A Failure to Regulate: Data Protection and Ethnic Profiling in the Police Sector in Europe

Police in Europe can typically locate personal data on individuals, including their ethnicity, from countless sources, even though similar information on policing techniques is hard to get, writes **Ben Hayes**.[†]

The collection of data is relevant to ethnic profiling by police for two reasons. First, data is required to discover whether police are, in fact, engaging in profiling on the basis of race or ethnicity. Data on the ethnicity of individuals stopped by police is critical for monitoring police performance and ensuring it is nondiscriminatory. According to EU law, this kind of information can be lawfully collected with the consent of the individual, and used to generate statistical information as long as it is anonymized. Second, criminal or terrorist profiles can be generated by police on the basis of personal data gathered in numerous other contexts, including immigration points and places of employment and education—and these may include an ethnic component unless expressly prohibited. However, European law has consistently failed to improve on a non-binding Council of Europe Recommendation of 1987 on the collection, storing, and processing of personal data in the police sector, including "sensitive" data relating to race and ethnicity.

The two issues are connected: regulation defining the kinds of data police can collect, conditions on its collection, and limits on its use must be clarified and codified. The UK has taken first steps by requiring police to monitor their stops and searches in order to discover whether profiling or discrimination is taking place. Yet regulation of police collection and use of personal data is more pressing than ever today, given the recent revival of ethnic profiling in the context of antiterrorist action in both the UK and the rest of Europe. Much can be learned from looking at the legislative history in Europe, the practical experience in the UK, and the increasing demands for personal data in the context of the "war on terrorism."

European legislation I: Council of Europe data protection measures

International data protection law in Europe is derived from the 1981 Council of Europe (COE) Convention on the "Protection of Individuals with regard to Automatic Processing of Personal Data,"[1] itself the result of a COE parliamentary assembly resolution of 1968.[2] The principles embodied in the Convention are that the collection of personal data, and access to it, must be restricted. Data should only be used for the purpose

for which it was collected, and retained only as long as strictly necessary. Individuals should be able to find out what data is held on them and have recourse to mechanisms to challenge its use, accuracy, or retention. The convention matters, as most EU member states do not have a constitutional right to privacy and the European Court of Human Rights has so far been unable to give meaningful effect to this right as guaranteed in Article 8 of the European Convention on Human Rights (ECHR).[3]

The convention singles out "special categories of data" for particular attention. Thus, "[p]ersonal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards."[4] However, states can ignore these safeguards "in the interests of … protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences."[5] The police, in other words, were effectively exempt. To counteract this outcome, the COE drew up a recommendation in 1987 "regulating the use of personal data in the police sector."[6] This document advised that data held by the police be supervised independently, suggests limits on its collection, storage and use, and recommends restrictions on the exchange of information with other public bodies, as well as time limits, data security, and notification of the data subject. The recommendation included a stricter rule on the processing of "special categories of data," such as race or religion:

> The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular enquiry.[7]

The UK reserved the right to "comply or not" with the provision on "sensitive" data.

COE recommendations, however, are non-binding. While their adoption implies and encourages acceptance by all member states, reservations are common, explicitly so in this case. The UK, for instance, reserved the right to "comply or not" with the provisions on notification of data subjects and on "sensitive" data.[8]

Three evaluations of the recommendation have been undertaken to date, but none have looked in any detail at how—or even if—it has been implemented by states. The evaluations suggested unsuccessfully, in 1994, the adoption of a new and binding convention, expressed concerns in 1998 about data mining[9] and police access to genetic data, and ultimately, in 2002, recommended that no further evaluations be undertaken.[10]

In sum, then, COE legislative efforts to protect personal data amount to a 1981 Convention from which police forces effectively can—and frequently do—exempt themselves, and a

police-specific 1987 Recommendation with which states may "comply or not."

European Legislation II: EU data protection measures

By the late 1980s, data protection advocates were concerned that the 1981 COE Convention was not implemented to a sufficient or uniform degree. To address this, the European Commission proposed binding EU legislation on data protection in 1990.

