UIC John Marshall Journal of Information Technology & Privacy Law

Volume 22
Issue 4 *Journal of Computer & Information Law - Summer 2004*

Article 4

Summer 2004

Retention of Communications Data: A Bumpy Road Ahead, 22 J. Marshall J. Computer & Info. L. 731 (2004)

Abu Bakar Munir

Siti Hajar Mohd Yasin

RETENTION OF COMMUNICATIONS DATA: A BUMPY ROAD AHEAD

ABU BAKAR MUNIR†
SITI HAJAR MOHD YASIN††

I. INTRODUCTION

The EU Electronic Privacy Directive 2002[1] requires Member States to ensure the confidentiality of communications. In particular, Member States shall prohibit listening, taping, storage or other kinds of interception or surveillance of communications.[2] The communications service providers are obligated to delete all traffic data no longer required for the provision of a communications service.[3] Yet, Member States are permitted to restrict the scope of this protection to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences.[4]

Despite strong criticism by privacy experts, data protection commissioners, civil liberties groups and the ISP industry, a provision on the retention of communications data was inserted. This new Directive reverses the position under the 1997 Telecommunications Privacy Directive by explicitly allowing the EU countries to compel Internet Service Providers and telecommunications companies to record, index and store their subscribers' communications data.[5] Under the terms of the new Directive, Member States may now pass laws mandating the retention of traffic and location data of all communications taking place over mobile phones, SMS, landline telephones, faxes, e-mails, chat rooms, the Internet, or any other electronic communication device.[6] Article 15 of the

† Associate Professor, Faculty of Law, University of Malaya, Malaysia.
†† Senior Lecturer, Law Faculty, University Technology MARA, Malaysia / Researcher, Law School, University of Strathclyde, United Kingdom.

1. *Directive on Privacy and Electronic Communications*, 2002/58/EC (July 12, 2002) (concerning the processing of personal data and the protection of privacy in the Electronic communication sector) (available in LEXIS at 2002 OJ L 201).
2. *Id.* at art. 5.
3. *Id.* at art. 6.
4. *Id.* at art. 15(1).
5. Directive 97/66/EC (repealed).
6. *Supra* n. 4.

Directive provides that Member States may adopt legislative measures when such restrictions constitute a necessary, appropriate and proportionate measure within a democratic society.[7] Specifically, Member States may adopt legislative measures providing for the retention of data for a limited period.[8]

The EU countries were given until October 31, 2003 to implement the Directive. Thus, it is topical and interesting to make an assessment on the implementation of one of the most controversial and much debated subjects of the Directive - the retention of communications data. In doing so, perhaps it is logical to focus on the position in the UK, being the only country that has a comprehensive legislation on this matter, so far. This paper traces the origin of the new Directive. It lays down the UK's legal frameworks concerning retention of communications data. Criticism on the data retention and UK's legal regime is given considerable attention. In closing, the paper examines the need to strike the right balance between fighting crime and terrorism and protecting the fundamental rights of the individual.

II. THE EMERGENCE OF THE ELECTRONIC PRIVACY DIRECTIVE

In 1997, the European Union supplemented its 1995 Data Protection Directive by introducing the Telecommunications Privacy Directive. This Directive established specific protections covering telephone, digital television, mobile networks and other telecommunications systems. It imposed wide-ranging obligations on carriers and service providers to ensure the privacy of users' communications, including Internet-related activities.[9] It covered areas that, until then, had fallen between the cracks of data protection laws. Access to billing data was severely restricted, as was marketing activity. Caller ID technology was required to incorporate an option for per-line blocking of number transmission. Information collected in the delivery of a communication was required to be purged once the call was completed.[10]

In July 2000, the European Commission issued a proposal for a new directive on privacy in the electronic communications sector. The proposal was introduced as a part of a larger package of the telecommunications directives aimed at strengthening competition within the European electronic communications markets. As originally proposed, the new directive would have strengthened privacy rights for individuals by ex-

7. *Id.*

8. *Id.*

9. Electronic Privacy Information Center, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* 11 (EPIC: US 2002).

10. *Id.*

tending the protections that were already in place for telecommunications to a broader, more technology-neutral category of 'electronic communications.'[11] During the process, however, the Council of Ministers began to push for the inclusion of data retention provisions, requiring the Internet Service Providers and telecommunications operators to store logs of all telephone calls, e-mails, faxes and Internet activity for law enforcement purposes. These proposals were strongly opposed by most members of the Parliament. In July 2001, the European Parliament's Civil Liberties Committee approved the draft directive without data retention, stating:

> The Civil Liberties Committee ('LIBE Committee') expressed itself in favor of a strict regulation of law enforcement authorities' access to personal data of citizens, such as communication traffic and location data. This decision is fundamental because in this way the EP blocks European Union States' efforts underway in the Council to put their citizens under generalized and pervasive surveillance, following the Echelon model.[12]

The events of September 11, however, have changed the political climate. The Parliament came under increasing pressure from the Member States to adopt the Council's proposal for data retention. The United Kingdom and the Netherlands, in particular, questioned whether the privacy policy rules still struck 'the right balance between privacy and the needs of the law enforcement agencies in the light of the battle against terrorism.' The Parliament stood firm and up to a few weeks before the final vote on May 30, 2002, the majority of MEPs opposed any form of data retention. Finally, after much pressure by the European Council and European Union governments, and well-organized lobbying by two Spanish MEPs, the two main political parties (PPE and PSE, the centre-left and centre-right parties) reached a deal to vote in favor of the Council's position.[13]

The initiatives, in fact, began immediately after September 11. On September 20, 2001, the European Commission requested the Council of the European Union to submit proposals "for ensuring that law enforcement authorities are able to investigate criminal acts involving the use of electronic communications systems and to take legal measures against their perpetrators."[14] At a specially called meeting of the EU's Justice and Home Affairs, the Council adopted a series of 'Conclusions' which included requiring service providers to retain traffic data (instead of de-

---

11. *Id.*

12. *Id.*

13. *Id.* at 12.

14. Statewatch News Online, *EU Governments Want the Retention of all Telecommunications Data for General Use by Law Enforcement Agencies Under Terrorism Plan*, http://www.statewatch.org/news/2001/sep/20authoritarian.htm (accessed July 28, 2004).

stroying it) and for legal enforcement authorities to have access to it "for the purposes of criminal investigations."[15] Only two weeks before this request, on September 6, 2001, the European Parliament recommended in a resolution that "a general data retention principle must be forbidden" and that "any general obligation concerning data retention" is contrary to the proportionality principle.[16]

The external pressure from the United States came in the form of forty demands on the EU. In a letter dated October 16, 2001 to the President of the European Commission, President Bush requested that the European Union consider data protection issues in the context of law enforcement and counter-terrorism imperatives and, as a result, to revise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period. Simply, the demand was that the draft privacy directives that call for mandatory destruction should be revised to permit the retention of critical data for a reasonable period.[17]

Understandably, the group of eight Justices and Interior Ministers (G8), in May 2002, made similar requests:

> States should examine their policies concerning the availability of traffic data and subscriber information so that a balance is struck between the protection of privacy, industry's considerations and law enforcement's fulfillment of the public safety mandate. Data protection policies should strike a balance between the protections of personal data, industry's considerations such as network security and fraud prevention, and law enforcement's needs to conduct investigations to combat crime and terrorist activities.[18]

A policy document from the G8 states,

> To the extent that data protection legislation continues to permit the retention of data only for billing purposes, such a position would overlook crucial legitimate societal interests - particularly when applied to the Internet service provider area, where flat rate pricing and free Internet and E-mail services foreclose the need to retain traffic data for

---

15. *See* Statewatch News Online, *Conclusions Adopted by the Council (Justice and Home Affairs)*, 3, http://www.statewatch.org/news/2001/sep/03926-r6.pdf (accessed July 28, 2004).

