Anti-Terrorism Laws and Data Retention: War is over?

by

Clive Walker* **and Yaman Akdeniz****

Citation: (2003) *Northern Ireland Legal Quarterly*, 54(2), Summer edition, pp 159-182.

Contact: lawya@cyber-rights.org for further information about this article.

* Professor of Criminal Justice Studies, Department of Law, University of Leeds. An earlier version of this paper was presented by to the South East Conference of the American Association of Law Schools, Kiawah Island, South Carolina, July 2002 by invitation of Professor Russ Weaver, University of Louisville.

** Lecturer in Cyberlaw, Department of Law, University of Leeds.

NILQ page 159

Abstract:

The Anti-Terrorism, Crime and Security Act 2001 signals a determined response to the attacks of September 11th. One aspect involves the facilitation of the use of electronic surveillance in order to prevent, detect or prosecute the perpetrators of terrorism. The role of Part XI of the 2001 Act is to augment existing surveillance powers in the Regulation of Investigatory Powers Act 2000. This papers plots the relationships between those two statutes and also their relationship to data protection laws. Delays and difficulties in enforcement are noted and are related to a process of return to greater normality after an initial period of panic.

Cyberspace under investigation

Several deeply-seated factors have tended to impel policing agencies in late modern societies towards a focus on communications data. One concerns the reliance of society on such technology and therefore its augmented vulnerability to attack. This feature is reflected in changes to the definition of 'terrorism'. Section 1 of the Terrorism Act 2000 explicitly encompasses:[1]

'(2) Action ... if it ...

(e) is designed seriously to interfere with or seriously to disrupt an electronic system.'

The enhanced perception of the vulnerabilities of networks to terrorist attack has also resulted in the appointment within the Cabinet Office of a Central Sponsor for Information Assurance and Resilience[2] and the creation of a National Infrastructure Security Co-ordination Centre (NISCC), an interdepartmental organisation set up to co-ordinate and develop existing

NILQ page 160

work within Government departments and agencies and bodies in the private sector to defend the Critical National Infrastructure against electronic attack.[3]

As well as a defensive stance, communications data also elicit an offensive disposition in the form of techniques of surveillance. Reasons for this development include that information technologies have developed enormously and pervade the economies and societies in western states.[4] Their uses are both for good and ill, the latter being the subject of policing.

---

1 For a discussion of the definition in section 1, see: C. Walker, *The Anti-Terrorism Legislation* (Oxford: Oxford University Press, 2002).

2 Defence Committee, Defence and Security in the United Kingdom (2001-02 HC 518) para.125.

3 See further <http://www.niscc.gov.uk/>. Note also the activities of the Communications-Electronics Security Group (CESG) at <http://www.cesg.gov.uk/>.

4 See Y. Akdeniz, C. Walker, and D. Wall, *The Internet, Law and Society* (London: Longman, 2000).

The technologies provide both a new site for policing[5] and quasi-policing[6] regulatory activity and also furnish a variety of opportunities for surveillance which would not previously have been feasible but which also raise significant privacy concerns.[7] They may allow 'investigators for example to establish links between suspected conspirators (itemised bill) or to ascertain the whereabouts of a given person at a given time, thereby confirming or disproving an alibi (cell site analysis)'.[8] The trend next represents part of a fundamental switch away from the reactive and overt policing of incidents to the proactive and covert policing and management of risks,[9] which may either take the form of people (such as 'target criminals')[10] or sites of activity such as the perennial panics about internet chat rooms and their use by paedophiles.[11]

In line with these impulses towards greater police attention to information and communications technologies, the National Hi-Tech Crime Unit (NHTCU) was launched within the National Criminal Intelligence Service in April 2001.[12] The NHTCU is tasked with the key role in the response to cyber-crime, especially as practised by serious and organised crime. The NHTCU comprises of four main divisions - Investigation, Intelligence, Support and Forensic Retrieval.

NILQ page 161

Given the process of the 'hollowing out' of the late modern state,[13] one cannot expect that all the data of interest to the forces of law and order will conveniently be held by compliant public authorities. Rather, a great deal of computer and communication data will be in the clutches of the private Communications Service Providers (CSPs), who sign up

5 It is estimated that around 500,000 mobile phone records are checked by the police each year: *The Independent* 21 December 2002 4; Philips, E., 'Mobile phone – friend or foe?' (2002) 42 *Science & Justice* 225. The All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group (January 2003, <http://www.apig.org.uk/APIGreport.pdf>, paras.9, 10) suggests requests for communication data are closer to a million per year (mainly relating to subscriber data) but emphasises that fewer requests by far are made to Internet Service Providers.

6 See especially the activities of the Internet Watch Foundation (<http://www.iwf.org.uk/>).

7 See C. Dandeker, *Surveillance, Power and Modernity* (Cambridge: Polity Press, 1990); D. Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Cambridge: Polity Press, 1994); S. Davies, *Big Brother: Britain's Web of Surveillance and the New Technological Order* (London: Pan, 1996); D. Banisar, *Privacy & Human Rights: An International Survey of Privacy Laws and Developments* (Washington DC: EPIC, 2000).

8 Home Office, Regulatory Impact Assessment: Anti-terrorism, Crime and Security Bill (London, 2001).

9 See R.V. Ericson, and K.D. Haggerty, *Policing the Risk Society* (Oxford: Clarendon Press, 1997).

10 See <http://www.ncis.gov.uk/business.asp>.

11 The issue was immediately raised, for example, in the case of the disappearance Jessica Chapman and Holly Wells in Soham: *The Times* 10 August 2002 7.