The latest figures show that black people in the UK are still six times more likely to be stopped and searched than whites, and Asians twice as likely.

Over the next five years, the COE Convention was harmonized to eliminate variation between member states' national laws, and transposed into the EC Data Protection Directive.[11]

The new directive did not regulate Europe's police. It not only incorporated the "state security" exemption from the COE convention, but actually broadened it to include all "processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."[12] Lest there be any doubt, the directive clarifies that it does not apply to activities "which fall outside the scope of Community law," such as in the areas of foreign and security policy, and justice and home affairs — precisely where policing policy sits.

Furthermore, the directive makes no reference to the 1987 COE recommendation on data protection in the police sector. This was to be addressed instead in a council resolution under the EU's "Third Pillar" (policing, criminal law, and immigration). Despite lengthy negotiations, the final draft, agreed in 2001, was never adopted, apparently due to some states' disagreement with its effective dilution.[13] Several months later, in June 2001, the relevant working party was disbanded as part of a "streamlining" exercise.[14] Although no explanation was offered, the impasse demonstrates significant resistance from member states to the introduction of meaningful rules governing the protection of personal data in policing and security work.

The right to data protection, as subsequently included in the EU Charter of Fundamental Rights of 2000 (and hence in the draft EU Constitution), offers a broader exemption for state agencies from data protection than that found in either the COE convention or the EC Data Protection Directive. However, at a minimum, the rights of individual access to data and the rectification of errors are entrenched.[15]

States may similarly restrict the right to privacy accorded by the ECHR where:

> 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.[16]

In 2002, the EU set an alarming precedent when updating and amending an earlier (and separate) directive on data protection in telecommunications.[17] The update removed the crucial obligation on service providers to erase communications traffic data immediately after it has been used for billing purposes. This reflected longstanding demands from law enforcement for the introduction of "data retention" regimes—whereby all internet and telecommunications traffic data is to be stored for 12-24 months and made accessible to law enforcement agencies.[18] A majority of EU member states have now introduced such regimes—despite the unanimous view of European data protection commissioners,[19] privacy advocates, and respected legal opinion that the regimes are unlawful and disproportionate to the need "in a democratic society," as required by the ECHR.[20] In 2004, the European Council went further still, proposing mandatory data retention across the EU.[21] Though that draft Framework Decision was finally withdrawn, the issue remains on the table and the European Commission has indicated that it will issue fresh proposals later in 2005.[22]

Nevertheless, despite this assault on privacy and data protection, the EU remains at least ostensibly committed to the introduction of binding data protection standards in the police sector.[23]

The United Kingdom: ethnic profiling, data protection and police accountability

The UK has introduced data regulation in the police sector to keep track of the impact of police stop and search operations on ethnic minorities. The collection of stop and search statistics is permissible within both the generable exemptions of the EC Data Protection Directive applicable to police and a specific exemption for national census data and other "scientific research."[24] Moreover, the directive does not prohibit the processing of data rendered anonymous "in such a way that the data subject is no longer identifiable."[25] It is unfortunate, then, that at least two EU governments, Spain and Germany, have apparently claimed in the past that they are unable to put in place an ethnic monitoring mechanism for stop and search because they are prohibited by data protection rules.[26]

To begin, some background on stop and search in the UK. *Statewatch* published critical analyses of the Home Office stop and search statistics in 1998, and again in 1999, finding that black people in England and Wales were almost eight times more likely to be stopped and searched than whites.[27] Where the Home Office had simply produced a total number of stops for each ethnic group within the most of the country's 43 police districts, *Statewatch* researchers cross-referenced this data with that on ethnicity and population provided by the national census.

The use of stop and search powers by police was the issue raised most often by black and Asian communities during the 1999 "Macpherson inquiry" into the police handling of the racist murder of Stephen Lawrence, and the "institutional racism" identified by the report in the police force. The Macpherson report recommended that:

> the Home Secretary, in consultation with Police Services, should ensure that a record is made by police officers of all 'stops' and 'stops and searches' made under any legislative provision (not just the Police and Criminal Evidence Act). Non-statutory or so-called 'voluntary' stops must also be recorded. The record [should] include the reason for the stop, the outcome, and the self-defined ethnic identity of the person stopped. A copy of the record shall be given to the person stopped.[28]

One response of the German authorities to September 11 was to instruct police units to collect data on young men with Islamic backgrounds.