16. Clive Walker & Yaman Akdeniz, *Anti-terrorism Laws and Data retention: War is Over?*, 54 N. Ireland Leg. Q. [No.2] (citing 167 Extraordinary Council meeting, Justice, Home Affairs and Civil Protection, Brussels (Sept. 20, 2001)).

17. There is no similar obligation for the general retention of data in the U.S. even after the passing of the U.S.A. *Patriot Act*. When debating the passage of the Act, the U.S. Congress repeatedly rejected a full data retention approach.

18. Department of Justice Canada, *G8* Statement: *Principles on the Availability of Data Essential to Protecting Public Safety*, http://canada.justice.gc.ca/en/news/g8/doc3.html (Feb. 5, 2004).

> billing purposes - and thereby seriously hamper public safety.[19]

It has been argued that while the European Parliament was still "discussing the changes to the 1997 EC Directive on Privacy in Telecommunications, the Belgian government was drafting (and circulating for comment) a binding Framework Decision on the retention of traffic data and access for the law enforcement agencies."[20] According to the Statewatch, the document "shows that the EU governments always intended to introduce an EC law to bind all member states to adopt data retention."[21]

In June 2001, "the incoming Danish Presidency of the Council of the European Union (the 15 EU governments) submitted 'Draft Council conclusions' on this topic, which [contained] four recommendations to the EU's Multidisciplinary Group on Organized Crime (MDG)."[22] The Draft Conclusions state:

> Within the very near future, binding rules should be established on the approximation of member States' rule on the obligation of telecommunications service providers to keep information concerning telecommunications in order to ensure that such information is available when it is of significance for a criminal investigation.[23]

One of the arguments put forward in legitimizing "the move during the discussions in the European Parliament was that the change to the 1997 Directive simply enabled governments to adopt laws for data retention if national parliaments agreed."[24] "The draft Framework Decision [states] that data should be retained for twelve to twenty-four months in order for law enforcement agencies to have access to it."[25]

III. THE UK'S DATA RETENTION REGIME

The Anti-Terrorism, Crime and Security Act 2001 ("ATCSA"), in Part 11, is specifically dedicated to the retention of communications data.[26] Sections 102-107 give power to the Secretary of State to ensure

19. Department of Justice Canada, *G8 Statement on Data Protection Regimes*, http://canada.justice.gc.ca/en/news/g8/doc5.html (Feb. 2, 2004).

20. A copy of which has been leaked to Statewatch, Statewatch. *Statewatch Analysis no. 11, Surveillance of Communications: Data Retention to be Compulsory for 12-24 months*, 1, http://www.statewatch.org/news/2002/aug/analy11.pdf (accessed Oct. 25, 2004) (analyzing the draft framework decision).

21. *Id.* at 2.

22. *Id.*

23. *Id.*

24. *Id.*

25. Statewatch. *Statewatch Analysis no. 11, Surveillance of Communications: Data Retention to be Compulsory for 12-24 months*, 2, http://www.statewatch.org/news/2002/aug/analy11.pdf (accessed Oct. 25, 2004).

26. *See Anti-terrorism, Crime and Security Act* §§ 102-107 (2001) [hereinafter ATCSA].

that communications providers retain data.[27] Section 102(1) provides that "the Secretary of State shall issue, and may from time to time revise, a code of practice relating to the retention by communications providers of communications data obtained by or held by them."[28] Under subsection (2), "the Secretary of State may enter into such agreements as he considers appropriate with any communications provider about the practice to be followed by that provider in relation to the retention of communications data obtained by or held by that provider."[29]

Any code of practice or agreement may contain provisions that appears to the Secretary of State to be necessary "(a) 'for the purpose of safeguarding national security;' or '(b) for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security."[30] This phrase 'may relate directly or indirectly to national security' was included apparently as a last minute opposition amendment in the House of Lords to act as a limitation of the purposes envisaged. Whatever is intended, there may only be limited practical difference - the agreement or code of practice seems likely to require communication providers to retain all information they have of certain types for a period of time, and it would be probably not be practical to retain data selected on a message-by-message basis. It seems unlikely that in most circumstances it would be possible to distinguish between that data which is so potentially relevant to national security and that which is not, so the requirement in practice may be to retain it all.[31]

The procedure for making the code of conduct of practice is governed by Section 103. The Secretary of State is required to publish the code in draft and to consider any recommendations about the draft.[32] He is specifically required to consult with the Information Commissioner and with communication service providers to whom the code will apply.[33] He is then to lay the draft code before Parliament.[34] The code is to be brought into force by statutory instrument, which is to be approved by Parliament under the affirmative resolution procedure.[35]

---

27. *Id.*

28. *Id.* at § 102(1).

29. *Id.* at § 102(2).

30. *Id.* at § 102(3).

31. Philip Westmacott, *Computer Law and Security Report: Big Brother Never Forgets - The Data Retention Provisions of the Anti-Terrorism, Crime and Security Act 2001*, vol. 18, no. 3, 206 (2002).

32. ATCSA § 103(1).

33. *Id.* at § 103(2).

34. *Id.* § 103(4).

35. *Id.* § 103(5), (7).

Failure to comply with the code of practice or agreement shall not in and of itself render the communications service providers liable for any criminal or civil proceedings.[36] However, "a code of practice or agreement shall be admissible in evidence in any legal proceedings in which the question arises [as to] whether [ ] the retention of any communications data is justified on the grounds that a failure to retain the data would be likely to prejudice national security, the prevention or detection of crime or the prosecution of offenders."[37] This subsection provides a basis of admissibility of a voluntary code of practice or agreement to protect any communications provider in the event that the retention of data is sought to be justified on the grounds of national security or crime prevention, detection or prosecution on the basis of national security.

In the event that voluntary scheme fails, section 104 of the ATCSA empowers the Secretary of State to issue a direction.[38] Under this section, the Secretary of State may issue a direction by order made by statutory instrument, specifying the maximum period that communications service providers may be required to retain data.[39] The power to issue such an order is only to be exercised if, after reviewing the operation of any Code or agreement under section 102, the Secretary of State considers it to be necessary to do so.[40] Such an order may only be made for the statutory purposes prescribed in section 102(3).[41] Accordingly, the legislation envisages that the Secretary of State must first seek to achieve a workable system of voluntary data retention for national security purposes and only if that fails adequately to meet those objectives may he resort to compulsory powers. As with the Code, there are statutory consultation requirements, but these do not include the Commissioner.[42]

The Regulation of Investigatory Powers Act 2000 ("RIPA") "permits a range of public authorities to obtain access to such communications data for a wide variety of public interest purposes beyond issues concerning national security."[43] The ATCSA provides for the retention of data for the purposes of safeguarding national security or for the prevention or detection of crime or the prosecution of offences, which relates directly or indirectly to national security. Ben Emmerson QC and Helen Mountfield wrote:

---

36. *Id.* § 102(4).
37. ATCSA § 102(5).
38. *Id.* at § 104.
39. *Id.* at § 104(1).
40. *Id.*
41. *Id.*
42. *See* ATCSA § 104(4).
43. Ben Emmerson QC & Helen Mountfield, *Anti-Terrorism, Crime and Security Act 2001: Retention and Disclosure of Communications Data: Summary of Councils' Advice*, ¶ 4, http://www.privacyinternational.org/countries/uk/surveillance/ic-terror-opinion.htm (accessed Apr. 30, 2004).

