retention across Europe imposes significant costs on pan-European communications providers and that harmonization of such regulations was necessary for economic reasons. But a provision on the conditions of national *police* access to the retained data, even as minimal a provision as was included in the Directive, was highly questionable. Objectively speaking, police access was a Third Pillar matter. Similarly, it was doubtful that the Data Protection Supervisor's opinion was his to give. The legislation under which the Data Protection Supervisor was established was aimed at guaranteeing privacy in the data processing operations of the European Community's own institutions. It was not directed at protecting privacy at the national level.

The mismatch between what is good—for rights and democracy—and what is the law is an artifact of the European Union's idiosyncratic historical trajectory. The European Union is proving to be the nation-state in reverse chronology. The functions that the nation-state developed first—protection from physical violence—the European Union is acquiring last. Those functions that the nation-state acquired last—administrative regulation of complex markets—the European Union took on first. Because nation-states have been reluctant to cede sovereignty over their core protection functions, these matters

---

prevent a crime but would not have to go before an independent government officer. See Proposal for Protection of Personal Data in Criminal Matters, art 5 (cited in note 2).

68 For a comprehensive list of such initiatives as of March 23, 2004, see Statewatch, *Statewatch's "Scoreboard" on the Threats to Civil Liberties and Privacy in EU Terrorism Plans*, (Mar 2004), available online at <http://www.statewatch.org/news/2004/mar/21eu-terr-scoreboard.htm> (visited Apr 21, 2007).

are governed by the Third Pillar. Yet precisely because tools of coercion are necessary to keep public order, classic liberal rights are especially important in this area of government activity. Decisions concerning the criminal justice system should not be secretive. And they should not be made by national ministries of the interior acting alone, as is largely the case when decision-making power rests with the Council. While the bureaucratic mission of protecting public security is all-important, it can also be blindsiding. Other public servants, attentive to other public values, as well as ordinary citizens, should take part in the process.

At this stage, it is probably too much to ask for the Third Pillar to be amended out of existence.[69] The data retention experience, however, suggests a more modest reform that would render debates on criminal cooperation more public and that would encourage a more balanced, rights-attentive approach to legislation: a human rights analogue to the data protection authorities. An EU human rights body, with advisory powers over Third Pillar initiatives, would improve the emerging criminal justice system. Such a government body would bring a wealth of national experience to bear on Europe-wide cooperation. Through its organization—which would probably take the form of a network of national ombudsmen and human rights advocates—it would render the Council's initiatives more visible at the national level. The agency's opinions would focus public attention on Third Pillar proposals and their flaws. And this human rights watchdog would improve the European Parliament's contribution on Third Pillar matters: the Parliament could use the watchdog's opinions as a point of departure in exercising its power of consultation.

This suggestion is not novel. On February 15, 2007, after over two years of legislative debate, a European Union Agency for Fundamental Rights ("Agency") was established.[70] It is charged with gathering data and conducting studies on rights abuses in the Member States, with the aim of promoting better implementation of existing EU laws and identifying new areas for legislative action. The Agency's powers, however, are limited. It can advise on proposed EU laws only if requested to do so by one of the institutions involved in the legislative process.[71] More to the point of this discussion, the Agency has power only over First Pillar matters, not over criminal justice matters in the Third

---

69 The Constitutional Treaty would have abolished the European Union's pillar structure. In doing so, it would have extended the more transparent and democratic procedures of the First Pillar to criminal cooperation initiatives currently in the Third Pillar. It is unlikely, however, that the Constitutional Treaty will be ratified any time soon.

70 Council Regulation No 168/2007 of 15 February establishing a European Union Agency for Fundamental Rights, 2007 OJ (L 53) 1.

71 Id, art 4.2.

Pillar.[72] Yet the involvement of rights advocates in the drafting of the Data Retention Directive demonstrates precisely how valuable their advice can be for proposed criminal legislation in the Third Pillar.

Indeed, in the debates over the shape of the future agency, a number of participants took the view that the Agency should exercise such powers. The Select Committee on the European Union of the UK House of Lords released a report recommending that the Agency's mandate be extended to reviewing proposed laws in the Third Pillar.[73] From the very beginning, the Commission proposed that the Agency should have powers both in the First and the Third Pillars.[74] Yet to secure a deal among the Member States sitting in the Council, the Third Pillar component of the legislative package was dropped at the eleventh hour.[75] A handful of Member States were adamantly opposed to giving the Agency prerogatives over such a sensitive area of national sovereignty and were determined to use their veto power to block the initiative.

Going forward, the positive experience of the Data Retention Directive should be kept in mind. The founding charter of the Agency will undoubtedly be amended in the future, at which time the issue of powers will be revisited. The protection of the right to privacy in the Data Retention Directive demonstrates that human rights scrutiny can be extremely valuable and that it can work on Third Pillar matters when basic rights come under pressure from the police, prosecutors, and the courts.

---

72 Id, arts 2, 3.

73 See House of Lords, Select Committee on European Union, Human Rights Protection in Europe: The Fundamental Rights Agency, 29th Report of Session 2005–2006, HL Paper 155 ¶ 80 (Apr 4, 2006).

74 Proposal for a Council Regulation establishing a European Union Agency for Fundamental Rights and Proposal for a Council Decision empowering the European Union Agency for Fundamental Rights to pursue its activities in areas referred to in Title VI of the Treaty on European Union, COM (2005) 280 final.

75 See Note from President to Council, Council Doc 16108/06 at 4 (Nov 29, 2006), available online at <http://register.consilium.europa.eu/pdf/en/06/st16/st16018.en06.pdf> (visited Apr 21, 2007).