Although this recommendation has led to increased police accountability and sparked ongoing public debate, it has not resulted in significant reductions in the numbers of stops and searches conducted or their disproportionate impact on non-whites. The latest Home Office figures on stop and search, for 2003-4, showed that black people are still six times more likely to be stopped and searched than whites, and Asians twice as likely. Under the 2000 Terrorism Act, which gives police the power to stop and search persons and vehicles without *any* suspicion in an "authorized" area, stops and searches have increased steadily since "9/11", by 150 percent in total in 2002/3—with those affecting Asians up 285 percent and black persons up 229 percent.[29] The total number of stops and searches under the Terrorism Act went up by a further 36 percent in 2003/4. Taking all the stop and search powers into account, those conducted on white people have increased by less than 4 percent compared with 66 percent for blacks and 75 percent for Asians.[30]

These increases have produced attempts to justify the disparities, which in turn have often simply exacerbated the climate of distrust between police and communities.[31] In March 2005, Home Office Minister Hazel Blears made the extraordinary statement that antiterrorism legislation would inevitably be "disproportionately experienced by" the Muslim community since that is the nature of the terrorist threat.[32] No minister before has publicly admitted that certain laws will be used in a discriminatory manner contrary to the Race Relations Act and the other equality legislation in force in the UK.

Antiterrorism: Ethnic profiling as EU police policy

Developments in law enforcement policy and practices since September 11, 2001, demonstrate afresh the

importance of data protection (or its lack) in the police sector, and raise serious concerns about increased ethnic profiling in the exercise of police powers. The "war on terror" coincides with rapidly developing law enforcement technology. Europe's national data protection commissioners have expressed alarm about the "processing of personal data from different sources on an unprecedented scale."[33] Much of this data specifically identifies and marks individuals as Muslims.

For instance, it has emerged that one response of the German authorities to September 11 was to instruct police units to collect data on young men with Islamic backgrounds from universities, registration offices, health insurance companies, Germany's "Central Foreigners Register," and other sources.[34] It is not known how many other states are creating similar databases.

In 2002, the EU's Working Party on Terrorism drew up recommendations for member states on the use of "terrorist profiling," using "a set of physical, psychological, or behavioural variables, which have been identified as typical of persons involved in terrorist activities and which may have some predictive value in that respect."[35] The UK and Germany are among a number of countries participating in an expert group on "terrorist profiling," with Europol, the European police office, participating.[36] Member states are also running a program on "radicalism and recruitment" within the EU framework, targeting Muslim communities' places of education and worship.[37]

The EU Network of Independent Experts in Fundamental Rights, an association of experts in international law set up by the European Commission to review recent developments, has serious concerns about the development of terrorist profiles by police or immigration authorities. Profiling on the basis of characteristics such as psycho-sociological features, nationality, or birthplace, they say, "presents a major risk of discrimination."[38] To be acceptable, a statistical link would have to be demonstrated between these defined characteristics and the risk of terrorism, which has not yet been done.

Europol, even before September 11, worked on the "express assumption that organized crime groups are ethnically based."

Europol, according to one scholar, even before September 11, worked on the "express assumption that organized crime groups are ethnically based,"[39] a controversial modus operandi, and one that is, theoretically at least, incompatible with data protection principles. Europol was further empowered by the European Council to collect precisely the sort of "sensitive information" (on ethnicity, religion, political beliefs, and activities) prohibited by the COE.[40]

Ethnically marked data is increasingly the subject of exchange between

law enforcement agencies both within EU countries and with non-EU countries. International agreements on the exchange of personal data regarding air travelers (passenger-name-record ["PNR"] data), have been signed within the EU and with the United States.[41] The justification is that law enforcement agencies need this data to enable screening of passengers against terrorist watchlists, and to create profiles on individual visa entrants (lifetime profiles, in the case of the United States). Data pertaining to nationality, ethnicity, and religion will clearly have a central role to play in this process, and may even subject innocent travelers to arbitrary stops, interrogations, and travel restrictions due to information added to a profile by a state agent.