> The consequence of these two overlapping regimes is that data may be retained for longer than they otherwise would be, on the ground that their retention is necessary for the purposes of safeguarding national security, but that the data may then be accessed for a variety of collateral public purposes which have no connection (direct or indirect) with national security.[44]

Caspar Bowden of the Foundation for Information Policy Research ("FIPR") noted that Part 11 of the ATCSA would "allow automated surveillance of the private lives of a substantial proportion of the population through analyzing the patterns of their electronic communications. The powers are deliberately broad and can be exercised quite generally for non-terrorist, as well as terrorist, investigations."[45] He further noted that, in short, it permits:

- Traffic Analysis - computerized 'trawling' of who people talk to (by phone or e-mail), where they go (pinpoint tracking via mobile phones), what they read (websites browsed).
- Blanket data retention - Internet and telephone companies will be required to stockpile such data on the entire population for long periods-the penultimate step towards a national 'traffic data warehouse,' sought jointly by police, customs, intelligence and security agencies.
- Mass-surveillance - a police Superintendent or equivalent rank can authorize access to data on a single person or millions of people, without any judicial or executive warrant, and with no guidance on proportionality. Data thus obtained can be accumulated centrally and exploited speculatively.
- Public order, minor offences, health and safety, and tax - are valid purposes for the exercise of these powers, as well as counter-terrorism.[46]

IV. CONSULTATION PAPER AND RESPONSE

On March 11, 2003, the Government published a consultation paper on the *Code of Practice for Voluntary Retention of Communications Data* required under ATCSA.[47] Together with this, a draft Code of Practice was attached in Annex A.[48] The paper invites views and comments on the Code of Practice on "whether the approach being taken is appropriate and proportionate . . . whether the retention regime is appropriate

44. *Id.* ¶ 5.

45. Casper Bowden, *Closed Circuit Television For Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-terrorism Legislation*, 2002 Duke L. & Tech. Rev. 0005, ¶ 1 (Apr. 5, 2002) http://www.law.duke.edu/journals/dltr/articles/2002dltr0005.html.

46. *Id.*

47. U.K. Home Office, *Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data*, http://www.homeoffice.gov.uk/docs/vol_retention.pdf (Mar. 2003).

48. *Id.* at 17-25.

under the data protection [regime]," the effects of compliance with the Code on the industry, "whether the likely [expenditures] to comply with the Code . . . is justified by the end product of such retention," and finally, and interestingly, whether the UK "should adopt new legislation on data retention that removes the question of disparity that currently exists."[49]

The Home Office does not seem to be keen on data preservation as suggested by many. It does not consider data preservation on a case-by-case basis to be an adequate tool for fighting terrorism and safeguarding national security because "data preservation will never aid in the investigation of a person who is not currently suspected of involvement with a terrorist organization."[50] The Government argues that "data preservation is a very useful tool for investigating the activities of someone already under suspicion."[51] The attitude is "data preservation can be used to supplement data retention but not replace it."[52]

According to the consultation paper, the "Code of Practice is intended to outline how communication service providers can assist in the fight against terrorism by meeting agreed time periods for retention of communications data that may be extended beyond those periods for which their individual company currently retains data for business purposes."[53] Specifically, the "Code of Practice is intended to ensure that communication service providers may retain data . . . after the need for retention for business purposes has elapsed and there is otherwise an obligation to erase or anonymise retained data."[54]

The paper states that "the usefulness of different types of communications data for the purpose of safeguarding national security will vary and this is reflected in the different retention periods."[55] The retention periods are: twelve months for subscriber information as well as telephony data, six months for SMS, EMS and MMS data, six months for e-mail data, six months for ISP data, and four days for web activity logs.[56] For other services, such as instant message type services (log-on/off time) and collateral data, the retention is relative to the service provided and

49. *Id.* at 3 ¶ 1.5.

50. *Id.* at 15 ¶ 12.4.

51. *Id.*

52. *Id.* at 15 ¶ 12.7.

53. *See* U.K. Home Office, *Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data: Draft Code of Practice*, 20, ¶ 1, http://www.homeoffice.gov.uk/docs/ vol_retention.pdf.

54. *Id.* at 20, ¶ 3.

55. *Id.* at 23, ¶ 18.

56. U.K. Home Office, *Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data: Draft Code of Practice: Appendix A*, 26-27, http://www.homeoffice.gov.uk/ docs/vol_retention.pdf.

to data to which it is related.[57] The Government argues that the data categories and retention periods have been determined with regard to considerations of necessity and proportionality.[58] The retention specification "has been drafted taking into account a number of factors, including Article 8 of the European Convention on Human Rights."[59] The Secretary of State considers the retention periods set out to be both necessary and proportionate in light of the individual's right to respect for private life and the national security purposes for which the retention of data is required.[60]

> On the costs arrangements, the consultation paper suggests that:
> Where the period of retention of data for national security purposes is not *substantially* longer than the period of retention for business purposes, the retention costs will continue to be borne by the communication service providers. Where data retention periods are *significantly* longer for national security purposes than for business purposes, the Secretary of State will contribute a reasonable proportion of the marginal cost as appropriate. Marginal costs may include, for example, the design and production of additional storage and searching facilities. This may be in the form of capital investment into retention and retrieval equipment or may include running costs.[61]

In its regulatory impact assessment, the Government has given assurances that measures taken in the context of the emergency legislation should not commercially disadvantage UK business or impact on the confidence of users and operators in the UK as the best place to do e-business. The *details* of the requirements will be covered in the code of practice.[62] The questions are whether the provision of the Code of Practice contains the details as promised and how to interpret both the words 'substantially' and 'significantly' mentioned in the Code.

In the twelve-week consultation period, a total of fifty-seven replies have been received by the Home Office which concludes, "The consultation paper provoked a lively debate about data retention across a broad spectrum of interested parties and reconfirmed industry's commitment to helping the government achieve its aims in the fight against terrorism."[63] Some have criticized the consultation itself. Ian Brown of the FIPR, skeptical about the process, argued that:

---

57. *Id.* at 27.

58. *Draft Code of Practice* at 21, ¶ 11.

59. *Id.*

60. *Id.*

61. *Id.* at 23, ¶¶ 23-24 (emphasis added).

62. *See* U.K. Home Office, *Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data*, http://www.homeoffice.gov.uk/docs/vol_retention.pdf (accessed July 28, 2004).

63. U.K. Home Office, *Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data (under the Anti-Terrorism Crime and Security Act 2001): Re-*

> The data retention consultation is a sham.. . . The Home Office has failed to address any of the well-known substantive issues and is merely going through the motions so it can come back with a compulsory scheme. The compulsory scheme is also likely to be unlawful and will be incredibly expensive. The Home Office needs to drop data retention and start again, perhaps with a targeted preservation scheme such as seems to be successful in the USA.[64]

> On the questions of the appropriateness and proportionality of the code, many of those responding indicated that they did not feel the threat to national security was a subject on which they had sufficient knowledge to enable them to judge the extent of the proposals. Of the replies received, 34 commented on this issue and, of those, 25 believed that, based on the information available, the approach was not appropriate or proportionate. The validity of data retention under the Code, in relation to data protection legislation, provoked comment from 27 respondents. Of those, 22 believed that the regime would be inappropriate. . . . Two-thirds of those who contributed to the consultation process expressed a view on the need for a retention regime. Of these, 22 were against the concept of retention, while 14 favored such a regime. . . . Of the total responses 26 contained comment on the retention timescales proposed in the Code. Nineteen of these indicated that the periods identified were not reasonable.[65]

Liberty, "one of the UK's leading civil liberties and human rights organizations,"[66] objected fundamentally, "as a matter of principle[,] to any approach to protection of national security or prevention of crime that [involved] the creation of a pool of personal data [on] millions of innocent people."[67] According to the Liberty, nothing in Section 102 of the ATCSA suggests that Parliament contemplated a step that allows the creation of a pool of retained data about large numbers of people against whom there is not the faintest suspicion of unlawful activity with a view to its being made available to the state.[68] The Liberty further argued:

---

sponse to the Consultation Paper, ¶ 17, http://www.homeoffice.gov.uk/docs2/vol_retention_comms_data.html (Sept. 11, 2003).

