DUKE LAW SCHOOL

Duke Law School
Science, Technology and Innovation
Research Paper Series

Research Paper No. 13
January 2007

Protecting Privacy against the Police in the European Union: The Data Retention Directive

Francesca Bignami
Professor of Law
Duke Law School
bignami@law.duke.edu

PROTECTING PRIVACY AGAINST THE POLICE IN THE EUROPEAN UNION: THE DATA RETENTION DIRECTIVE

Francesca Bignami*

Forthcoming, *Chicago Journal of International Law*, *Spring 2007*

ABSTRACT

This paper examines a recent twist in EU data protection law. In the 1990s, the European Union was still primarily a market-creating organization and data protection in the European Union was aimed at rights abuses by market actors. Since the terrorist attacks of New York, Madrid, and London, however, cooperation on fighting crime has accelerated. Now, the challenge for the European Union is to protect privacy in its emerging system of criminal justice. This paper analyzes the first EU law to address data privacy in crime-fighting—the Data Retention Directive. Based on a detailed examination of the Directive's legislative history, the paper 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—was 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.

INTRODUCTION

A world without data privacy would be a bit like a world in which we were all animals in a zoo. Based on our millions of pieces of electronic data, we would be the object of constant inspection by others. Like the giraffes and the pandas, we would never be asked, "Excuse me, but do you mind if I look?" And, like the giraffes and the pandas, we would never be able to reply "Yes, I do mind. *Go away*!"

In the European Union, data privacy is one of the oldest of human rights policies. The Data Protection Directive, proposed in 1990 and passed in 1995, sets down a

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

complex regulatory scheme at the national level to protect individual rights.[1] In the 1990s, data protection was aimed at possible abuses by market actors or by government agencies as service providers—to be expected in a European Union still focused on the common market. Recently, however, EU data protection has taken a new turn. Now the challenge is to safeguard privacy against governments when they exercise their core sovereignty powers: domestic policing and protecting national security.

This essay examines the European Union's new turn towards protecting personal data against the police. The first part explores the developments that have given rise to these policies: the dramatic possibilities of today's digital technologies for the police 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 piece of legislation with the most significant data protection ramifications to be enacted at the time of this writing: the Data Retention Directive.[2] The essay concludes with some thoughts on how the largely positive rights 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.

I. 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. Their focus was large-scale data collection by the government and 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 hit hardest those parts of government administration that routinely and publicly collected large amounts of information from citizens for purposes of providing services such as health care,

[1] See generally Francesca Bignami, Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network, 26 Mich. J. Int'l L. 807, 813-19, 837-45 (2005).

[2] Directive 2006/24/EC, 2006 O.J. (L 105) 54 (on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC). At the time of this writing, two other initiatives with far-reaching consequences for data protection were being negotiated in the Council: the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM (2005) 475 final (Oct. 4, 2005), and the Proposal for a Council Framework Directive on the exchange of information under the principle of availability, COM (2005) 490 final (Oct. 12, 2005).

education, and welfare. Intelligence and law enforcement officials were relatively untouched by data protection regulation. Under their national laws, intelligence and law enforcement officers were prohibited from accessing—indiscriminately—the records of other government agencies. They had to answer petitions from individuals seeking to verify that information in police and security files was accurate. Otherwise, such information-gathering activities fell under the legal umbrella of criminal procedure. Eavesdropping on phone calls, bugging homes, and other forms of surveillance were covered by a specific set of criminal procedure laws. For the most part, the police had to apply for warrants from the judicial authorities before they could undertake surveillance. In contrast, intelligence officers responsible for security-related surveillance were subject to less rigorous standards and were overseen by independent government officials or parliamentary committees.[3]

Since the 1970s, one development has radically altered the nature of law enforcement and, with it, the relationship between law enforcement and data protection laws: technology. Increasingly, we live our lives in digital space. We run our errands, conduct our business, and socialize with our friends in the virtual world of the internet. When not connected to the web, we are on our cellphones. 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 for many different types of actors: direct marketers, credit agencies—and law enforcement officials. By monitoring our internet traffic, the police can learn, in minutes, where we like to shop, what we do in our spare time, how we make a living, with whom we have personal ties. And that is but one small example of what can be done, now, and what might be done with our data in the future to investigate and prevent criminal acts.