European data protection commissioners say profiles compiled by the U.S. authorities could be shared by up to 1,500 law enforcement agencies.

Another logical concern is that the exchange of this data will lead in future to the *de facto* mutual recognition of arbitrary decisions, such as refusals of visas or admission at borders, placement of individuals on watchlists, or inclusion in databases, depriving people of their rights and offering no opportunity for redress.

The EU has entered into three treaties with the United States involving the exchange of law enforcement data (regarding Europol, PNR, and mutual legal assistance).[42] Although EU data protection law requires an equivalent level of protection from any state receiving data from the EU, U.S. privacy law only covers U.S. citizens, with no meaningful rules applying to data held on foreigners. European data protection commissioners say the profiles compiled by the U.S. authorities could be shared by up to 1,500 law enforcement agencies. The European Parliament three times voted to reject the EU-U.S. treaty on the exchange of passenger data and, having been ignored by the Commission, is now seeking the treaty's annulment at the European Court of Justice.[43]

Biometric data (fingerprints and facial scans) will also be included in these individual profiles. Encouraged by the United States to fingerprint all entrants, the EU has gone one step further, agreeing not only that all passport-holders, residence permit-holders and visa applicants will be fingerprinted, but also, in principle, that this and other personal data will be held in electronic chips in travel documents and in an EU-wide database to which there will be broad law enforcement access.[44] The clamor for "biometrics" is also driving plans for new national ID card systems in, for example, Britain.

Population registers, foreigner registers, ID cards, terrorist profiling, "watchlists": these are all issues that appear strongly to promote, rather than restrict, ethnic profiling by police. They should also be seen in the context of restrictive immigration and expulsion policies, and the accompanying resources deployed to enforce these policies.

Where now for data protection in the police sector?

Three main problems inhibit data protection in the police sector. First is the absence of binding international standards. Second is the processing of personal data from different sources on an unprecedented scale. Third is the unregulated exchange of police data around the world. If and when the EU does introduce rules on data protection in the police sector, they are likely, in the current context of law enforcement "globalization," to meet a very low standard.

Recent developments give further cause for concern. In October 2004, the EU agreed on a new "principle of availability."[45] Under this principle, all law enforcement agencies in the EU should have access to all data held by all other law enforcement agencies, for the broad purpose of "cooperation to prevent, detect, investigate and prosecute crime and threats to security." The EU has committed itself to this ambitious project, which is already well underway, for the next five years.

During the 1980s, when the Council of Europe was first writing up international data protection law, it was accepted that the police, for the purpose of preventing or investigating crime, need access to personal data—but that the processing of this data could not be unlimited and should be regulated by law. Moreover, it was understood that the processing of "sensitive" data should be the exception rather than the norm. Under the "war on terror" that has so far defined the twenty-first century, we can no longer be sure that these basic principles still hold true.

In December 2004, the new European Commissioner for Justice and Home Affairs, Franco Frattini, discussed "new balances … between privacy and security." A new framework, he suggested, was necessary to "take account of the times we are living in" and address "some of the supposed obstacles thrown up by the notion of privacy."[46] The "principle of availability" and the "notion of privacy": the future looks grim for data protection in the police sector in Europe.

Notes

† Ben Hayes is a researcher with *Statewatch*, UK.

1. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention no 108 (January 28, 1981), available at: http://conventions.coe.intreaty/ENreaties/Html/108.htm.

2. See Recommendations and Resolutions on Data Protection of the COE Committee of Ministers.

3. European Convention on Human Rights and Fundamental Freedoms, 213 E.T.S.222, entered into force September 3, 1953 [ECHR], art. 8: "Everyone has the right to respect for his private and family life, his home and his correspondence."