64. *See* ZDNet UK, Matt Loney, *Government's data retention back-pedal fails to impress*, http://news.zdnet.co.uk/internet/0,39020369,2131747,00.htm (accessed Apr. 29, 2004).

65. *Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data*, *supra* n. 63, at ¶¶ 5-6, 10-11.

66. Liberty, *Liberty Response to the Home Office Consultation: 'A Code of Practice for Voluntary Retention of Communications Data,'* 2, http://www.liberty-human-rights.org.uk/resources/policy-papers/policy-papers-2003/pdf-documents/vol-retention-of-comms-data.pdf (June 2003).

67. *Id.* at ¶ 4.

68. *Id.* at ¶¶ 5-6.

> Even if potentially authorized by the Act, the "data pool" approach would be neither legally nor politically defensible unless supported by the most compelling justification. The mere possibility that information about citizens' prima facie lawful activity will be of future interest to the police or security services is far too contingent to provide justification for the blanket adoption of periods of retention that substantially exceed those mutually contemplated by the provider and user of communications services. Such an approach cannot be reconciled with the principles of necessity and proportionality.[69]

The Joint Committee on Human Rights of the House of Lords and the House of Commons, which examined the Draft Code, has raised four matters of concern on human rights grounds.[70] First, if the communications providers which retain communications data "are not 'public authorities' for the purposes of the Human rights Act 1998, then they are not directly subject to the legal obligations imposed by Section 6 of that Act to act compatibly with Convention rights. It is therefore unclear how the Draft Code would ensure that the state could discharge its obligations under the ECHR Article 8 in relation to the retention and storage of the data."[71] Second, "it is not clear how the Draft Code's standard periods of retention would meet the requirement of proportionality which form part of the test of necessity" under Article 8 of the ECHR.[72] Third, "the availability of the communications data to agencies for purposes other than the protection of national security would call in the question the legitimacy of the aim for which the data are to be retained, [as well as] the necessity for that retention and its proportionality."[73] Fourth, "it is not clear how thoroughly the consultation exercise . . . was carried out and how far the fruits of it have been taken into account in the Draft Code."[74]

The Committee noted that:

> Any invasion of the right must be strongly justified. Safeguards are essential. Making those who retain communications data subject to the Human Rights Act might be one such safeguard. Unless the primary legislation is amended to provide expressly that the providers are, are not, public authorities for that purpose, only the courts can answer the

69. *Id.* at ¶ 7.

70. House of Lords and House of Commons Joint Committee on Human Rights, *Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001, Sixteen Report of Session 2002-03*, 7, http://www.parliament.the-stationery-office.co.uk/pa/jt200203/jtselect/jtrights/181/181.pdf (Nov. 11, 2003). The Committee was disappointed that the Home Office did not explicitly seek its views before laying the draft order bringing the Draft Code into effect. *See id.* at 6.

71. *Id.* at 7, ¶ 7(a).

72. *Id.* at 7, ¶ 7(b).

73. *Id.* at 7, ¶ 7(c).

74. *Id.* at 7, ¶ 7(d).

question authoritatively.[75]

The Committee noted that "if the Government's view is correct, it increases the importance of ensuring that the provisions of the Code, under which the communications providers will work, are fully compatible with Convention rights, particularly ECHR Article 8."[76]

On the second issue, the Joint Committee recognized that the state has an obligation to ensure that the blanket retention of communications data is necessary for a legitimate purpose, and that it is proportionate to the aim which it seeks to achieve.[77] "In the context of communications data, appropriate safeguards might also include legislation [that imposes] on service providers an obligation to ensure that an assessment of proportionality is made in relation to different pieces of data."[78] According to the Committee, "neither the Regulation of Investigatory Powers Act 2000, the Anti-terrorism, Crime and security Act 2001 nor the Draft Code indicates that there is a requirement of proportionality, let alone offers advice on how it should be applied."[79] The Committee remarked:

> We agree that Parliament accepted that there may be a need for data retention for those purposes. . .However, we have not been able to establish how pressing the needs is, or how often the police and security and intelligence services find it necessary to make use of such data or are significantly hampered by its absence. Those matters seem to us to be relevant to the assessment, to be made by each House, of the necessity for the retention which would be sought by the Draft Code, and of the proportionality of the periods set for retention of each kind of communications data.[80]

Regarding the use of retained data for purposes unrelated to national security, the Joint Committee is "prepared to accept the Government's view that, as a matter of policy, it should be possible to have access to any communications data which are available and relevant to a case if the conditions are satisfied on the facts of the particular case."[81] The Committee has come to the conclusion that the safeguards,[82] cou-

75. House of Lords and House of Commons Joint Committee on Human Rights, at 8, ¶ 12, http://www.parliament.the-stationery-office.co.uk/pa/jt200203/jtselect/jtrights/181/181.pdf.

76. *Id.* The Government takes the view that the retention of communications data by communications providers is "a private function that arises out of the commercial service that the communication services providers provide." *Id.* at 19.

77. *Id.* at 8-9, ¶ 12.

78. *Id.* at 9, ¶ 16.

79. *Id.* at 9, ¶ 16.

80. *Id.* at 10, ¶ 19.

81. House of Lords and House of Commons Joint Committee on Human Rights, at 12, ¶ 25, http://www.parliament.the-stationery-office.co.uk/pa/jt200203/jtselect/jtrights/181/181.pdf.

82. The safeguards are: (1) any access will have to be authorized or required by a designated person in a public authority empowered to access such data by the RIPA, (2) the

pled with the availability of judicial review of a notice or authorization under the RIPA and the need to comply with the Data Protection Principles under the Data Protection Act 1998, "are capable[,] in principle[,] of providing appropriate protection for the right to respect for private life and correspondence under ECHR Article 8."[83]

On the consultation process, the Committee "asked the Government what views the Information Commissioner expressed when consulted on the Draft Code and what steps were taken to consult with the communications service providers."[84] The Committee is satisfied that the steps taken were "sufficient to comply with the Secretary of State's duty under section 103(2) of [the ATCSA] to consult the communications providers to whom the Draft Code will apply."[85]

> The Joint Committee in its conclusion explicitly noted that they are very concerned that the communications providers who will be retaining communications data under the provisions of Part 11 of the ATCSA, often for long periods, as a matter of course will not. . . be functional public authorities for the purposes of the Human rights Act 1998, and so will not be subject to any of the obligations arising under ECHR Article 8.[86]

As already mentioned, the Committee is of the view that this "makes it particularly important to ensure that the Draft Code, and the standard periods of retention which it contains, are necessary for a legitimate aim and are proportionate to the objective sought to be achieved."[87] The Committee regrets that "more time has not been allowed to permit Parliament to consider more fully these far-reaching proposals."[88] The Committee noted, "[t]he Home Secretary has convinced us that making communications data accessible is likely to be useful investigative tool, but we are not able to say that we are satisfied that the arrangements in the Draft Code would be proportionate to legitimate objectives."[89]

---

designated person will be a public authority, bound by the Human Rights Act 1998 and the Convention rights, (3) the designated person will also be bound to refuse a notice or authorisation unless he or she believes that the requirements of necessity and proportionality are met on the facts of each particular case under section 22(1) and (5) of the RIPA, (4) the availability of judicial review of a notice or authorisation under the RIPA, and (5) the need to comply with the Data Protection Principles under the Data Protection Act 1998.

83. House of Lords and House of Commons Joint Committee on Human Rights, at 12, ¶ 25, http://www.parliament.the-stationery-office.co.uk/pa/jt200203/jtselect/jtrights/181/181.pdf.

84. *Id.* at 12, ¶ 27.

85. *Id.* at 13, ¶ 28.

86. *Id.* at 14, ¶ 31.