The use of this wealth of information by government investigators has given rise to a host of new privacy concerns that old-fashioned criminal procedure cannot address. Under criminal procedure rules, before government investigators can review personal

[3] For a description of the German and U.S. systems, see Paul M. Schwartz, German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance, 54 Hastings L. J. 751 (2002-2003).

records, they must demonstrate to an independent judicial officer their reason to believe that a crime has been committed and that a search of those records will produce evidence of the crime. But when the records are electronic, such criminal procedure rules are inadequate. They are ill-suited both to preventing possible abuses, by the police, of private facts once gathered, and to protecting the more general liberty interest in being free of constant government surveillance.

Because of the ease with which electronic records are stored and transmitted, the risk of security breaches by third parties who wish to use our personal data fraudulently is much greater than with paper records. For example, our credit cards are more likely to be wrongfully charged and our bank accounts wrongfully emptied when our information is stored electronically rather than on paper. Not only third parties, but also government officers can more easily engage in fraudulent uses of personal information when that information is electronic rather than paper.

More importantly, the threat of government fishing expeditions increases exponentially with electronic data. On a fishing expedition, investigators review correspondence, bills, and other types of personal records without any clear expectation of what type of evidence, or what type of crime, they might find. 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.

What about old-fashioned criminal procedure? Why not put an independent judiciary between the police and the data and require the police to demonstrate to the judiciary that the data will likely turn up evidence of a crime? Not only data such as the content of emails, but also information on when and to whom emails are sent. When data is electronic, not only does the government temptation to engage in over-reaching surveillance increase, but the perceived privacy interest in each piece of personal data decreases. Even in Europe, where traffic data is protected under the fundamental right to privacy, the privacy interest in such data is perceived as one less substantial than, for instance, the privacy interest in the content of an email, a phone conversation, or a

personal diary. What we reveal about ourselves in the former is believed to be far less significant than what may be revealed in the latter.

Enter personal data protection. Before the terrorist attacks in New York, Madrid, and London, such data protection rules would have fallen to national legislators, together with the Council of Europe. Jurisdiction (*competence*) over police matters was still strictly national, with a limited oversight role for the Council of Europe[4] and the Schengen Joint Supervisory Authority.[5] The European Union's data protection rules were designed to regulate market actors, not the police.[6] As Advocate General Léger observed in a recent opinion, the Data Protection Directive, adopted in 1995, expressly does *not* apply to data processing for purposes of public security and criminal law enforcement.[7]

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-Europe cooperation on fighting terrorism. Instead, these attacks have triggered collaboration on a wide range of law enforcement matters.[8] The exchange of personal data to prevent and to prosecute criminal acts is a critical form of such collaboration.[9]

---

[4] 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 contains rules applicable to private and public actors, including the police; the Convention establishes a committee of representatives of the signatory parties, whose mission it 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 the 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.

[5] The Schengen Joint Supervisory Authority is a committee of representatives of the parties to the Schengen Convention. It is responsible for overseeing compliance with data protection principles when the police and the judiciary cooperate under the auspices of Schengen. The most important element of this cooperation is the Schengen Information System, a jointly managed data base with information on immigrants and individuals suspected of criminal activity.

[6] Article 68 of the Charter of Fundamental Rights guarantees the protection of personal data in all the European Union's activities. Although the Charter is binding on the institutions of the European Union, it cannot be enforced in the European Courts.

[7] Cases C-317/04 and C-318/04, European Parliament v. Council and European Parliament v. Commission, para. 96.

[8] See Jörg Monar, Problems of Balance in EU Justice and Home Affairs and the Impact of September 11, in Police and Justice Co-operation and the New European Borders 165-82, 177 (Malcolm Anderson & Joanna Apap eds., 2002).

[9] European Commission, Communication to the Council and the European Parliament: Towards enhancing access to information by law enforcement agencies, COM (2004) 429 final, June 16, 2004.

The corollary of EU law enforcement are EU privacy rights against unwarranted intrusions by law enforcement officers. Before handing over data, evidence, or, indeed, suspects, the police and judiciary of one state must be convinced that the police and judiciary of the other, requesting state will respect the rights of their nationals. They must have a great deal of confidence in the fairness of the other state's justice system. The same goes for citizens, because any citizen is potentially at risk of being investigated, tried, and imprisoned in another country. In recent years, therefore, a number of attempts have been made to set down a common rights framework for the European Union's criminal justice system.[10] Data protection is one piece of that rights package.