12 See NCIS Press release 18/010.

customers in return for communication services such as home phone and mobile phone connection and related services such as Wireless Application Protocol (WAP) and General Packet Radio Service (GPRS), e-mail and Internet access and facilities. At the same time as this proliferation of communications access is viewed as a positive trend from the point of view of the establishment of the information society,[14] the abundance of nodes of entry can become a negative trend from the law enforcement perspective. Not only may it result in greater complexities in terms of locating the relevant network and database on which to track down the desired information, but also it may mean that there is nothing to be discovered at the end of the day because customer and financial pressures on fiercely competitive CSPs demand that data be shed as soon as possible. According to the Home Office's Regulatory Impact Assessment: Retention of Communications Data in 2001:[15]

> 'Changes to the business model are leading to a reduction in the amount of data which is needed for billing purposes (e.g. pre-pay/ subscription/ "always on"). Combined with pressure from the privacy lobby, this is leading to a decrease in data retention overall.'

Leading policing and security agencies have pondered for some time how to react to the new challenges of cyberspace. The attacks of September 11th 2001 on the World Trade Centre, New York and the Pentagon, Washington DC, reinforced by subsequent apprehensions about assaults by anthrax and other horrifying weapons of mass destruction, constructed a compelling trigger for action both by policy-makers and legislators. In the months that ensued, there was a readiness to enact virtually any measure which was conceivably related to 'the first war of the twenty-first century'[16] conjured by US President Bush against terrorism and many which were not even claimed to be vaguely connected. However, it is the contention of this article that the first phase of official reaction to September 11th which afforded such indulgence has passed and that there has been a partial re-establishment of earlier legal stances in relation to terrorism, which emphasise the rule of law and policing models, rather than derogation and military models, though without allaying concerns about privacy rights. This trend is evidenced by the development of the law providing for the retention of communications data both before and after September 11th.

---

13 See B. Jessop, 'Post-Fordism and the State' in A. Amin, (ed.), *Post-Fordism: A Reader* (London: Blackwell, 1994) 251.

14 See Y. Akdeniz, C. Walker, and D. Wall,, *The Internet, Law and Society* (Longman, London, 2000) chap.1.

15 *Loc. cit.* para.6.

The enactment of Part XI of the Anti-terrorism, Crime and Security Act 2001

Part XI of the Anti-terrorism, Crime and Security Act 2001 seeks to ensure that CSPs will retain communications data for an investigatory rainy day.[17] The data must be held for a specified period. If access for investigatory purposes is actually required, attention must then be turned to the Regulation of Investigatory Powers Act 2000 ('RIPA 2000'), since the Anti-terrorism, Crime and Security Act 2001 itself grants no further provisions about access, disclosure or utilisation.

Despite this limit, Part XI was criticised as excessive during its passage. Whilst confined to 'communications data', the effect can be to provide a complete dossier on private life - who you contact, what are your interests and habits and where you are and have been – like a CCTV inside your head, as one commentator put it.[18] The measure suggests a certain failure on the part of those authorities tasked to collect focused intelligence so as to combat terrorism, with the result that the entire population must be treated as potentially suspect. Part XI may have been easier to stomach if designed around the concept of 'terrorist investigations' under section 32, but the current text is explicitly wider and encourages mass snooping, and like other parts of the Act,[19] it betokens earlier and wider origins than the combating of terrorism.

Taking up the last point, Part XI was not entirely devised after September 11th. The idea may probably be traced to lobbying from the National Criminal Intelligence Service (on behalf of the police, HM Customs and Excise, the Security Service, Secret Intelligence Service and GCHQ) as the next step on from the passage of the Regulation of Investigatory Powers Act

---

16 *The Guardian* 14 September 2001 5.

17 See generally House of Commons Research Paper on Communications Data: Access and Retention, 02/63, 21 November 2002.

18 C. Bowden, 'CCTV for inside your head' (2002) 8 *Computer and Telecommunications Law Review* 21. Even the Home Office admits that 'a detailed profile' can be compiled: Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003, para.5.2.

19 The criticism was directed, for example at Parts III (relating to the disclosure of information held by government department and agencies) and X (relating to extended powers granted to the Ministry of Defence Police and British Transport Police). See: C. Walker, *The Anti-Terrorism Legislation* (Oxford: Oxford University Press, 2002) chaps.4, 9; Northern Ireland Select Committee, The Financing of Terrorism in Northern Ireland (2001-02 HC 978) para.119.

2000[20] and to ensure that it will be effective in implementation. It is alleged that those agencies called for communications data to be retained by CSPs for a minimum period of 12 months and then to be archived, either in-house or by a Trusted Third Party agency or contractor, and retained for a further six-year period.[21] According to their Report, the retention of communications data has great value to law enforcement:

NILQ page 163

> '1.2.1 Communications data is crucial to the business of the Agencies. It is pivotal to reactive investigations into serious crime and the development of proactive intelligence on matters effecting not only organised criminal activity but also national security. At the lower level, it provides considerable benefit to the detection of volume crime. ... Short term retention and then deletion of data will have a disastrous impact on the Agencies' intelligence and evidence gathering capabilities.
>
> 1.2.2 Communications data is becoming increasingly important to provide evidence to establish innocence. Premature deletion will seriously compromise the interests of justice. Communications data has a unique value to promoting a safe and free society. This provides the overriding justification for longer-term retention.'

This progeny is officially denied.[22] However, conspiracy theories seem to be abound in this field, and a further allegation is that the retention of communications data was alleged to be part of the demands for enhanced security written by the US President to the European Commission President Romano Prodi on the 16 October 2001, including the call for the moderation of data protection principles 'in the context of law enforcement and counter-terrorism imperatives'.[23]

In detail, Part XI establishes that, under section 102, the Secretary of State can issue a voluntary code of practice[24] relating to the retention of 'communications data' by 'communications providers' (by section 107, meaning a person who provides a postal service or a telecommunications service). No distinction is made between public and private

---

20 See Y. Akdeniz, N. Taylor, and C. Walker, 'Regulation of Investigatory Powers Act 2000: Bigbrother.gov.uk' [2001] *Criminal Law Review* 73.

21 R. Gaspar, NCIS Submission to the Home Office; Looking to the Future: Clarity on Communications Data Retention Law (see <http://cryptome.org/ncis-carnivore.htm>, 2000) para.6.