87. *Id.*

88. House of Lords and House of Commons Joint Committee on Human Rights, at 14, ¶ 33, http://www.parliament.the-stationery-office.co.uk/pa/jt200203/jtselect/jtrights/181/181.pdf.

89. *Id* at 14, ¶ 31.

V. DATA RETENTION UNDER HEAVY CRITICISM

From the government's perspective, according to Marco Cappoto, a radical MEP and long term civil liberties campaigner, "it should be easy for the Council to find agreement on a common framework decision on data retention once the 'technicalities' can be arranged."[90] He stated,

> Of the governments surveyed, Denmark 'can support' a European instrument. Greece, Ireland, Italy, Luxembourg, Spain, Portugal, the UK and Sweden warmly support the idea. The only countries expressing some uncertainties are Austria and Germany. The German authorities say that they need proof that the European instrument is compatible with the German constitutional law.[91]

The Electronic Privacy Information Center ("EPIC"), however, predicts that the implementation phase of the data retention provision may become bumpy in many EU countries.[92] "While a few countries have already established data retention schemes (e.g. Belgium, France, Spain, and the United Kingdom), the implementation phase of the Directive's data retention provision" may not be smooth in other Member States principally because the Directive could be considered as being in conflict with the constitutions of some EU countries[93] with respect to fundamental rights, such as the presumption of innocence, right to privacy, confidentiality of communications and freedom of expression.[94]

The principle of data retention still faces strong criticism from many parties. It has been argued that, although the data retention provision of the new Directive is supposed to constitute an exception to the general regime of data protection established by the Directive:

> [T]he ability of the governments to compel ISPs and telecommunications companies to store all data about all of their subscribers can hardly be construed as an exception to be narrowly interpreted. The practical result is that all users of new communication technologies (the Internet, e-mail, mobile phones, etc.) are now considered worthy of scrutiny and surveillance in a generalized and preventive fashion for periods of time that states' legislatures or governments have discretion to determine.[95]

---

90. The Register, John Leyden, *Germany, Austria take stand against EU ISP data retention laws*, http://www.theregister.co.uk/content/6/28228.html (Nov. 21, 2002).

91. *Id.*

92. Electronic Privacy Information Center, *Data Retention*, http://www.epic.org/privacy/intl/data_retention.html (last updated Mar. 25, 2004).

93. The Austrian Federal Constitutional Court held on Feb. 27, 2003 that the statute that compelled telecommunication service providers to implement wiretapping measures at their own expense is unconstitutional.

94. Electronic Privacy Information Center, http://www.epic.org/privacy/intl/data_retention.html.

95. *Id.*

The "Global Internet Liberty Campaign ("GILC"), a coalition of 60 civil liberties groups, [that] organized a campaign against data retention" during the debate of the Directive, argues that "data retention. . . is contrary to well-established international human rights conventions and case law."[96] The "Data Protection Commissioners in the EU and their officials, who attended a multitude of working parties, have long been aware" of the data retention initiative.[97] The spring conference of European Data Protection Commissioners in Stockholm, April 6-7, 2000, issued a declaration on the 'Retention of Traffic Data by Internet Service Providers,' stating:

> Such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights. Where traffic data are to be retained in specific cases, there must be demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law.[98]

Again, on September 11, 2002, during the international conference of data protection commissioners in Cardiff, the European Data Protection Commissioner released a declaration that strongly warned against any future EU-wide mandatory and systematic data retention scheme. The Commissioners expressed "grave doubt as to the legitimacy and legality of such broad measures."[99]

The International Chamber of Commerce ("ICC") based its criticisms on consumers' privacy concern and confidence, as well as the unreasonable cost and technical burdens on the telcoms and ISPs.[100] According to the ICC, "public concern about the privacy of communications and activities on the Internet has been widely expressed in the context of proposals for mandatory traffic data retention, and it is unlikely to diminish as more countries consider legislation."[101] The ICC also questioned the need for the data retention regime as the data kept for billing purpose can be used by the law enforcement agencies.[102] The ICC assures governments of the world:

---

96. *Id.*

97. Statewatch, *EU Governments to Give Law Enforcement Agencies Access to All Communications Data*, http://www.statewatch.org/news/2001/may/03Benfopol.htm (accessed Apr. 29, 2004).

98. *Id.*

99. *See* Foundation for Information Policy Research, *Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data*, http://www.fipr.org/press/ 020911DataCommissioners.html (accessed Oct. 29, 2004).

100. *See* ICC, *"Don't Play Big Brother" is Business Plea to Governments on Internet Traffic*, http://www.iccwbo.org/home/news_archives/2002/stories/big_brother.asp (Nov. 29, 2002).

101. *Id.*

102. *Id.*

> Business is as determined as anybody to fight crime and terrorism. But we are convinced that law enforcement agencies can get all the information they need from traffic data already kept by business for billing purposes without impairing public confidence in Internet services through Orwellian intrusiveness.[103]

The ICC has issued a policy statement to warn governments against the emerging traffic data retention laws.[104] It recommends that governments should favor "targeted data preservation over data retention regimes."[105] Other recommendations include:

- Data retention must be justified, proportionate and necessary for the purposes of investigating and prosecuting terrorism and other criminal activity only. The types and time period of data to be retained should be kept to an absolute minimum.
- Access to traffic data should be limited to law enforcement agencies on production of a warrant or similar instrument.
- Governments should bear the infrastructure costs of mandatory data retention regimes.
- Transparent and effective oversight procedures are necessary to prevent abuses and safeguard consumer confidence.[106]

The ICC concludes:

> Any traffic data storage requirements imposed by governments should be focused, narrow, publicly funded, limited to the measures absolutely necessary to protect society, and balances the interests of government, business and users.[107]

The European Internet Services Providers Association ("EuroISPA") and the US Internet Service Provider Association ("USISPA")

> Urge all governments to undertake a serious cost benefit analysis of the impact of applying mandatory data retention requirements before moving forward in this area. This should be accompanied by equally serious analysis and comparison of alternative regulatory approaches, in particular, that of 'data preservation'. The ISP industry is convinced that the later approach, in conjunction with appropriate use of data managed by ISPs for the security of their services, is the right and only way forward.[108]

The EuroISPA and USISPA argue that:

> Mandatory data retention is an extreme step. Governments have not sufficiently demonstrated that the absence of mandatory data retention

---

103. *Id.*

104. ICC, *Policy Statement: Storage of Traffic Data for Law Enforcement Purposes*, http://www.iccwbo.org/home/e_business/policy/373-22-106E.pdf (Nov. 18, 2002).

105. *Id.* at 1.

106. *Id.* at 2, 4, 5.

107. *Id.* at 6.

108. *EUROISPA and US ISPA Position on the Impact of Data Retention Laws on the Fight Against Cybercrime*, 1, http://www.euroispa.org/docs/020930eurousispa_dretent.pdf (Sept. 30, 2002).