II. THE DATA RETENTION DIRECTIVE

On March 15, 2006, the Data Retention Directive was passed.[11] Its aim was to facilitate Europe-wide cooperation on 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.[12] This traffic data includes the information necessary to identify the originator and the recipient of phone calls and emails (including internet telephony), together with information on the time, date, and duration of phone calls and emails.[13] Such data must be made available to the national police and, via national police, to police officers in other Member States.[14]

Why was such a directive necessary? Why wouldn't communications providers store traffic data on their own initiative? Unlike the United States, where communications providers routinely store such information for marketing purposes,[15] in Europe, communications providers have been legally required, for decades, to erase such information as soon as it is no longer useful for billing purposes.[16] When, in the wake of

[10] See, e.g., Proposal for a Framework Decision on certain rights in criminal proceedings throughout the European Union, COM (2004) 3289 (final), April 28, 2004.
[11] Directive 2006/24/EC, 2006 O.J. (L 105) 54 (on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) (hereinafter "Directive").
[12] Directive, arts. 3, 6.
[13] Directive, art. 5.
[14] Directive, arts. 1, 4, 8.
[15] Is Nothing Private?, Newsweek, May 22, 2006, p. 22.
[16] See, e.g., Directive 2002/58/EC, art. 6, 2002 O.J. (L 201) 37.

the terrorist attacks, police authorities became convinced that such information was indispensable to fighting crime, a law was needed to reverse the presumption in favor of information destruction.

The Directive's procedural history was rocky. The first complication was the 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 powers to fight crime, known as the Third Pillar. The principal aim was to promote cooperation on law enforcement by improving the information available to the police. Yet the initiative also had a plausible single-market effect: by standardizing the data retention requirements imposed on electronic communications providers by their police authorities, it would be easier for providers to do business in multiple jurisdictions. The choice of the measure's legal basis mattered because of the less supranational character of the Third Pillar: a Third Pillar measure could be proposed by single Member States, not only by the Commission, as under the First Pillar; to pass a Third Pillar measure, unanimity in the Council would be necessary, whereas to pass a First Pillar measure, only a qualified majority was needed; in the Third Pillar, the European Parliament would only be consulted, but in the First Pillar, the European Parliament would enjoy full legislative prerogatives under the co-decision procedure; moreover, the Court of Justice's jurisdiction over a Third Pillar measure is narrower than over a First Pillar measure.[17]

Initially, the measure was proposed by France, Ireland, Sweden, and the United Kingdom as a framework decision under the Third Pillar.[18] A year later, however, the institutions reversed course: the measure was proposed by the Commission as a First Pillar harmonization directive,[19] and it was finally passed, in March 2006, on that same legal basis. Ultimately, the more democratic co-decision procedure appeared better

[17] See Treaty on European Union, art. 35. 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. Fourteen out of twenty-five Member States had acceded to the Court of Justice's jurisdiction. Council, Information concerning the declarations by the French Republic and the Republic of Hungary on the their acceptance of the jurisdiction of the Court of Justice, 2005 O.J. (L 327) 19.

[18] Draft Framework Decision, Council Doc. 8958/04, April 28, 2004

[19] Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM(2005) 438 final, Sept. 21, 2005. The legal basis for the proposed and the final versions of the directive was EC Treaty, art. 95.

suited to an issue with implications for a fundamental right—the right to personal data protection.

A second complication was the plethora 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, sometimes on its own initiative, on legislative initiatives with data protection ramifications. The other authority—the European Data Protection Supervisor—is a more recent institution, created in 2001 to oversee the use of personal data by European Community institutions.[23] For the most part, the European 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 for receiving notifications of data processing by Community bodies 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 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, including the right of consultation on directives regulating national data processing. Yet, at the same time that the European Commission proposed the Data Retention Directive, it