22 House of Lords Deb. vol.629 col.770 4 December 2001, Lord Rooker.

23 <http://www.statewatch.org/news/2001/nov/06uslet.htm>; W. Malcolm, and D. Barker, 'Privacy and surveillance' (2002) 152 *New Law Journal* 80, 81.

24 A draft code has been published for consultation in March 2003: Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003.

communication service providers,[25] such as the United Kingdom universities' JANET network[26] or the Parliamentary Data and Video Network,[27] though one hopes that purely domestic networks operated for personal, family or household affairs will be exempt.[28] 'Communications data' has the same interpretation as in section 21(4) in Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000, which means it is data relating to the mode and nature of telephone, Internet and postal communications (traffic, service, and subscriber data), but it is not meant to include the contents of the

NILQ page 164

communications itself. This distinction is thought to be fallible in the case of Internet data:[29]

> 'Knowing the numbers dialled by an individual may yield useful information to the authorities but does not, by itself, reveal the content of the conversations which took place. However, if you have access to the clickstream, you can ascertain the content of everything that the target has read, viewed or downloaded. And because everything is in digital form, the whole process can be automated. The algorithm goes like this: read the URL; fetch the page; parse the content; decide whether content matches certain criteria; store decision; read next URL. A five-year-old could write the code to do it.'

The Telecommunications (Data Protection and Privacy) Regulations 1999[30] currently regulate the retention of such data by communication service providers but do so from the opposite, restrictive approach to Part XI. Such data can only be retained for certain specific commercial purposes such as to send a bill to a customer and ensure legal enforcement where necessary (regulation 7), otherwise it must be erased or made anonymous. Whilst the Regulations (regulations 32 and 33) permit the retention of communications data on national security and crime prevention grounds, there is currently no general guidance as to where these

---

25 House of Lords Deb. vol.629 col.756 4 December 2001, Lord Rooker.

26 <http://www.ja.net/>.

27 <http://www.adaptwestminster.co.uk/html/HoCDepts/PDVNGuidInfo.htm>.

28 This is the current intention: Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003, Annex A, para.13.

29 J. Naughton, 'Take a tip m'lord - save cookie talk for teatime' (2000) *The Observer* 18 June (<http://www.guardian.co.uk/Archive/Article/0,4273,4030723,00.html>).

30 S.I. no.2093. These Regulations implement Directive 97/66/EC of the European Parliament and the Council concerning the processing of personal data and privacy in the telecommunications sector. It is intended to replace by 31 October 2003 this Directive by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

might apply or for how long.[31] Several Data Protection Principles in the Data Protection Act 1998, including the First (having a legitimate basis for processing), Third (to ensure that data are relevant and not excessive in relation to the purpose for processing) and Fifth (a data controller should not hold personal data for longer than necessary for its own purpose for processing the data) would almost certainly forbid the blanket storage of logs recording such details as web-sites browsed or e-mail addresses. Other data, such as the length of the link to the CSP, may be kept so long as relevant to billing or fraud control, as permitted by the Telecommunications Regulations of 1999. The need for retention of data would be judged against the continued necessity for the business purposes of the CSP such as for sending out a bill, dealing with a disputed matter or ensuring the security of its network. Whilst national security or crime prevention purposes may empower the retention of data beyond these in-house purposes under sections 28 and 29 of the Data Protection Act 1998 under exceptional circumstances, they certainly do not place the CSP under a duty to retain on the chance that such a purpose will arise.[32] In practice,

NILQ page 165

while some CSPs already keep data for a year or more (and have therefore expressed some acceptance of these measures),[33] others delete it just days after the traffic has occurred and so would incur costs to adopt other practices for law enforcement purposes only.

---

31 In the case of national security requirements under regulation 32, there is also the difficulty that a cumbersome Ministerial certificate has to be issued.

32 Applications for access under the Data Protection Act 1998 are also considered unsatisfactory since the legislation grants a privilege against subject action for disclosure of their data, but it does not impose any duty to comply with the requests of law enforcement agencies (see All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, at http://www.apig.org.uk/APIGreport.pdf, para.59). There is the further problem that a request granted by a compliant data user might then become disclosable to the data subject. The Regulation of Investigatory Powers Act 2000 Chapter 1 Part II would provide for enforceable and secretive requests but is not yet in force. It should be noted that access under compulsion may in the meantime be obtained under a variety of legislation, the most notable of which is the Police and Criminal Evidence Act 1984 ss.8, 9, but which also includes the Charities Commission Charities Act 1993, the Environment Agency Environmental Protection Act 1990, the Health & Safety Executive Health & Safety at Work etc Act 1974, the Inland Revenue Taxes Management Act 1970, the Radiocommunications Agency Wireless Telegraphy Act 1974, the Telecommunications Act 1974, the Serious Fraud Office Criminal Justice Act 1987, the Social Security Investigators Social Security Administration Act 1992, and the Trading Standards Officials Consumer Protection Act 1987 (see All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, <http://www.apig.org.uk/APIGreport.pdf>, para.104).

33 Internet Service Providers Association (ISPA) Council Statement, <http://www.ispa.org.uk/html/statement_2510dp.htm> , 26 October 2001.