4. COE 1981 Convention, Chapter II, art. 6.

5. COE 1981 Convention, art. 9(2).

6. COE Recommendation R (87) 15 of the Committee of Ministers to Member States, Regulating the Use of Personal Data in the Police Sector (1987), available at: http://cm.coe.inta/rec/1987/87r15.htm. See also Explanatory Report, available at: http://cm.coe.inta/rec/1987/ExpRec(87)15.htm.

7. COE Recommendation R (87) 15, art. 2(4).

8. Michael Spencer, *States of Injustice,* London: Pluto, (1995) 166.

9. Data mining was also addressed in part in a non-binding 1995 COE Recommendation on the "Problems of Criminal Procedure Law Connected with Information Technology," which covers search and seizure of computer data, technical surveillance, legal obligations of service providers vis-à-vis investigating authorities, electronic evidence, encryption, research into computer crime and international cooperation. See COE Recommendation R (95) 13, Concerning Problems of Criminal Procedure Law Connected with Information Technology, available at: http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html.

10. See 1994, 1998 and 2002 COE Evaluation reports on Recommendation R (87) 15, available at: http://www.coe.int/E/Legal_affairs/Legal_cooperation/Data_protection/Documents/Reports/default.asp#TopOfPage.

11. Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (October 24, 1995) ["EC Data Protection Directive"].

12. Directive 1995/46/EC, art. 3(2).

13. See EU Council doc. 6316/2/01 REV 2, "Draft Resolution on the personal data protection rules in instruments under the third pillar of the European Union" (April 12, 2001), available at: http://register.consilium.eu.int/pdf/en/01/st06/06316-r2en1.pdf.

14. This working party should not be confused with the EC working party on data protection (the "Article 29" Committee) established under the 1995 Directive and consulted by the EU on "First Pillar" issues (economic and social policy).

15. Although the Charter is not yet in force, it has been cited in some judgments of the European Court of Justice. Article 8 of the Charter reads "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified...." See EU Charter of Fundamental Rights, available at: http://www.europarl.eu.int/charter/pdfext_en.pdf.

16. ECHR, art. 8(2).

17. Directive 1997/66/EC "concerning the processing of personal data and the protection of privacy in the telecommunications sector" (December 15, 1997), available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf.

18. Directive 2002/58/EC "concerning the processing of personal data and the protection of privacy in the electronic communications sector" (July 12, 2002), available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

19. All EU member states have Data Protection Commissioners to oversee the implementation of national laws. In addition, the Commissioners meet in a number of institutional fora, including a Joint Supervisory Body on data protection for Europol, Eurojust, the Schengen Information System, and the Customs Information System. On September 14, 2004, European Data Protection Commissioners met in Wroclaw, Poland and adopted a Resolution to set up a "joint EU forum on data protection in police and judicial cooperation matters (data protection in the third pillar)."

20. On the data retention regimes introduced by member states, see *Statewatch*, "Majority of Governments Introducing Data Retention of Communications" (undated), available at: http://www.statewatch.org/news/2003/jan/12eudatret.htm. For legal opinion on "data retention," see *Privacy International*, "Data Retention Violates Human Rights Convention" (October 10, 2003), available at: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-57875&als[theme]=Data%20Retention.

21. See "Draft Framework Decision on Data Retention," EU Council doc. 8958/04 (April 28, 2004). For full text and analysis of this proposal, see *Statewatch*, "Data Retention Comes to Roost—Telephone and Internet Privacy to be Abolished" (April 2004), available at: http://www.statewatch.org/news/2004/apr/21dataretention.htm.

22. The proposal was withdrawn in April 2005 after *Statewatch* published the opinions of the legal services of the European Commission and the EU Council. Both admit that the EU measure alone cannot lawfully introduce mandatory data retention and that an EC Directive (First Pillar) is required to give the policy an adequate legal basis, see *Statewatch*, "EU: Data Retention Proposal Partly Illegal, Say Council and Commission Lawyers" (undated), available at: http://www.statewatch.org/news/2005/apr/02eu-data-retention.htm.

23. Since the draft resolution on data protection in the police sector was abandoned in 2001, the European Commission has consistently said it will propose legislation, although none has yet been produced. The "Hague Programme" on cooperation in the field of Justice and Home Affairs to 2008 also commits the Commission to the introduction of data protection rules in the police sector.