[20] Opinions 9/2004 (Nov. 9, 2004), /2005 [WP 113] (Oct. 21, 2005), and 3/2006 (Mar. 25, 2006) of the Article 29 Data Protection Working Party.
[21] Opinion of the European Data Protection Supervisor (Sept. 26, 2005), 2005 O.J. (L 298) 1.
[22] See Data Protection Directive, art. 29. Formally, the Working Party's jurisdiction extends only as far as that of the Directive, namely, initiatives for the European Community (the First Pillar). See art. 29.3. However, the Working Party also gives opinions on initiatives in the Third Pillar. This practice appears to have been ratified and codified in the 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. Proposal for a Council Framework Decision, art. 31, COM (2005) 475 final (Oct. 4, 2005).
[23] Regulation No. 45/2001, 2001 O.J. (L 8) 1 (on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data).
[24] See Regulation No. 45/2001, art. 46.

requested an opinion from the Data Protection Supervisor. Therefore, two sets of opinions informed the debate on the Data Retention 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 other institutions judged the privacy guarantees in the final version satisfactory.

The best place to begin the data privacy analysis—and where European policymakers began *their* privacy analysis—is the European Convention on Human Rights (ECHR). 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.[25] The ECHR protects the right to private life under Article 8. In addition, a set of guarantees specific to data privacy are contained in Council of Europe Convention 108.[26] Again, although the European Union is not a party to the Convention, all of the Member States *are*. Moreover, the Convention served as the main point of reference for the European Data Protection Directive.

These many legal standards are complex and allow for significant variation in national data protection regimes. However, for purposes of this analysis, 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.[27] 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.[28] Second, the purpose of the interference must be legitimate. Namely, it must be related to one of the categories recognized under Article 8:

---

[25] Treaty on European Union, art. 6(2).
[26] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaties No. 108 (Jan. 1, 1981).
[27] See Opinion of the European Data Protection Supervisor, pp. 2-3, para. 9.
[28] See, e.g., Judgment of the ECHR of Feb. 16, 2000, Amann v. Switzerland, Application no. 27798/95, para. 50.

> [There shall be no interference with the right except as] is necessary in a democratic society 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.

Third, the interference with private life must be proportional.

The proportionality test has many different formulations, depending on the court and the commentator.[29] Even on the same court, on the same panel, the test can be articulated differently.[30] At the very least, however, it includes the following determinations: Is there evidence that the 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 but burden the right less?[31] As to this latter inquiry, a successful government defense often entails a showing that efforts were made not to restrict the right—that the government rejected more restrictive options—and that safeguards were put into place to protect the right. The burden of justification on the government under the proportionality test 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; the more important the public purpose, the lower the burden on the government.[32]

When the privacy right at stake is data protection, the proportionality investigation is guided by some of the more specific guarantees of Convention 108.[33] 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.[34] Such data must be "accurate and, where

---

[29] See, e.g., Catherine Barnard, The Substantive Law of the EU 243-44, 79-82 (2004); Paul Craig & Gráinne de Búrca, EU Law 372 (3d ed. 2003).

[30] For instance, the majority and the dissent employed different versions of the proportionality test in Judgment of the ECHR of Nov. 10, 2005, *Leyla Sahin v. Turkey*, Application No. 44774/98. Compare paras. 71-72 (majority) with Dissenting Opinion of Judge Tulkens, para. A1.

[31] 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.

[32] See Opinion of the Advocate General, Cases C-317/04 and C-318/04, European Parliament v. Council and European Parliament v. Commission, paras. 228-30.

[33] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaties No. 108 (Jan. 1, 1981).

[34] Convention 108, art. 5.c.

necessary, kept up to date"—otherwise, how would such data be able to accomplish the government's purpose? The *amount* of the data processed should be no more than necessary to accomplish this purpose;[35] nor should the *time* during which the data are stored be any longer than necessary.[36] 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.[37] Finally, as a special safeguard for the burdened 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 too, their personal data is being processed in accordance with the law.

These steps in the rights analysis were debated by the many institutional players involved in drafting the Data Retention Directive. The entire initiative turned on the need to provide a basis, in law, for personal data processing by private telecommunications providers and law enforcement officers. Without this, all involved—communications providers, national police, Member States, and the European Union—would be in flagrant breach of their legal duties. Under basic principles of European data protection, private actors may process an individual's personal data only if that individual consents, if such processing is necessary to performing a contract, or if one of a number of other conditions is satisfied. One of those conditions is the legal duty to process personal data. The Data Retention Directive was to impose such a legal duty on communications providers. In doing so, it would replace divergent national laws requiring communications providers to retain data for law enforcement purposes.[38] On this, all of the institutional actors—Council, Commission, Parliament, Working Party, Data Protection Supervisor—agreed.