In the light of this varied practice, Part XI and the envisaged code of practice[34] will give guidance to CSPs as to the basis for retaining on national security and crime prevention grounds communications data beyond the period that they require it for their own business purposes. Once finalised, the code of practice will apply to communications data that the CSPs have generated or otherwise possess. Further agreements[35] with specific CSPs (especially those with direct access to the Internet structure rather than those renting from the major half dozen operators) will afford greater detail as to the type of data to be retained and the conditions of retention and state subventions.[36] This partnership approach followed a meeting, on 24 October 2001, involving representatives of the Home Office and the Department of Trade and Industry, the Internet Services Providers Association (ISPA), the London Internet Exchange (LINX), the CBI and telecommunications companies. The sector as a whole comprises around 280 public telecommunications operators, 570 international simple voice resale providers and 300 Internet Service Providers.[37]

The core measure of Part XI is in section 102(3), by which the code and any agreements may contain provisions necessary to safeguard national security or for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security,

NILQ page 166

additional to, and without prejudice to, the communication provider's own business purposes. The width of the purposes should be noted. It was said to be impractical to limit the measure to terrorism data[38] and a House of Lords amendment to this effect was reversed.[39] An amendment in the dying stages of the Parliamentary process, up against the deadline of the Christmas recess and without time for full debate,[40] added the words 'which may relate directly or indirectly to national security' to the purpose of prosecution, but the permissive 'may' does not absolutely delimit the purposes (albeit that the Government opposed the amendment). In addition, the retention of data will only be accomplished on a blanket basis, so retained data

34 See Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003.
35 *Ibid.* Appendix B.
36 *Ibid.* Annex A para.20.
37 Home Office, Regulatory Impact Assessment: Retention of Communications Data (2001) paras.21-23.
38 House of Lords Deb. Vol.629 col.774 4 December 2001, Lord Rooker.
39 *Ibid.* col.981 6 December 2001, col.1479, 13 December 2001.
40 *Ibid.* col.1474 13 December 2001.

will be available for access under the Data Protection Act (and other legislation already described and under the Regulation of Investigatory Powers Act 2000 as described below). With his customary charm, Home Secretary David Blunkett explained the government's insouciance as follows:[41]

> 'The amendment, in relation to part 11 therefore suggests that we should try to separate out those parts of data. As I tried to explain on a number of occasions, including last night, it is not possible to do that, but paradoxically, because it is not possible to do it, it is not reasonable to suggest that we should not do it. I am therefore prepared to accept the amendments that have been tabled. In order to be able to implement what they want, we will have to retain the data, so that it can be accessed to test out whether the intelligence services are right in believing that it is relevant in tackling terrorists. That is how stupid the Liberal Democrats are.'

The Government may now seek to justify its stance by comparison with the recent European Union Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).[42] The relevant provision on data warehousing, article 15, allows for (but does not require) the retention of data for a limited period to safeguard national security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the

NILQ page 167

electronic communications system, as referred to in article 13(1) of Directive 95/46/EC. The inclusion of such a provision within the Directive represents a sea-change in data retention policy. It mainly follows the request of the Council of the European Union on 20 September, 2001 from the European Commission to submit proposals 'for ensuring that law enforcement authorities[43] are able to investigate criminal acts involving the use of electronic communications systems and to take legal measures against their perpetrators.'[44] Only two

41 HC Debs. vol.376 col.1111, 13 December 2001.

42 EU Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) of 12 July 2002, Official Journal of the European Communities 31.7.2002, L 201 pp 37-47.

43 Note also Enfopol 55: Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services, 9194/1, Brussels 20 June, 2001.

44 Extraordinary Council meeting, Justice, Home Affairs and Civil Protection, Brussels, 20 September 2001, 12019/01 (Presse 327), para 4.

weeks before this request, on 6 September, 2001, the European Parliament recommended in a resolution that 'a general data retention principle must be forbidden,'[45] and that 'any general obligation concerning data retention' is contrary to the proportionality principle.[46] It is also no secret that the UK government strongly lobbied for the explicit reference to the scope for data retention provisions during negotiations in Council.[47] Despite strong criticism from civil liberties organisations,[48] the communications industry,[49] and Radical Party MEPs,[50] and despite this being a third pillar issue under Title VI of the EU Treaty, a data retention provision was included within article 15 of the new first pillar EU Directive on privacy and electronic communications.

In devising the code under Part XI, there are three stages to be followed under section 103. First, there must be consultation with the CSPs and also with the Information Commissioner (the successor to the Data Protection Commissioner under the Freedom of Information Act 2000). In practice, the Internet Crime Forum,[51] consisting of policing and industry members, played a significant consultative role. Home Office ministers have met twice with

NILQ page 168

45 Strategy for Creating a Safer Information Society (A5-0284/2001), text adopted by the European parliament on 6 September, 2001: Recommendation of the European Parliament on the Strategy for Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (2001/2070(COS)), C 72 E/323-329 Official Journal of the European Communities, 21.3.2002.

46 *Ibid*, paragraph J.

47 See for example House of Commons European Scrutiny Committee Thirty-Second Report, HC 152-xxxii, Session 2001-02, July 2002 (19. DTI (23528) Personal data and privacy in telecommunications).

48 Global Internet Liberty Campaign (representing around 60 public interest organisations) letter dated 22 May, 2002 at <http://gilc.org/cox_en.html>.

49 EuroISPA, ETNO & ECPA, Joint Industry Memo in view of the 2nd Reading of the Cappato Report: The Implications of 'Data Retention' in Article 15.1 of the Common Position on the Electronic Communications Data Protection Directive addressed to the Members of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs. April 16, 2002, at <http://www.euroispa.org/docs/160402_dataretent.doc>.

50 Open letter of Marco Cappato, Radical MEP and EP draftsman on privacy in electronic communications, to the President of the EU Council and to the President of the EU Telecoms Council: the fight against terrorism shall not hinder foundamental freedoms and rights such as the right to privacy, 5 December 2001, at <http://www.radicalparty.org/privacy/lett_cap_e.htm>. See further Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (Rapporteur: Marco Cappato), Recommendation For Second Reading on the Council common position for adopting a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (15396/2/2001 – C5- 0035/2002 – 2000/0189(COD)), A5-0130/2002, 22 April 2002.

the Forum representatives, and on three occasions with the Office of the Information Commissioner to discuss data retention policy between January and March 2002.[52] Second, the code must be published in draft, allowing for public representations; it has at last appeared in this form in March 2003. Once the consultation on the draft is over, the final stage will involve the authorisation of the code by a statutory instrument approved by Parliament.[53]