> is detrimental to the public interests. In countries like the United States, where there is no *mandatory data retention*, the law enforcement agencies routinely obtain the evidence they need. The US law enforcement has also endorsed *data preservation* as workable solution.[109]

Data retention, according to these organizations, "would be a major blow to the current European legal framework on data protection. [The] industry is extremely concerned that the issue of privacy seems to be raised mainly when discussing the duration of retention and not its scope."[110]

According to the EuroISPA and USISPA, "Mandatory Data Retention by ISPs – for which there is no business purpose – would impose serious technical, legal and financial burdens on ISPs."[111] It will "put much personal information at risk of accidental disclosure or intentional misuse," and "data preservation is a significantly less radical and currently available solution" for evidence-gathering tool.[112] The EuroISPA and USISPA assert:

> ISPs find that there is no compelling or convincing evidence of greater efficiency benefits for law enforcement with the data retention approach. . . . Mandatory data retention is a drastic step that should not be taken unless drastic alternatives have been tested and proven inadequate.[113]

The All Party Internet Group ("APIG") conducted an "inquiry into all aspects of communications data retention and the subsequent access to that data from a UK, European and global perspective. The inquiry [primarily focuses] on the enforcement of the powers contained in the [RIPA] and the [ATCSA] and their subsequent effect on communications service providers."[114] In January 2003, APIG published a crucial document, *Communications Data: Report of an Inquiry by the All Party Internet Group*.[115] The report states, "in some people's view, Parliament was mistaken and the retention of communications data, even for reasons of national security, is not proportionate and therefore not 'human rights compliant.'"[116] The APIG argues:

> In view of the clear evidence presented to us of its inevitable failure, we can see nothing to be gained from the spectacle of seeing a voluntary scheme proposed, approved by Parliament and then being ignored by the communications service providers. We can reach no other conclu-

109. *Id.* (emphasis original).
110. *Id.* at 2.
111. *Id.*
112. *Id.*
113. *Id.* at 1, 3.
114. All Party Parliamentary Internet Group, *Communications Data: Report of an Inquiry by the All Party Internet Group*, 34, http://www.apig.org.uk/APIGreport.pdf (Jan. 2003).
115. All Party Parliamentary Internet Group, http://www.apig.org.uk/APIGreport.pdf.
116. *Id.* at 20, ¶ 134.

> sion than to recommend that the Home Office immediately drop their plans to introduce a voluntary scheme for data retention under ATCSA.[117]

Mandatory data retention scheme, according to the APIG, "will do immense harm to the [CSP] industry and will not actually achieve the results wished for by Law Enforcement."[118] The APIG does not believe that it is practical "to retain all communications data on the off chance that it will be useful one day."[119] It recommends very strongly for the Government not to invoke their powers under Section 104 of the ATCSA and impose a mandatory data retention scheme.[120] Instead, the Home Office should "enter into a dialogue with the CSP industry to develop an appropriate data preservation scheme to meet the needs of Law Enforcement."[121] The APIG believes "that the moves in other EU states towards a data retention policy are entirely mistaken. In particular, . . . ["S]addling the entire European communications service providers industry with costs that do not have to be incurred by their American competitors will cause immense damage."[122] The APIG urgently recommends that the Government "enter into Europe-wide discussion to dismantle data retention regimes and to ensure that data preservation becomes EU policy."[123]

The FIPR believes that the creation of warehouses of communications data will lead to significant abuses of the individual's rights.[124] The FIPR argues that "it is predictable that excuses will be found to trawl through them looking for patterns of behavior or patterns of association. Such warehouses are exactly the tools needed to create a totalitarian state, and it is foolish in the extreme to create them."[125]

VI. BALANCING THE COMPETING COMMUNITY INTERESTS

The Home Office, in recognizing the relationship between privacy and freedom, states "We value our privacy. We value our freedom. In the same way our freedom is balanced against society's rules, our privacy has to be balanced against the needs of society for preventing and de-

117. *Id.* at 22, ¶141.

118. *Id.* at 27, ¶177.

119. *Id.*

120. All Party Parliamentary Internet Group, at 27, ¶178, http://www.apig.org.uk/APIGreport.pdf.

121. *Id.* at 28, ¶186.

122. *Id.* at 29, ¶189.

123. *Id.*

124. *See* FIPR's comments submitted to the APIG inquiry, 2, http://www.apig.org.uk/fipr.pdf (accessed Oct. 29, 2004).

125. *Id.*

tecting crime."[126] On the other hand, in achieving the twin objectives of enhancing privacy and making better use of personal data to deliver smarter public services, the Government insists that it will opt for the least intrusive approach.[127] This means that where it "can achieve improvements in services or efficiency without requiring more information and affecting personal privacy, it should do so."[128] The Government pledges that it will consider alternative approaches that have a lesser impact on privacy in achieving the objectives.[129] After all, the protection of privacy, according to the Government, is in and of itself a public service.[130] As argued by many, data preservation being the least intrusive is the option.

"The tragic terrorist attacks against the United States have highlighted the necessity for democratic societies to engage in the fight against terrorism. This objective is both a necessary and valuable element of democratic societies. In this fight, certain conditions have to be respected which also form part of the basis of the democratic societies."[131] "Measures against terrorism should not and need not reduce standards of protection of fundamental rights which characterizes democratic societies. A key element of the fight against terrorism involves ensuring the preservation of these fundamental values that are the basis of the democratic societies and the very values that those advocating the use of violence seek to destroy."[132] "There is an increasing tendency to represent the protection of personal data as a barrier to the efficient fight against terrorism."[133]

As stated by the EU Working Party, "terrorism is not a new phenomenon and cannot be qualified as a temporary phenomenon."[134] And legislation is not the only weapon in the counter-terrorism armory, nor is it the most important. Lord Lloyd of Berwick in his report, *Inquiry Into Legislation Against Terrorism*, stated that the primary function of the law in this area is to support policies and activities which tackle the

126. Home Office, *Access to Communication Data: Respecting Privacy and Protecting the Public from Crime, A Consultation Paper* http://www.homeoffice.gov.uk/docs/consult.pdf (Mar. 2003).

127. Cabinet Office, *Privacy and Data-sharing: The Way Forward for Public Services*, Apr. 8, 2002 (available at http://www.number-10.gov.uk/su/privacy/downloads/piu-data.pdf (accessed July 29, 2004)).

128. *Id.* at 5.

129. *Id.* at 6.

130. *Id.* at 5.

131. Article 29 – Data Protection Working Party, *Opinion 10/2001: On the Need for a Balanced Approach in the Fight Against Terrorism,* 2 (Dec. 14, 2001) (available at http:// www.statewatch.org/ news/2002/jan/wp53en.pdf (accessed Nov. 1, 2004)).

132. *Id.* at 4.

133. *Id.*

134. *Id.* at 3.

menace of terrorism directly. The first, and overriding, response to terrorism is the political.[135] According to the report, some terrorist campaigns may ultimately be brought to an end only by political means, backed as necessary by security measures.[136] Other forms of terrorism must simply be suppressed - there is no practical alternative.[137] And since terrorist violence presents a direct challenge to the government's primary responsibility to ensure public safety, fighting terrorism is, itself, a political activity.[138]

Lord Lloyd has formulated four general principles that should govern any code of laws designed to counter violent subversion. First, legislation against terrorism should approximate as closely as possible to the ordinary criminal law and procedure.[139] Second, additional statutory offences and powers may be justified but only if they are necessary to meet the anticipated threat.[140] They must then strike the right balance between the needs of security and the rights and liberties of the individual.[141] Third, the need for additional safeguards should be considered alongside any additional powers, and fourth, the law should comply with the UK's obligations under international law.[142]

In considering data retention measures, regard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole. In *Hatton v. U.K.*,[143] the applicants complained that the failure of the United Kingdom authorities to prevent night flights which disturbed their sleep during take-off and landing at Heathrow airport amounted to a violation of their right to respect for private and family life.[144] In striking the required balance, the Court held that the states must have regard to the whole range of material considerations:

> States are required to minimize, as far as possible, the interference with these rights, by trying to find alternative solutions and by generally seeking to achieve their aims in the least onerous way as regards human rights. In order to do that, a proper and complete investigation and study with the aim of finding the best possible solution, which will,

135. Rt. Hon. Lord Lloyd of Berwick, *Inquiry Into Legislation Against Terrorism*, vol. 1, no. 7 (1996).

136. *Id.*

137. *Id.*

138. *Id.*

139. *Id.*

140. Rt. Hon. Lord Lloyd of Berwick, *Inquiry Into Legislation Against Terrorism*, vol. 1, no. 7.

141. *Id.*

142. *Id.* at 9.

143. [2001] European Ct. of Human Rights 36022/97 (Oct. 2, 2001) (available at [2001] ECHR 36022/97).