They strongly disagreed, however, on whether the 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

[35] Convention 108, art. 5.c.
[36] Convention 108, art. 5.e.
[37] Convention 108, art. 7.
[38] 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.

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. Unsurprisingly, the Working Party, the Data Protection Supervisor, and the European Parliament took the opposite position.[39] Why unsurprisingly? Because their institutional clout on the question of police access depended on it. If the issue were to be regulated nationally, or in the Third Pillar, the power of these supranational institutions would be minimal. Ultimately, a provision on police access was included.[40] The substance of this provision, however, is barebones compared to what the Parliament, following the lead of the two advisory bodies, had requested.

Not only were the institutional players divided on the question of who should regulate the police, but they also disagreed on who should, in the future, bring the Directive into line with changing technological and social realities. In the Commission proposal, revisions to the types of traffic data to be retained were to made through an administrative process: a regulatory comitology committee, which, in practice, means close supervision of the Commission's rulemaking by the Council.[41] The data protection bodies and the Parliament objected. They wanted the full-blown legislative procedure of co-decision for an issue with such far-reaching implications for fundamental rights. In their view, Europe's only directly elected legislative body—the European Parliament—should be entitled to decide.[42] Ultimately, the Parliament's position prevailed.

Observe that the disagreement between the Council and the Commission, on the one hand, and the data protection advocates, on the other, was driven not by the need to meet fundamental rights standards. Under Article 8 of the ECHR, any law, national or

[39] Working Party, Opinion /2005 of Oct. 21, 2005, p. 8; European Data Protection Supervisor, Opinion, p. 3, 10-11. The Parliament, in agreement with these two data protection advisory bodies, proposed a series of amendments giving effect to their recommendations. See Parliament Resolution, P6_TA (2005) 0512, Dec. 14, 2005 (approving amended version of the Data Retention Directive); Committee on Civil Liberties, Justice and Home Affairs, Report, A6-0365/2005, Nov. 28, 2005, p. 14, pp. 15-16, pp. 33-34 (report with amendments of the proposal for the Data Retention Directive) (hereinafter "Parliament Report").
[40] Directive, art. 4.
[41] See Commission proposal, arts. 5 and 6.
[42] European Data Protection Supervisor, Opinion, p. 11, para. 60; Working Party, Opinion /2005 of Oct. 21, 2005, p. 9; Parliament Report, p. 34.

EU, is satisfactory as long as it is precise and accessible to the public.[43] Rather, the debate was over the nature of EU democracy. Should national ministries of the interior, sitting on the Council, decide alone on the privacy safeguards to be respected by the police? Does the unanimity requirement, which gives each state a veto right, together with the power of national parliaments to supervise their executives, ensure that the decisions of the Council will respect the will of European electorates? Or should the Council, *together* with the European Parliament, decide? For the directly elected European Parliament is a democratic body that might be expected to improve the deliberative, rights-abiding quality of the law. Yet, at the same time, one might argue that the European Parliament is more removed from the European peoples than the national governments that sit on the Council and the national parliaments that hold their governments in check.

The institutions also debated the second step of the rights analysis: legitimate purpose. To satisfy fundamental rights standards, the retention requirement had to advance a legitimate purpose. At the beginning of the legislative debate, the purposes of data retention were quite broad. In the Council's draft, the data was to be used to fight all crimes—and not only to investigate and prosecute past crime, but to prevent future crimes.[44] In the Commission's proposal, the crimes were paired down to "serious criminal offences, such as terrorism and organised crime."[45] In the final version, the purpose was further narrowed: prevention of crime was stricken from the text. Thus, as 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.[46]

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

[43] 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 & Lorna Woods, German Constitutional Law: The protection of civil liberties 80-81 (1999).
[44] Draft Framework Decision, art. 1.
[45] Commission Proposal, art. 1.
[46] Directive, art. 1.1.

were extremely critical of the nearly unfettered rights of access that such broad purposes would confer upon police authorities.[47]

Notice, however, that the debate did not focus on the legitimacy of the government purpose. Under Article 8 of the ECHR, any kind of fighting of 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 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 could be justified only by the need to catch the perpetrators of serious crimes and the perpetrators of crimes that were certain, not speculative.