Under section 106, there may be government payments in order to compensate CSPs (similar to the largesse distributed under the Regulation of Investigatory Powers Act 2000, section 24). The ISPA has estimated costs at around £20m; the Government says at least £9m.[54] Part of the discrepancy may arise because, according to the draft code of practice, where the national security need for retaining data is not substantially different from the business need, retention costs will continue to be borne by the CSPs.[55] A reasonable proportion of the marginal cost as appropriate would be provided by the government only when data retention periods are significantly longer for national security purposes than for business purposes.[56] Phone companies keep detailed records of traffic data in order to calculate customers' bills, and the main provider, BT, retains it for seven years. By contrast, Internet Service Providers do not charge by traffic volume, and so do not need to keep the information that long (AOL retains email traffic data for three months, Freeserve for 90 days and Claranet for two weeks).[57] In the light of this pattern, there is a worry that the burdens will fall upon smaller or niche-market firms and will more widely affect international competitiveness.[58] However, even a major CSP like AOL, which retains data as necessary for billing purposes, fraud prevention or security, has argued at the European Commission level that 'imposing mandatory longer data retention period will not be proportionate, will impose vast costs which will not be in line with business needs'.[59]

---

51 <http://www.internetcrimeforum.org.uk/>. See further its paper on data types: Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003.

52 House of Lords Deb.vol.632 col.143wa 20 March, 2002, Lord Rooker.

53 House of Lords Deb. vol.629 col.1282 11 December 2001, Lord Rooker.

54 Home Office Regulatory Impact Assessment: Retention of Communications Data (2001) para.27.

55 Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003, Annex A para.23.

56 Marginal costs may include, for example, the design and production of additional storage and searching facilities. See *ibid*, para 24.

57 (2001) *The Guardian Online* 15 November.

58 Home Office, Home Office Regulatory Impact Assessment: Retention of Communications Data (2001) paras.9, 10.

It is emphasised that the code will be voluntary, and there are no legal penalties in the 2001 Act for non-compliance, though the code or any specific agreement can be invoked in legal proceedings brought against a communications provider by a person whose communications data they hold. This proviso is intended to prevent a CSP incurring civil liability for storing data in accordance with the code (though, as discussed below, it may not overcome express restraints under data protection laws which may ultimately be interpreted over the heads of UK legislatures and judiciary by the

NILQ page 169

European Court of Justice). Retention for a maximum period of 12 months for subscriber information and telephony data[60] will be required under the provisions of the draft code of practice without prejudice to any longer retention period which may be justified by the business practices of the communications provider.[61] However, communications data may eventually be subject to compulsory retention under European law for 12-24 months[62] according to a draft EU Framework Decision on the retention of traffic data and access to this data in connection with criminal investigations and prosecutions[63] which was drafted by the Belgium presidency and leaked to Statewatch.[64] Under the draft Framework Decision, such retention of traffic data would not be disproportionate in view of the needs of criminal prosecutions as against the intrusion into privacy that such a retention would entail.[65] Terrorism is just one of the possible crimes for which data retention would be required, and the

---

59 AOL and Data Retention, document presented at the EU Cybercrime Forum plenary meeting, 27 November, 2001. See generally <http://cybercrime-forum.cec.eu.int/>.

60 A maximum period of 6 months is required for email data, ISP data, SMS, EMS, and MMS data. On the other hand the draft code requires a maximum retention period of 4 days for web activitiy logs. See Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003, Annex A, Appendix A for further technical details.

61 Home Office, Draft Code of Practice on the Retention of Communication Data under Part XI of the Anti-Terrorism Crime & Security Act 2001, Pre Public Consultation Process Draft Document, August 2002, para 15. See further Home Office Regulatory Impact Assessment: Retention of Communications Data (2001) para.11.

62 Interpol also supports a retention period of 12-24 months for traffic data. Interpol Expert Statement, Overview of vital traffic data necessary for investigations which the European Working on Information Technology Crime asks the general retention by telecommunication operators and telecommunication access and service providers, EU Cybercrime Forum plenary meeting, 27 November, 2001. See generally <http://cybercrime-forum.cec.eu.int/>.

63 Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions, Belgian proposal for Third Pillar legislation, at <http://www.statewatch.org/news/2002/aug/05datafd.htm>.

64 Statewatch Analysis No 11: Surveillance of telecommunications: data retention to be 'compulsory', August 2002, at <http://www.statewatch.org/news/2002/aug/05datafd1.htm>.

65 Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions, Belgian proposal for Third Pillar legislation, para 12.

draft Framework Decision would extend data retention for any serious crime including rape, arson, swindling, and offences under the Council of Europe CyberCrime Convention.[66] One EU member states' competent authority would also be able to access data retained in another member state under the draft Framework decision.[67]

Returning to the 2001 Act, if, 'after reviewing the operation of any requirements contained in the code of practice and any agreements under section 102, it appears to the Secretary of State that it is necessary to do so', then, by section 104, the Secretary of State can issue compulsory directions.

NILQ page 170

So, compulsion can apply if the CSPs 'don't volunteer enough'.[68] Precise criteria on which to judge success of failure are not set out in the Act but were expected to be detailed in the voluntary code of practice (in fact, there is no mention as yet in the current draft).[69] Mandatory directions may apply to all CSPs, a particular type of CSPs, or one or several specific CSPs. Some consultation is again required (including with the CSPs and the Information Commissioner), as well as approval of a statutory instrument by Parliament. Compensation may be payable under section 106. In the event of non-compliance by CSPs, the Secretary of State may bring civil proceedings for an injunction or other appropriate relief.

The absence of criminal sanctions demonstrates how hesitant Parliament felt about the grant of these powers. This apprehension is also evidenced by section 105, by which any mandatory scheme under section 104 will itself lapse after two years (on the 14 December 2003) unless renewed (which can occur more than once) by affirmative order.