144. *Id.*

> in reality, strike the right balance should precede the relevant project.[145]

Applying this test to all aspects of respect for private life (and not just in the field of environmental protection), it can be argued that the question of whether the state has carried out a thorough review of the laws concerning the protection of national security, as well as the prevention and detection of crime, before venturing into data retention is very relevant. The question of whether any alternative means are available which would minimize any interference with the rights of Article 8 is also relevant.

It must be emphasized that the right balance that must be struck here is not only between the competing interest of the individual against the interest of the community, but, also the interest of the community as a whole, to be protected against crime as well as against surveillance.

VII. POSSIBLE LEGAL CHALLENGE

The EU network of independent experts in fundamental rights ("CRF-CDF") published a thematic comment, *The Balance between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threat*, on March 31, 2003.[146] The report states that the independent experts on fundamental rights are, in fact, convinced that the effectiveness of steps to fight terrorism cannot be measured by the extent of restrictions which these steps impose on fundamental freedoms.[147] In other words, the increase in security is not inversely proportional to the restriction of freedom; on the contrary, certain practices minimize the scope of restrictions on fundamental rights whilst offering a high level of effectiveness.[148] The report concludes:

> International law on human rights is not opposed to States taking measures to protect against terrorist threat. But as a counterpart to restrictions that the States adopt to respond to that threat, it must imagine mechanisms by which the consequences for the guarantee of individual freedoms are limited to a strict minimum. In particular, independent control mechanisms must be provided that can counter possible abuse by the Executive or the criminal prosecution authorities. In addition, restrictions imposed on individual freedoms in response to the terrorist threat must be limited to what is absolutely necessary. These restrictions were adopted to cope with an immediate threat, but one that is not

145. *Id.* at ¶ 97.

146. EU Network of Independence Experts in Fundamental Rights, *The Balance Between Freedom and Security in the Response by the European Union and its Member states to the Terrorist Threats* (Mar. 31, 2003).

147. *Id.*

148. *Id.* at 10.

> necessarily permanent, and as such, they should be of a temporary character and be assessed regularly under some kind of mechanism. They should be targeted sufficiently precisely and not affect other phenomena or possibly other categories of persons, on the pretext of terrorist threat.[149]

Article 15 of the Electronic Privacy Directive allows data retention measures where "necessary, appropriate, and proportionate" within a democratic society.[150] The Directive sensibly and prudently only permitted retention measures if these conditions could be satisfied within a democratic society. The unrestricted, blanket data retention is expressly rejected. Furthermore, the Member States *may* take legislative measures providing for data retention only if is necessary, appropriate, and proportionate.[151] It is imperative for the government to demonstrate that data retention satisfy those requirements. This means that proper assessments of the necessity, appropriateness, and proportionality of the data retention legislative measures have to be carried out. There is also a need to assess whether less intrusive and less costly measures, such as data preservation, might effectively achieve what the data retention regime seeks to achieve.[152]

Article 8 of the European Convention on Human Rights ("ECHR") encompasses the right to be oneself, to live as oneself and to keep to oneself.[153] In the leading case of *Niemitz v. Germany*,[154] the court pronounced that respect for private life must also comprise, to a certain degree, the right to establish and develop relationships with other human beings. The Court in *Z v. Finland*[155] has asserted that the protection of personal data is of fundamental importance of a person's enjoy-

149. *Id.* at 52.

150. *Directive on Privacy and Electronic Communications*, 2002/58/EC at Art. 15. (July 12, 2002).

151. *Id.*

152. The current practice in Europe is that communication operators work closely with law enforcement agencies, police forces, and other national agencies. This cooperation includes real-time interception of communications and the preservation and disclosure of communications data that is routinely collected for legitimate business purposes. Indeed, the efforts of industry to assist with criminal and anti-terrorist investigations since September 11, 2001 have been praised by many EU governments. The current cooperation between law enforcement and industry has proven effective. There have been very few occasions when communications service providers have been unable to satisfy a request to disclose data because the data had already been deleted. If the current cooperation between law enforcement and industry has been and is effective, then it is even more imperative to demonstrate the application of the directive data storage provision be proportionate, necessary, and justified. *See* American Chamber of Commerce to the European Union, *"Position Paper on Data Retention in the EU,"* (June 4, 2003).

153. Lord Lester of Herne Hill & David Pannick, *Human Rights: Law and Practice* (1999).

154. 16 European Human Rights Rep., ¶ 29 (1992).

155. 25 European Human Rights Rep. 371, ¶ 95 (1998).

ment of his or her right to respect for privacy and family life under Article 8.

As already mentioned, many argue that the UK's data retention regimes constitute an interference with the right to respect for private life and correspondence enshrined in Article 8. The Government seems to admit this.[156] Relying on Article 8(2), the Government, interestingly, argues that communications data retention will be in accordance with the [ECHR,] provided that the *retention periods* are proportionate to the legitimate aims being pursued.[157] The Government also argues that in the ATCSA, "Parliament concluded that the retention of communications data was necessary for the purposes set out," and the "draft Code of Practice sets out the retention periods for different types of communications data that the Secretary of State considers proportionate."[158] Simply, the Government sees proportionality in the context of retention periods. Perhaps, the real issue is not so much on the retention periods, but whether the legal regimes allowing the retention and the act of retention itself are proportionate with the aims being pursued. As stated by the European Commissioners for data protection: "Systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case."[159]

Article 8(2) acknowledges that interference by the State is justified provided it is in accordance with the law and is necessary in a democratic society.[160] Article 8(2) has been given a narrow interpretation.[161] The European Court of Human Rights in the case of *Klass v. Fed. Republic of Germany*[162] stated that "powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as *strictly* necessary for safeguarding the democratic institutions."[163]

'In accordance with the law' means that the state must be able to show that its conduct must have some basis in domestic law whether by

156. The Government states that the retention of communications data by communications service providers in accordance with the Code beyond the periods that they would otherwise hold it for business purposes may engage the rights under Article 8 of the ECHR; *See Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data*, *supra* n. 47 at 9, ¶ 7.7.

157. *Id.* at 10, ¶ 7.7 (emphasis added).

158. *Id.* at 10, ¶ 7.8.

159. Foundation for Information Policy Research, *supra* n. 102.

160. Privacy International, *Memorandum of Laws Concerning the Legality of Data Retention with regard to the Rights Guaranteed by the European Convention on Human Rights*, 8, http://www.privacyinternational.org/issues/terrorism/rpt/data_retention_memo.pdf (Oct. 10, 2003).

161. *Id.*

162. 2 European Human Rights Rep. 214 (1979).

163. *Id.* at 231.

statute or by common law.[164] It might be argued that although the ATCSA provides a framework for a code of practice and/or agreement, and requires any code to be brought into force by statutory instrument, it may fail to meet this requirement of being 'in accordance with law' because of its voluntary nature.

'In accordance with law' does not merely refer to the existence of domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law.[165] The Court in the case of *Amann v. Switzerland*[166] reiterated this requirement of quality of law and held that the legal basis must be accessible and foreseeable. "The principle behind the foreseeability requirement is the simple notion that the State should give citizens an adequate indication of the circumstances in which public authorities are empowered to interfere in their private lives."[167] Thus, "individuals can regulate their conduct accordingly . . . to avoid invoking unwelcome intrusions by the State."[168]

> The requirement of foreseeability is not satisfied by blanket regulations, such as those envisaged in the [Draft Code], that allow everyone to foresee that the State will interfere with their right to a private life. As the Court said in respect of secret surveillance in *Malone v. United Kingdom* 'it would be "contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power.'" What makes a law foreseeable is the extent to which it distinguishes between different classes of people, thereby placing a limit on arbitrary enforcement by the authorities. Thus, in *Kruslin v. France*, the Court found that a law authorizing telephone tapping lacked the requisite foreseeability because it nowhere defined the categories of people liable to have their telephones tapped or the nature of the offences which might justify such surveillance. In *Amman v. Switzerland*, the Court reached the same conclusion with regard to a decree permitting the police to conduct surveillance because the decree gave no indication of the persons subject to surveillance or the circumstances in which it could be ordered. Data retention laws that fail to distinguish between different classes of people would have a more pernicious impact on individual privacy than the vague laws at issue in *Kruslin* and *Amann*.[169]

"Blanket data retention laws also offend the principle of foreseeability because they make no distinction for relationships the State already recognizes as sufficiently special to warrant a degree of protection."[170]

164. *Silver v. United Kingdom*, 5 European Human Rights Rep. 347 (1983); *Sunday Times v. United Kingdom*, 2 European Human Rights Rep. 245 (1979).

