RETENTION OF COMMUNICATIONS DATA: SECURITY VS PRIVACY

by Abu Bakar Munir

I. Introduction

The EU Electronic Privacy Directive 2002[1] requires Member States to ensure the confidentiality of communications. It prohibits listening, tapping, 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, defence, 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 has been 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.[6] Article 15 of the 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]

II. The Emergence of the Electronic Privacy Directive

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 extending the protections that were already in place for telecommunications to a broader, more technology-neutral category of 'electronic communications.'[9] 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.

---

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

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 favour of the Council's position.[10]

The initiatives, in fact, began immediately after September 11. Nine days after the tragic event, the European Commission requested the Council of the EU 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.[11] 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 and for legal enforcement authorities to have access to it "for the purposes of criminal investigations."[12] Only two weeks before this request, 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.[13]

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 EU consider data protection issues in the context of law enforcement and counter-terrorism imperatives and to revise draft privacy directive that call for mandatory destruction to permit the retention of critical data for a reasonable period.[14] 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.[15]

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

---

10. *Id.* at 12.
11. 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.html (accessed July 28, 2004).
12. *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).
13. 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)).
14. 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.
15. 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).

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 billing purposes - and thereby seriously hamper public safety".[16]

III. Data Retention : The Legal Framework in the UK

The Anti-Terrorism, Crime and Security Act 2001 ("ATCSA"), in Part 11, is specifically dedicated to the retention of communications data.[17] Sections 102-107 give power to the Secretary of State to ensure that communications providers retain data.[18] 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.[19] 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.[20]

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.[21]

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.[22] He is specifically required to consult with the Information Commissioner and with communication service providers to whom the code will apply.[23] He is then to lay the draft code before Parliament.[24] The code is to be brought into force by statutory instrument, which is to be approved by Parliament under the affirmative resolution procedure.[25]

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.[26] 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.[27] 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.

---

16. Department of Justice Canada, *G8 Statement on Data Protection Regimes*, http://canada.justice.gc.ca/en/news/g8/doc5.html (Feb. 2, 2004).
17. *See* Anti-terrorism, Crime and Security Act ss 102-107 (2001) [hereinafter ATCSA].
18. *Ibid.*
19. *Id.* at s 102(1).
20. *Id.* at s 102(2).
21. *Id.* at s 102(3).
22. *Id* at s 103(1).
23. *Id.* at s 103(2).
24. *Id.* at s 103(4).
25. *Id.* at s103(5), (7).
26. *Id.* at s 102(4).
27. *Id* at s 102(5).

In the event that voluntary scheme fails, section 104 of the ATCSA empowers the Secretary of State to issue a direction.[28] 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.[29] 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.[30] Such an order may only be made for the statutory purposes prescribed in section 102(3).[31] 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.[32]

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. Meanwhile, 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.[33]

IV. Criticism

The Electronic Privacy Information Centre ("EPIC") argues that the implementation phase of the data retention provision may become bumpy in many EU countries:[34]

> "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[35] with respect to fundamental rights, such as the presumption of innocence, right to privacy, confidentiality of communications and freedom of expression.[36]

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

---

28. *Id.* at s 104.
29. *Id.* at s 104(1).
30. *Ibid.*
31. *Ibid.*
32. *See* ATCSA s 104(4).
33. Ben Emmerson QC & Helen Mountfield, *Anti-Terrorism, Crime and Security Act 2001: Retention and Disclosure of Communications Data: Summary of Councils' Advice*, para 4, http://www.privacyinternational.org/countries/uk/surveillance/ic-terror-opinion.html (accessed Apr. 30, 2004).
34. Electronic Privacy Information Center, *Data Retention*, http://www.epic.org/privacy/intl/dataretention.html (last updated Mar. 25, 2004).
35. 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.
36. Electronic Privacy Information Center, http://www.epic.org/privacy/intl/dataretention.html

conventions and case law."[37]

The Data Protection Commissioners in the EU and their officials, who attended a multitude of working parties meetings have long been aware of the data retention initiative.[38] Their spring conference 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.[39]

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."[40]

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.[41] 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."[42] 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.[43] The ICC has issued a policy statement to warn governments against the emerging traffic data retention laws.[44] It recommends that governments should favour "targeted data preservation over data retention regimes."[45]

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.[46] The EuroISPA and USISPA argue that:

---

37. *Ibid.*
38. Statewatch, *EU Governments to Give Law Enforcement Agencies Access to All Communications Data*, http://www.statewatch.org/news/2001/may/03Benfopol.html (accessed Apr. 29, 2004).
39. *Ibid.*
40. *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).
41. *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).
42. *Ibid.*
43. *Ibid.*
44. 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).
45. *Id.* at 1.
46. *EUROISPA and USISPA Position on the Impact of Data Retention Laws on the Fight Against*

> Mandatory data retention is an extreme step. Governments have not sufficiently demonstrated that the absence of mandatory data retention 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.[47]

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.[48] They argue that mandatory data retention by ISPs – for which there is no business purpose – would impose serious technical, legal and financial burdens on them.[49] 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.[50]

The EuroISPA and USISPA further 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.[51]

The All Party Internet Group ("APIG") in its 2003 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.'"[52] It 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 conclusion than to recommend that the Home Office immediately drop their plans to introduce a voluntary scheme for data retention under ATCSA.[53]

Mandatory data retention scheme, according to the APIG, will do immense harm to the industry and will not actually achieve the results wished for by Law Enforcement.[54] It does not believe that it is practical to retain all communications data on the off chance that it will be useful one day.[55] It believes that the moves in other EU states towards a data retention policy are entirely mistaken. It urgently recommends that the Government enter into Europe-wide discussion to dismantle data retention regimes and to ensure that data preservation becomes EU policy.[56]

The FIPR believes that the creation of warehouses of communications data will lead to

---

Cybercrime, http://www.euroispa.org/docs/020930eurousispa_dretent.pdf (Sept. 30, 2002).

47. *Ibid.* (emphasis original).
48. *Id.* at 2.
49. *Ibid.*
50. *Ibid.*
51. *Ibid.* at 1, 3.
52. *Id.* at 20, para 134.
53. *Id.* at 22, para 141.
54. *Id.* at 27, para 177.
55. *Ibid.*
56. *Ibid.*

significant abuses of the individual's rights.[57] It argues that "it is predictable that excuses will be found to trawl through them looking for patterns of behaviour 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."[58]

V. Privacy vs. Security

The Home Office, in recognising 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 detecting crime."[59]

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.[60] This means that where it "can achieve improvements in services or efficiency without requiring more information and affecting personal privacy, it should do so."[61] The Government pledges that it will consider alternative approaches that have a lesser impact on privacy in achieving the objectives.[62] After all, the protection of privacy, according to the Government, is in and of itself a public service.[63]

"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."[64] "Measures against terrorism should not and need not reduce standards of protection of fundamental rights which characterises 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."[65] "There is an increasing tendency to represent the protection of personal data as a barrier to the efficient fight against terrorism."[66] As stated by the EU Working Party, "terrorism is not a new phenomenon and cannot be qualified as a temporary phenomenon."[67] And legislation is not the only weapon in the counter-terrorism armory, nor is it the most important.

In considering data retention measures, regard must be had to the fair balance that has to

---

57. *See* FIPR's comments submitted to the APIG inquiry, 2, http://www.apig.org.uk/fipr.pdf (accessed Oct. 29, 2004).
58. *Ibid.*
59. 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).
60. 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)).
61. *Id.* at 5.
62. *Id.* at 6.
63. *Id.* at 5.
64. 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)).
65. *Id.* at 4.
66. *Ibid.*
67. *Id.* at 3.

be struck between the competing interests of the individual and of the community as a whole. In striking the required balance, the Court in *Hatton v. U.K.*,[68] held that the states must have regard to the whole range of material considerations:

> States are required to minimise, 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, in reality, strike the right balance should precede the relevant project.[69]

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 minimise any interference with the rights of Article 8 is important. It must be emphasised 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. Legal Challenge

The EU network of independent experts in fundamental rights ("CRF-DF") 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.[70] 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.[71] In other words, the increase in security is not inversely proportional to the restriction of freedom; on the contrary, certain practices minimise the scope of restrictions on fundamental rights whilst offering a high level of effectiveness.[72] 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 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.[73]

Article 15 of the Electronic Privacy Directive allows data retention measures where

---

68. [2001] European Ct. of Human Rights 36022/97 (Oct. 2, 2001) (available at [2001] ECHR 36022/97).
69. *Id.*at para 97
70. 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).
71. *Ibid.*
72. *Id.* at 10.
73. *Id.* at 52.