The implications of Part XI of the Anti-terrorism, Crime and Security Act 2001

One way or another, many more terabytes of data will have to be stored by CSPs as a result of the threat or operation of Part XI. Yet, it may be doubted whether Part XI will achieve

66 ETS 185, 2001.

67 As far as the implementation of the draft Framework Decision is concerned, member states would be required to comply by 31 December 2003.

68 'The net's eyes are watching', *Guardian Online*, 15 November 2001.

its ultimate objective of providing evidence against nefarious activities for at least two practical reasons.

The first is the doubt whether it can provide convincing evidence of wrongdoing. Though computer evidence is potentially admissible as evidence,[70] traffic data cannot beyond reasonable doubt link a technical occurrence recorded as data to personal identity. In other words, the mobile phone or the e-mail message might be used by an identifiable username but the person making the keystrokes may not necessarily be the username owner.[71] This first doubt is not, however, fatal to the enterprise. Just as with arrests under section 41 of the Terrorism Act 2000 and its predecessors, few police interventions either result in court cases or are intended to do so. The main point of anti-terrorism policing is preventing and countering the threat rather than producing cases to be processed beyond reasonable doubt through courts in the public domain.[72]

The second practical obstacle is that evasion is relatively simple. With standard e-mail programs (such as Pegasus or Microsoft Outlook), the e-mail address and name of the person being contacted is logged by the system and the potentially unique Internet Protocol (IP) address[73] of the sender is

NILQ page 171

revealed. Detection is thereby facilitated by the evidence chain so created. However, the task of law enforcement becomes much more tricky if web-based e-mail systems, such Hotmail, are used. For example, the FBI only discovered that Zacarias Moussaoui, charged as a conspirator in the September 11th attacks, had utilised three Hotmail accounts through his written pleadings in July and August 2002. Amongst the challenges faced by investigators in that case are the initial problem that the identities of account-holders are not verified by Microsoft, the owners

---

69 House of Lords Deb. Vol.629 col.800 4 December 2001, Lord Rooker.

70 P. Sommer, 'Downloads, logs and captures: evidence from cyberspace' (2002) 8 *Computer and Telecommunications Law Review* 21.

71 C. Bowden, 'CCTV for inside your head' (2002) 8 *Computer and Telecommunications Law Review* 21, 21.

72 See C. Walker, *The Anti-Terrorism Legislation* (Oxford: Oxford University Press, 2002) chap.5.

73 Every machine logged into the Internet uses a unique identifying 32-bit binary number, called an IP Address (your own IP address can be readily found by logging into <http://www.anonymizer.com/snoop/test_ip.shtml>). 'Dynamic' IP addresses are often assigned from a pool by CSPs at the start of a customer's log-in, but this is less common with ADSL (cable) connections.

of Hotmail. Provided the account-holder gives a false identity,[74] does not use a traceable IP address (which can be achieved by using an Internet terminal in a public library, Internet cafe[75] or shopping mall) and does not download information to a traceable storage mechanism (a hard-disk or floppy disk),[76] then the usage can remain anonymous. Microsoft can in theory (but refuses as a matter of policy) to trace messages by a combination of IP address and date/time of the message, provided the information has not been erased from its records because an account has been inactive for 30 days. But even that potential path to detection can be defeated by the use of more sophisticated anonymised web browsing systems such as Anonymizer.com. Although the draft Code of Practice will require CSPs to retain communication data that relates to 'subscribers resident in the UK or subscribing to or using a UK-based service…. whether the data is generated or processed in the UK or abroad,'[77] it is relatively easy to set up a foreign POP3 or IMAP e-mail account and then access that account securely by using web based systems like mail2web.com. In this way, the mail will always be stored and accessed in a foreign system, circumventing not only the purpose of data retention but also any e-mail interception power under RIPA 2000.[78] In the main, Part XI is conceived with switched telephony in mind, and it was forlornly admitted by one government minister that 'e-mail is more difficult… I do not fully understand the details of headers and so forth. I have never used hotmail,

NILQ page 172

although I have used Internet and e-mail services.'.[79] So much more likely is it that trained terrorists will know how to cover their tracks. One is therefore left with the worry that the

74 Moussaoui's accounts were called xdesertman@hotmail.com, pilotz123@hotmail.com and Olimahammed2@hotmail.com, with his registered name in one case as Zuluman Tangotango: *US v Zacarias Moussaoui*, Crim. No. 01-455-A, US District Court for the Eastern District of Virginia (Alexandria Division): Government's Response to Court's order on computer and email evidence, <http://news.findlaw.com/hdocs/docs/terrorism/usmouss90402grsp.pdf>, 2002.

75 Moussaoui was a customer of Kinko's (<http://www.kinkos.com/>), a company which also strengthens privacy by wiping the memory of their computers every 24 hours.

76 The http log of the computer used will only show that the site <http://www.hotmail.com> was visited and not any e-mail details.

77 Home Office, Draft Code of Practice on the Retention of Communication Data under Part XI of the Anti-Terrorism Crime & Security Act 2001, Pre Public Consultation Process Draft Document, August 2002, para 12.

78 Within this context see further I. Brown and B. Gladman, 'The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses', <http://www.fipr.org/rip/RIPcountermeasures.htm>, 2000. The Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003, Annex A para.13, accepts that CSPs who store data abroad may not be able to comply with the Code.

79 House of Lords Deb. Vol.629 cols.757, 781 4 December 2001, Lord Rooker.

government was as much engaged in an exercise of flexing muscles against the allegedly anarchic Internet as in actually garnering useful information to combat terrorism.

In the process, and as a further more principled objection, one can expect damage to individual rights, especially respect for individual privacy under article 8 of the European Convention, which expressly applies to communications.[80] In her comments on the Bill, the then Information Commissioner, Elizabeth France, has stated that the proposed provisions 'could have a significant impact on the privacy of individuals whose data are retained' and suffer from a 'lack of proportionality such as to render the prospective legislation incompatible with Convention rights'.[81] Alongside the ethical emphasis on individual autonomy must be set democratic and legal accountability, not easy to square with private power-holders such as CSPs.