24. Under Article 13(2) of the 1995 EC Data Protection Directive, "Subject to adequate legal safeguards... Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict [data protection] when data are processed solely for purposes of scientific research or ... for the sole purpose of creating statistics". In addition, there have been two Council of Europe Recommendations on data protection and personal data used for statistical purposes (CoE Recommendations R (83) 10, September 23, 1983, and R (97) 18, September 30, 1997).

25. Recital 26, Directive 95/64/EC.

26. Open Society Institute EU Accession Monitoring Program, *Seguimiento de la protección de las minorías en la Unión Europea: La situación de los roma/gitanos en España*, Budapest: OSI (2003) 47. See also Andrea Krizsan (ed.), *Ethnic Monitoring and Data Protection: The European Context*, Budapest: CPS Books (2001).

27. See "Stop and search and arrest and racism," *Statewatch bulletin*, vol 8, no 3/4 (May-August 1998) and "The Cycle of UK Racism—Stop and Search, Arrest and Imprisonment," *Statewatch bulletin*, vol 9, no 1 (January-February 1999).

28. Recommendation 61, "The Stephen Lawrence Inquiry: Report of an Inquiry by Sir William Macpherson Of Cluny" (February 1999), available at: http://www.archive.official-documents.co.uk/document/cm42/4262/4262.htm.

29. See "Ethnic Injustice: More Black and Asian People Are Being Stopped and Searched Than Ever Before," *Statewatch news online* (August 2004), available at: http://www.statewatch.org/news/2004/aug/stop-and-search.pdf.

30. In 2003-4, the total number of stop and searches increased by 16 percent to 807,616—the highest recorded total to date. The vast majority are conducted under the Police and Criminal Evidence Act (PACE). In addition to the Terrorism Act 2000, the Criminal Justice and Public Order Act 1994 enables a police officer to authorize, for a period not exceeding 24 hours, stops and searches " in anticipation of violence." See "Stop & Search: Ethnic Injustice Continues Unabated", *Statewatch bulletin*, vol 15, no 1 (2005).

31. In the UK, continued discrimination against black and Asian communities has led to justifications of the disproportionality of stop and search practice for different ethnic groups. These have varied from arguably racist statements about the propensity to crime and terrorism of different ethnic groups to controversial research that has found, by studying the "available population" (people

on the street), that there is "no general pattern of bias against people from minority ethnic groups, either as a whole or for particular groups." See "Re-interpreting Stop and Search Statistics," *Statewatch bulletin*, vol 10, no 5 (September-October 2000). See also Joel Miller's article in the present issue of *Justice Initiatives*.

32. According to Minister Hazel Blears, "Dealing with the counter-terrorist threat and the fact that at the moment the threat is most likely to come from those people associated with an extreme form of Islam, or falsely hiding behind Islam ... inevitably means that some of our counter-terrorist powers will be disproportionately experienced by people in the Muslim community. That is the reality of the situation, we should acknowledge that reality and then try to have as open, as honest and as transparent a debate with the community as we counter the threat." *Home Affairs Select Committee, Uncorrected Minutes of Evidence*, 1 March, 2005, HC 156-v. See also *The Guardian* (March 2, 2005).

33. Cited in "Memorandum by the Europol, Eurojust, Schengen and Customs Joint Supervisory Authorities," *After Madrid: the EU's response to terrorism*, House of Lords' European Union Committee, 5th Report of Session 2004-05 (HL Paper 53), 148.

34. See "Police 'trawling' for suspect foreigners," *Statewatch bulletin*, vol 12, no 1 (Jan-Feb 2002).

35. See EU Council doc.: 11858/3/02 REV 3, "Draft Council Recommendation on the development of terrorist profiles" (December 18, 2002), available at: http://register.consilium.eu.int/pdf/en/02/st11/11858-r3en2.pdf. See also EU Council doc.: 7846/04, "'Terrorist Profiles' [reply to a written question by Sarah Ludford]" (March 30, 2004), available at: http://register.consilium.eu.int/pdf/en/04/st07/st07846.en04.pdf.