"necessary, appropriate, and proportionate" within a democratic society.[74] The Directive only permits retention measures if these conditions could be satisfied within a democratic society. The Member States *may* take legislative measures providing for data retention only if is necessary, appropriate and proportionate.[75] It is imperative for the government to demonstrate that data retention satisfies 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.[76]

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.[77] In the leading case of *Niemitz v. Germany*,[78] the court pronounced that respect for private life must also comprise, to certain degree, the right to establish and develop relationships with other human beings. The Court in *Z v. Finland*[79] has asserted that the protection of personal data is of fundamental importance of a person's enjoyment 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.[80] 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.[81] 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."[82] Simply, the Government sees proportionality in the context of retention periods. The real issue is not so much on the retention periods, but whether the laws 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

---

74. *Directive on Privacy and Electronic Communications*, 2002/58/EC at Art. 15. (July 12, 2002).
75. *Ibid.*
76. 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).
77. Lord Lester of Herne Hill & David Pannick, *Human Rights: Law and Practice* (1999).
78. 16 European Human Rights Rep., para 29 (1992).
79. 25 European Human Rights Rep. 371, para 95 (1998).
80. 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.
81. *Id.* at 10, para 7.7 (emphasis added).
82. *Id.* at 10, para 7.8.

be clearly disproportionate and therefore unacceptable in any case."[83]

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.[84] Article 8(2) has been given a narrow interpretation. The European Court of Human Rights in the case of *Klass v. Fed. Republic of Germany*[85] 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*."[86]

'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.[87] The Court in the case of *Amann v. Switzerland*[88] reiterated this requirement of quality of law and held that the legal basis must be accessible and foreseeable. 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*.[89]

The Court in *Kopp v. Switzerland*[90] 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.[91] 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.[92] 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."[93] 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 minimise, 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

---

83. *Supra* n. 41.
84. 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).
85. 2 European Human Rights Rep. 214 (1979).
86. *Id.* at 231.
87. Privacy International, *op cit.*
88. 30 European Human Rights Rep. 843 (2000).
89. *Supra* n. 84 at 8-9
90. 27 *EHRR* 91 (1998).
91. *Supra* n 84 at 9.
92. *Ibid.*
93. *Id.* at 9-10.

argues that "Article 8(2)'s limited exception requires that any interference be no greater than is necessary in a democratic society."[94] For a measure "to be proportional, the State must put in place safeguards ensuring that interference with those rights is no greater than necessary."[95] Mandatory data retention laws, according to the Privacy International, "fail on this score as well."[96]

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."[97] 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 Convention 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.[98]

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 generalised 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.[99] 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

---

94. *Id.* at 9.
95. *Id.* at 10.
96. 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/dataretentionmemo.pdf
97. Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data, para 7.7.
98. The Human Rights Act 1998: Study Guide, at para 3.8-9.
99. *Kopp v. Switzerland*, [1998] European Ct. of Human Rights 23224/94 (Mar. 25, 1998).

order to refine and improve the system for the prevention of terrorism.[100]

VIII. Conclusions

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, the views, comments and concerns of all stakeholders are too important to be ignored.

The right balance to be struck is between the right of the society to be protected from crime and terrorism on one hand and the right of the society and entire population to privacy and to be free from constant surveillance on the other. 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.[101]

100. *Ibid.* (Pettiti, J., concurring).

101. *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).

The Politics of Transborder Data Flows: Competing Values, Interests, and Institutions

Andreas Busch
Dept. of Politics and International Relations
University of Oxford
andreas.busch@politics.ox.ac.uk
http://users.ox.ac.uk/~busch

Paper presented at the conference
"Safety & Security in a Networked World:
Balancing Cyber-Rights & Responsibilities"

Oxford Internet Institute, 8.–10. September 2005

Abstract

Contrary to initial hopes, the increased economic, social-cultural and political importance of cyberspace has led to substantial state regulation of it. Since nation states are still the dominant force here, the regulation of transborder data flows requires the cooperation of nation states which encounters many difficulties.
These problems can be analysed along two dimensions: on the one hand, there are competing interests in the field of transborder data flows: economic interests centre on issues like cost-effectiveness; safety interests focus on the reduction of risk and the prevention of misuse; and civil liberty interests call for the upholding of privacy and freedom of information. On the other hand, national environments differ considerably, especially with respect to the values that inform political debate; the direction and mobilisation of interests; and the existence of institutions in relevant areas such as data protection.
This paper uses these two dimensions to analyse two illustrative cases: one is the "Safe Harbor" agreement between the U.S. and the EU that was meant to provide a framework for firms in the face of different standards of private sector data protection between the two areas; the other is the recent dispute between the U.S. and the EU about the transmission of airline passengers' personal data. The paper argues that these cases demonstrate that initial expectations for a "policy transfer" of EU privacy standards to the U.S. did not materialise, and that differences in institutions and underlying values can largely account for this.