Flowing from this principled problem, there are also troublesome legal implications. There is the basic issue of compatibility with the Human Rights Act 1998, which reproduces the requirements of Article 8 of the European Convention. It may be assumed at the outset that CSPs will be treated as 'public authorities' and are thereby within the duties of section 6 of the Human Rights Act 1998 for these purposes. Just as in *R (on the application of Ford) v Press Complaints Commission*,[82] the PCC readily conceded that it was a public authority when enforcing a code of practice recognised by statute (the Human Rights Act, section 12). At first glance, CSPs look to be in a similar position in regard to the enforcement of any codes under Part XI of the Anti-terrorism, Crime and Security Act 2001.[83]

Turning to the substantive legal issue of compatibility, the question is whether Part XI can be justified under article 8(2) 'as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. One might concede that the

---

80 See E.A. Mohammed, 'An examination of surveillance technology and their implications for privacy and related issues' (1999) (2) *Journal of Information, Law & Technology*; P.M. Schwartz, 'Privacy and democracy in cyberspace' (1999) 52 *Vanderbilt Law Review* 1609.

81 Information Commissioner news release, Information Commissioner contributes to scrutiny of anti-terrorism bill, <http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf>, 13 November 2001. See further Information Commissioner's Office press release, Monitoring must be justified, 10 July, 2002.

82 [2001] EWHC Admin 683 para.11.

83 This point has also been raised by B. Emmerson, & H. Mountfield, Advice to the Information Commissioner on ATCSA 2001 Retention and Disclosure of Communications Data, July 2002.

purposes for which the Part XI powers are likely to be used will amount to a *prima facie* legitimate purpose within Article 8(2). A more difficult hurdle is whether the interference will be 'in accordance with the law', given that the instrument for control is a voluntary code of practice. Codes of

NILQ page 173

practice have been viewed in the past as insufficiently clear instruments to guide officials or citizens, most notably in the case of *Malone v United Kingdom*.[84] However, Part XI may be distinguishable in that the code arises under a statutory requirement, and there are legal enforcement powers if it fails.

Even more tricky is that the interference must be 'necessary' and 'proportionate'. The Government could be criticised for promoting new legislation such as the Anti-Terrorism, Crime, and Security Act 2001 and extending its powers before the inadequacy of its existing measures has been established. These include such powers as the acquisition and disclosure of communications data under Part I Chapter II as described above, and the investigation of electronic data protected by encryption under Part III of the Act. While these are yet to be implemented by the government, and their impact to be tested, even more new powers are given to law enforcement agencies under the Anti-Terrorism, Crime, and Security Act 2001. Whether more surveillance will necessarily result in detection and prevention of such terrible crimes happening is debatable. As the Earl of Northesk stated in the House of Lords 'there is no evidence whatever that a lack of data retained has proved an impediment to the investigation of the atrocities on 11th September.'[85]

The issue of the retention of data in another context is currently being litigated in the case of the *R (on application of S) v Chief Constable of South Yorkshire* and *R (on application of M) v Chief Constable of South Yorkshire*.[86] The applicants sought judicial review of the Chief Constable's decision to retain fingerprints and DNA samples taken in the course of a criminal investigation in circumstances where there had been an acquittal or a discontinuance. Though the governing legislation, the Police and Criminal Evidence Act 1984, section 64(1A), as amended by the Criminal Justice and Police Act 2001, section 82, allows for indefinite

84 App.no. 8691/79, Ser A 82, (1984) 7 EHRR 14.

85 House of Lords Debates vol.629 col. 808 4 December 2001. But note the subsequent case of Moussaoui, discussed above, where data retention was one of several issues of concern.

retention even after an acquittal. The applicants argued this provision was incompatible with the right to respect for private life under article 8(1). The Administrative Court rejected the application, viewing section 64(1A) as compatible with article 8 (2) by addressing the pressing social need of the prevention of disorder or crime in a way which was proportionate. The actual retention of information (as opposed to accessing it) was not in any event considered an interference to an individual's right to privacy. Later, the Court of Appeal (Civil Division) did at least accept that the retention of fingerprints interfered with Article 8(1) rights but at the same time concluded that the adverse consequences to the individual were proportionate to the benefits to the public under Article 8(2). The Court also observed (Lord Justice Sedley dissenting) that whilst all citizens were entitled to be regarded as innocent, the differential treatment of those who had been the subject of an unproductive criminal investigation could be consistent with rights against discrimination under Article 14.

NILQ page 174

These interpretations appear rather more grudging than the sweeping approach of the European Court of Human Rights that[87]

> '… states do not enjoy unlimited discretion to subject individuals to secret surveillance or a system of secret files. The interest of a State in protecting its national security must be balanced against the seriousness of the interference with an applicant's right to respect for his or her private life.'

So far as the activities of intelligence services are concerned, the Strasbourg court reiterates that 'powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.'[88] Concerns for national security do not provide a blanket right for secret surveillance of citizens by the state and[89]

> '...in respect of national security as in respect of other purposes, there has to be at least a reasonable and genuine link between the aim invoked and the measures interfering with private life for the aim to be regarded as legitimate. To refer to the more or less indiscriminate storing of information relating to the private lives of individuals in terms of pursuing a legitimate national security concern is… evidently problematic.'

---

86 [2002] EWHC 478, [2002] EWCA Civ 1275.

87 *Rotaru v Romania*, App.no. 28341/95, judgment of 4 May, 2000, concurring opinion of Judge Wildhaber, joined by judges Makarczyk, Türmen, Costa, Tulkens, Casadevall and Weber.

88 See *Klass and Others v. Germany*, App.no. 5029/71, Ser A 28, para.42.

89 *Rotaru v Romania*, loc. cit. concurring opinion.