36. Europol is an EU-wide policing body set up by the member states in 1990 with the primary purpose of combating "organized crime," although its mandate is markedly broader in practice. EU member states are obliged to supply Europol with data relevant to its investigations and the agency is developing a sophisticated database and analysis system. Under recent EU legislation, Europol agents will be authorized to participate in "joint investigation teams" operating in the member states. See Europol website: http://www.europol.eu.int. See also Ben Hayes, *The Activities and Development of Europol: Towards an Unaccountable 'FBI' in Europe*, London: Statewatch (2002).

37. "Call for EU leaders to back scrutiny of mosques," *European Voice*, Vol. 10 No. 43 (December 9, 2004). See also "EU Action Plan on Combating Terrorism," Council doc. 10010/3/04 REV 3 (June 11, 2004).

38. E.U. Network of Independent Experts in Fundamental Rights, "The Balance Between Freedom and Security in the Response by the European Union and Its Member States to the Terrorist Threat" (2003), 38, available at: http://europa.eu.int/comm/justice_home/fsi/rights/networks/obs_thematiqu_en.pdf.

39. S. Peers, *EU Justice and Home Affairs Law*, London: Longman (2000), 216. The 19 operational projects ("Analysis Work Files") that Europol is working on include for example the "illegal immigration of Iraqi Kurds," "Illicit traffic in narcotic drugs by Turkish groups," "Islamic terrorism," and "Trafficking of Indian nationals." See *Statewatch news online* (April 2004), available at: http://www.statewatch.org/news/2004/apr/05europol-files.htm.

40. Council Act "adopting rules applicable to Europol analysis files" (November 3, 1998), available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/1999/c_026/c_026199901130en00010009.pdf.

41. Council Directive 2004/82/EC "on the obligation of carriers to communicate passenger data" (April 29, 2004), available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_261/l_26120040806en00240027.pdf; Council Decision "on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection" (May 17, 2004) available at: http://www.statewatch.org/news/2004/may/PNR-AGR.pdf. For analysis see *Statewatch Observatory* on the exchange of data on passengers: http://www.statewatch.org/pnrobservatory.htm.

42. On the Europol-United States Treaty (which has not been published), see: http://www.statewatch.org/news/2002/nov/analy15.pdf; on the EU-U.S. treaties on mutual legal assistance and extradition, see EU Council doc. 9513/03 (June 3, 2003), available at: http://www.statewatch.org/news/2003/jul/08euus.htm.

43. By an application notified to the Council on August 4, 2004, the European Parliament has brought an action under Article 230 of the EC Treaty before the Court of Justice, for the annulment of Council Decision (2004/496/EC) of May 17, 2004, on the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of PNR ("Passenger Name Record") data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection. At the same time, the European Parliament brought an action against the Commission, for the annulment of Commission Decision (2004/535/EC) of May 14, 2004, on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection.

44. Council Regulation (EC) No 2252/2004 "on standards for security features and biometrics in passports and travel documents issued by Member States" (December 13, 2004), available at: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf; "Proposal for a Council Regulation amending Regulation (EC) 1683/95 laying down a uniform format for visas" and "Proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals," *European Commission*, COM(2003)558 (September 24, 2003). On the agreement in principle that a central EU document register be created, and law enforcement granted access to that database, see *Statewatch*, "EU Declaration on combating terrorism," (March 25, 2004), available at: http://www.statewatch.org/news/2004/mar/eu-terr-decl.pdf.

45. See section 2.1 of the "Hague programme" on EU Justice and Home Affairs Cooperation to 2008, Council doc. 13302/2/04 REV 2, adopted by the Council of the EU on November 5, 2004. For full text and analysis, see: http://www.statewatch.org/news/2004/nov/hague-annotated-final.pdf.

46. Franco Frattini's address took place at a meeting of the EU joint supervisory authorities on data protection inBrussels, December 21, 2004.

47. See "EU: The 'principle of availability'...," *Statewatch bulletin*, vol 14, no 6 (November-December 2004).