Indeed, proportionality—the third step in the rights analysis—proved to be the thorniest issue of all. Neither the Working Party nor the Data Protection Supervisor believed that lawmakers had demonstrated with enough certainty that communications data over six months old would be useful in investigating crimes.[48] In other words, they did not believe that the legislature had shown 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 UK on police requests for communications data.[49] According to the report, traffic data older than six months was often useful in investigating serious crimes. Both data protection bodies dismissed this evidence as inadequate. European legislators, however, were persuaded otherwise, as demonstrated by the enactment of the 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. The original Council proposal would have required data retention for a period of one to three years.[50] In other words, in their implementing legislation, Member States could have chosen anything

[47] Working Party, Opinion /2005 of Oct. 21, 2005, p. 8; Parliament Report, p. 33.
[48] Note from Council Presidency to COREPER/JHA Council on Data retention, Doc. No. 15220/05, at 2 (Dec. 1, 2005) (on limiting purpose to fighting serious crime); European Data Protection Supervisor, Opinion, pp. 4-5 (on eliminating crime prevention); Working Party, Opinion /2005 of Oct. 21, 2005, p. 6 (on eliminating crime prevention).
[49] European Data Protection Supervisor, Opinion, p. 4.
[50] See draft Framework Decision, art. 4.

from a one to a three-year data retention period. This period, in the eyes of the critics, was excessive in light of the measure's burden on the privacy right—it was disproportionate. Responding to this criticism, the Commission reduced the data retention period considerably: the proposed directive would have required call data to be retained for one year, email and voice-over internet protocol data to be retained for six months.[51] After negotiations in the Council, however, the retention period in the final version was lengthened to 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 European Parliament, the difference was split exactly in two: one year shorter than the Council's initial position, one year longer than the European 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.[52] 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, for mobile equipment such as cell phones and hand-held email devices, (6) data necessary to identify the location of the equipment for the duration of the communication.[53]

Later, however, two points of contention over data content emerged. Should a call that was made, but not answered, be considered a "communication" and therefore be retained? Should location data on mobile equipment such as cellphones be collected for the entire call, enabling the police not only to monitor calls, but also to track the

[51] Commission proposal, art. 7. The Commission's position was largely satisfactory to the data protection bodies and the European Parliament. See European Data Protection Supervisor, Opinion, p. 12; Working Party, Opinion /2005 of Oct. 21, 2005, pp. 6-7; Parliament Report, pp. 22, 35.
[52] See draft Framework Decision, art. 1.2.
[53] See draft Framework Decision, art. 2; Commission proposal, Annex.

movements of their citizens? The Working Party recommended retention only for successful calls and only for the location of mobile devices at the beginning of the call.[54] The European Parliament in essence followed the Working Party's recommendation.[55] The Council and the Commission, however, successfully resisted this recommendation. In the final version of the Directive, data on unsuccessful calls and on the location of mobile equipment throughout the call must be retained.[56]

As was explained earlier, the proportionality inquiry can turn on the existence of an equally feasible, equally effective government measure with a lower burden on the privacy right. According to the data protection advocates, 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."[57] When the police have a suspect in mind, yet still do not have any evidence that would satisfy the standard for obtaining a court warrant, they can ask communications providers to store that person's communications data. Then, once the police do have the evidence necessary for a court warrant, they can access the data. This alternative, however, did not surface in any other parts of the legislative history; it does not appear to have been taken seriously by the other institutional players.

With this understanding of the legislative debates underpinning the Directive, the question posed earlier can now be addressed: Is privacy adequately protected in the Data Retention Directive? Basically, 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.

With the 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 law, albeit law that is 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

[54] Working Party, Opinion /2005 of Oct. 21, 2005, p. 10.
[55] Parliament Report, p. 35.
[56] See Directive, art. 3.2 (retention of unsuccessful call attempts), art. 5 (f)(2) (location data).
[57] European Data Protection Supervisor, Opinion, p. 5; Working Party, Opinion /2005 of Oct. 21, 2005, p. 6.

cooperation on criminal matters. 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.