165. Privacy International, *supra* n. 165.

166. 30 European Human Rights Rep. 843 (2000).

167. Privacy International, *supra*, n. 165, at 8.

168. *Id.*

169. Privacy International, *supra* n. 165 at 8-9 (internal citations omitted).

170. *Id.* at 9.

The Court in *Kopp v. Switzerland*[171] held "that the telephone tapping law failed to meet the standard of foreseeability because it provided no guidance on how authorities should distinguish between protected and unprotected attorney-client communications."[172] The data retention regulations suffer from the same flaw.

Article 8(2) allows interference. However, it must be for a legitimate aim and necessary in a democratic society.[173] The test of necessity involves deciding whether there is a "pressing social need" for the interference and whether the means employed are "proportionate to the legitimate aim pursued by the State."[174] In conducting such an examination, it is the nature, context and importance of the right asserted and the extent of interference that must be balanced against the nature, context and importance of the public interest asserted as justification.

As the Court mentioned in *Hatton*, states are required to minimize, as much as possible, the interference with the Article 8(2)'s rights by trying to find alternative solutions and by generally seeking to achieve their aims in the least onerous way. Privacy International argues that "Article 8(2)'s limited exception requires that any interference be no greater than is necessary in a democratic society."[175] For a measure "to be proportional, the State must put in place safeguards ensuring that interference with those rights is no greater than necessary."[176] Mandatory data retention laws, according to the Privacy International, "fail on this score as well."[177]

The Government argues that proportionality depends on assessment of three things: "degree of intrusion into an individual's private life involved; strength of public policy justification; [and the] adequacy of the safeguards in place to prevent abuse."[178] The Government should be reminded of its own Guidance, jointly produced with the Bar Council. The proportionality test is defined as follows:

> Even if a particular policy or action, which interferes with the Convention right, pursues a legitimate aim (such as the prevention of crime) this will not justify the interference if the means used to achieve the aim are excessive in the circumstances. Any interference with a Con-

171. 27 *EHRR* 91 (1998).

172. Privacy International, *supra* n. 165 at 9.

173. *Id.*

174. *Id.* at 9-10.

175. *Id.* at 9.

176. *Id.* at 10.

177. Privacy International, *Memorandum of Laws Concerning the Legality of Data Retention with regard to the Rights Guaranteed by the European Convention on Human Rights*, 10, http://www.privacyinternational.org/issues/terrorism/rpt/data_retention_memo.pdf.

178. *Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data*, *supra* n. 47, at 10, ¶ 7.7.

> vention right should be carefully designed to meet the objective in question and must not be arbitrary or unfair. Public authorities must not use a sledgehammer to crack a nut. Even taking all these considerations into account, interference in a particular case may still not be justified because the impact on the individual or group is just too severe.[179]

Simply, the means must not be arbitrary or unfair and excessive in the circumstances. The impact on the individual or group must not be too severe. It can be argued that the data retention measures, which involve the generalized and systematic surveillance of electronic communications of all users, can be arbitrary, unfair and excessive. It is also disproportionate. The impact on society is also too severe because the states can now lawfully require blanket surveillance of the electronic communication of the entire population. Arguably, the data retention regime may not be able to survive the proportionality test.

The Court in *Kopp* held unanimously that there had been a violation of Article 8.[180] The concurring opinion of Judge Pettiti deserves attention:

> It is regrettable fact that state, para-state and private bodies are making increasing use of the interception of telephone and other communication for various purposes. In Europe so-called administrative telephone monitoring is not generally subject to an adequate system or level of protection. . . . The European Court has clearly laid down in its case law the requirement of supervision by the judicial authorities in a democratic society, which is characterized by the rule of law, with the attendant guarantees of independence and impartiality; this is all the more important in order to meet the threat posed by new technologies. . . . Where monitoring is ordered by a judicial authority, even where there is valid basis in law, it must be used for a specific purpose, not as a general 'fishing' exercise to bring in information. . . . The legislation of numerous European states fails to comply with Article 8 of the Convention where the telephone tapping is concerned. States use - or abuse - the concepts of official secrets and secrecy in the interests of national security, where necessary, they distort the meaning and nature of that term. Some clarification of what these concepts mean is needed in order to refine and improve the system for the prevention of terrorism.[181]

VII. CONCLUSIONS

The road ahead seems to be difficult for the retention of communications data. The resistance against it started as soon as the Directive was

179. The Human Rights Act 1998: Study Guide, at ¶ 3.8-9.

180. *Kopp v. Switzerland*, [1998] European Ct. of Human Rights 23224/94 (Mar. 25, 1998).

181. *Id.* (Pettiti, J., concurring).

initiated. The GILC managed to collect 16,000 signatures against it in only a matter of days. The resistance has, overwhelmingly, been growing since then. The criticisms from many different groups and the reasons are various and numerous. This shows that data retention is, indeed, a critical and delicate issue. It affects and impacts, significantly, directly or indirectly, individuals, society as a whole, industry and e-commerce. Data retention legal regimes may be contested as contravening the fundamental rights under Article 8(1) of the ECHR and it may not be justified under Article 8(2). Obviously, and logically, all these views, comments and findings are too important to be ignored by the governments in the EU and elsewhere.

It is all about striking the balance between the right of society to be protected from crime and terrorism against the right of society and the entire population to privacy and to be free from constant surveillance. In this respect, it is even arguable whether Article 8(2) can be relied upon by the state to justify the data retention legislation.

The authorities may make a claim along the lines that 'only the guilty have to fear' Perhaps, this is a misunderstanding of the meaning of privacy. Privacy is about the right of individuals to go about their lawful activity without interference. Privacy is also the fundamental element for the activities on the Internet.[182] Data retention will probably undermine the use of the Internet and many might be migrating out of cyberspace. As one commentator stated:

> The negative impact of data retention is going to fall on the 95% of users who are mainly honest while the 5% of the hardcore criminals are clearly finding ways evading it. While most of the population is going to have all their online actions potentially traced it will be trivial for crooks to steal phone, hack into computers or a PBX, or use other techniques to protect their communications. At the same time, retention legislation will increase the cost of running the Internet related services, penalize new technologies, criminalize providers or users who do not wish to keep logs of everything, and seriously undermine the public's perception of the Internet and information technologies as a whole.[183]

If the UK and Europe are to fulfill the Lisbon objectives of 'becoming the most dynamic, competitive, knowledge based economy in the world', the Internet and communications users must feel confident that their privacy is both respected and protected.

---

182. *E.g.* World Summit on the Information Society, *Declaration of Principles*, 5, http://heiwww.unige.ch/~clapham/hrdoc/docs/worldinfodecl.pdf (Dec. 12, 2003) (regarded strengthening the trust framework, which includes privacy, as a prerequisite for the development of the Information Society and for building confidence among user of ICTs).

183. George Danezis, *Comments on the EU Cybercrime Forum: Technical Issues Around Data Retention*, http://www.cl.cam.ac.uk/~gd216/RetentionComments.pdf (accessed July 28, 2004).