The decision to go forward under the First Pillar was salutary. Giving the European Parliament co-decision powers meant that the Council's 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. The Council's burden of justification for this gargantuan data-gathering initiative was more substantial once the matter had to be decided by the Parliament, too. 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: Do we really need this privacy-invading communications data to fight *all* crime—aren't normal law enforcement methods good enough for ordinary crimes like theft? Is communications data over two years old really going to help with criminal investigations—wouldn't we expect those plotting a terrorist attack to have communicated 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, in the Third Pillar, the voting rule is unanimity, meaning that each government—under the scrutiny of a national parliament—can veto any measure and therefore, theoretically, 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 that, after the issue has been decided, the intergovernmental bargains can be unravelled 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 of national data protection authorities and the European 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 propose 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 European Parliament's amendments. Few parliamentarians can be expected to have experience with data protection; to protect privacy rights, the Parliament naturally looked for guidance to these two independent, European-level, data protection watchdogs.

The data retention scheme also satisfied the demands of proportionality. A maximum retention period of two years is 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 crime 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 policy alternative—the quick-freeze procedure—would not be as effective as data retention in combating crime. 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. In criminal investigations, how valuable is information on calls made, but not answered, by a suspected criminal to another party? It is difficult for the layperson to know. Perhaps,

since, logically speaking, only calls involving at least two parties can count as evidence of a conspiracy, only those 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; or, thanks to caller identification, even a call that goes unanswered is capable of communicating information to a co-conspirator. The latter set of arguments are not foolproof, but they are at least plausible.

The Directive's provisions on record-keeping contribute to the proportionality of data retention. Under the Directive, the Member States must provide yearly figures on the number of times that data was given to the police by communications providers, the age of that data, and the number of police requests that could not be satisfied.[58] 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 the data by the type of data requested by the police. 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, or that information on unconnected calls is useless, then it would be appropriate to consider the data retention program disproportionate and to amend the Directive.

Critical to this assessment of the 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; they are specifically directed to erase the data after the retention period.[59] Most importantly, national police

[58] Directive, art. 10.
[59] Directive, art. 7.

are allowed to access the data only "in specific cases."[60] 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, even if done by the police for imperative security reasons, as opposed to 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 then 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.[61] A new measure guaranteeing data protection in the work of intelligence agencies—not covered by the Third Pillar legislation—would also be welcome.

III. 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.[62] 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

[60] Directive, art. 4.
[61] See Note from Presidency of the Council to the Multidisciplinary Group on Organised Crime on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, Council doc. 6450/1/06, March 23, 2006. As the proposal currently stands, the police would have to provide a "factual indication" that personal data will help investigate or prevent a crime but would not have to go before an independent government officer. Art. 5.2.
[62] For a comprehensive list of such initiatives as of March 23, 2004, see Statewatch, "Scoreboard on post-Madrid counter-terrorism plans," available at http://www.statewatch.org.

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-Europe communications providers and that harmonization of such regulations was necessary. But a provision on the conditions on national *police* access to the retained data, even as minimal a provision as was included in the Directive, was highly questionable. 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, those matters are governed by the Third Pillar (and the Second Pillar for national security). Yet precisely because this is the area in which the state bites hardest, it is the domain in which classic, liberal rights are most important. 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 decisionmaking 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.[63] The data retention experience, however, suggests a more modest reform that would render debates on criminal cooperation more public and that would encourage

[63] 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.

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 European Union's emerging criminal justice system. Such a government body would bring a wealth of national experience to bear on Europe-wide cooperation. Through its organization—it would probably take the form of a network of national ombudsmen and human rights advocates—it would render the Council's Third Pillar 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 would be able to use the watchdog's opinions as a point of departure in exercising its power of consultation.

This suggestion is not novel. The EU Committee of the UK House of Lords has made a similar recommendation. Recently, the Committee released a report criticizing the European Commission's proposal for an EU Fundamental Rights Agency.[64] The House of Lords Committee concluded that the proposed agency's powers were too limited. Under the current scheme, the agency would collect information on the state of human rights at the national level and, based on that information, would make recommendations for improving national implementation of EU law. According to the House of Lords Committee, the agency's mandate should be broadened: the human rights agency should also be tasked with reviewing proposed EU laws. The Committee's conclusion is bolstered by the experience of the Data Retention Directive. The protection of the right to privacy in that legislation demonstrates that human rights scrutiny can be extremely valuable and that it can work in the Third Pillar when basic rights come under pressure from the police, prosecutors, and the courts.

[64] See House of Lords, Select Committee on European Union, Human Rights Protection in Europe: The Fundamental Rights Agency, para. 73 (April 4, 2006).