Although the retention of some data for national security purposes may well be justified under article 8(2) for an extended period of time, that does not necessarily mean that blanket retention is justified[90] or that access to such data under section 22 of RIPA 2000 is justified for any of the wider law enforcement purposes within that section. One may argue that access to communications data retained longer than it is necessary for business purposes is disproportionate and goes much further than pursuing a legitimate national security concern especially for reasons other than national security such as for wider law enforcement purposes under section 22(2) of RIPA 2000 (as described further below).[91] Part XI of the 2001 Act and section 102(3) in particular should have been narrowly tailored to address national security concerns only without providing access to such data under section 22(2) of RIPA 2000 for other law enforcement purposes. In fact, the draft Code of Practice encourages relevant public authorities under Chapter II of Part I of RIPA 2000 by stating that 'it is outside of the scope of this code of practice to address the issue of acquisition of data after it has been

NILQ page 175

retained'[92] and 'this code cannot itself place restrictions on the ability of these bodies or other persons to acquire data retained under the code for other purposes through the exercise of any statutory power' .[93] Even more explicitly, the draft code of practice states that:[94]

> 'In particular, this code can not place any restrictions on the ability of the public authorities listed in Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 to acquire data retained under this code for any of the purposes set out in section 22 of that Act which do not relate to national security.'

The next legal difficulty is that it is left unspecified what is the relation between Part XI and the Data Protection Act 1998. Part XI does not expressly amend or delimit the Data Protection Act. Presumably, the latter Act will override any codes or even statutory regulations which ask for retention of data on an excessive scale (by reference either to time length or

---

90 Compare the decision of the National Security Appeals Panel of the Information Tribunal in *Norman Baker v Secretary of State for the Home Department* (<http://www.lcd.gov.uk/foi/bakerfin.pdf>, 2001). An automatic blanket exemption from subject access under the Data Protection Act 1998 in respect of personal data held by the Security Service was quashed.

91 See further B. Emmerson, & H. Mountfield, Advice to the Information Commissioner on ATCSA 2001 Retention and Disclosure of Communications Data, July 2002.

92 Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003, Annex A, para.25.

93 *Ibid*., Annex A, para 27.

94 *Ibid*.

type).[95] In contrast to the interpretation in *R. (on the application of S) v Chief Constable of South Yorkshire*, it is clear that Data Protection Principles (Schedule 1, Principle 5) expressly view the retention of data as affecting *per se* data privacy. But the government view, expressed in the draft code, is that such retention of data for the specified period of time by the code is 'necessary for the purpose of national security'[96] and accordingly 'the national security exemption in section 28 of the Data Protection Act 1998 could be relied on to exempt such data from the fifth principle so enabling it to be retained in accordance with the code.'[97]

As mentioned before, if access to retained communications data for investigatory purposes is then actually required, attention must be turned to the Regulation of Investigatory Powers Act 2000, consideration of which throws up several legal problems in its intersection with Part XI.[98] Communications data can be accessed by a designated public authority under Chapter II of Part I of RIPA. Chapter II is yet to come into force (though there has been consultation on a draft code of practice).[99] The fact that it is not in force suggests strongly again that these measures in the 2001 Act were not as vital or as relevant to terrorism as alleged. Under section 21 of RIPA, there is a distinction between (i) interceptions of communications, including their contents, in the course of their transmission, which falls under chapter 1

NILQ page 176

of Part I of RIPA,[100] and (ii) conduct involving the obtaining or disclosure of 'communications data'. This term includes 'traffic data' comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted or other information about the usage or provision of telecommunications or postal services made by any person. Examples of

95 The draft code of practice states that 'data retained under the code are subject to the data protection principles found in the Data Protection Act 1998.' *Ibid*., page s20-21, para. 6-11.

96 *Ibid*., page 21, para 9.

97 *Ibid.*

98 See Y. Akdeniz, N. Taylor, and C. Walker, 'Regulation of Investigatory Powers Act 2000: Bigbrother.gov.uk' [2001] *Criminal Law Review* 73.

99 Home Office, Accessing Communications Data Draft Code of Practice, <http://www.homeoffice.gov.uk/ripa/pcdcpc.htm>, August 2001. The Regulation of Investigatory Powers Act 2000 (Commencement No. 2) Order 2001 SI No.2727 allows for draft and final Codes to be issued, but the consultation period on the draft code ended on 2 November 2001 and nothing has appeared since that time.

100 Note the Interception of communications code of practice, August 2002, at <http://www.homeoffice.gov.uk/ripa/ioccop.htm>. This code of practice relates to the powers and duties conferred or imposed under Chapter I of Part I of the Regulation of Investigatory Powers Act 2000.

'communications data' include equipment and location details, telephone subscriber details, itemised telephone bill logs, e-mail headers, Internet Protocol addresses, and information on the outside of postal items. Criticisms of this purported distinction have already been related, and the concern remains that far more detailed and intrusive records will be made available about electronic communications than would be the case for postal messages.[101]

Data of these kinds may be obtained under section 22(2) where necessary, *inter alia*, '(a) in the interests of national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; (c) in the interests of the economic well-being of the United Kingdom; (d) in the interests of public safety; (e) for the purpose of protecting public health...' Any action taken must be proportionate and necessary (section 23(8)). These purposes obviously go beyond those specified in the Anti-terrorism, Crime and Security Act 2001, so there is a potential not just for confusion but for the abuse of powers, when data retained for some purposes is requested for others as mentioned above. The CSP may not realise that an abuse is occurring since the reasons given by law enforcement agencies are unlikely to be very explicit. The problem could be solved if the Secretary of State issued a direction under section 25 (3) of RIPA, limiting further the purposes of requests for access to the data retained under the Part XI Code. But this would still depend upon CSPs being able to distinguish between data normally retained for business purposes, and therefore accessible under the wider objectives of RIPA, and data specially retained for the purposes listed in Part XI. Furthermore, if the latter purposes of Part XI are interpreted narrowly, and are confined essentially to security purposes, then would it be lawful to act upon an application under Schedule 1 of the Police and Criminal Evidence Act 1984 for the production of communications data which may relate to the investigation of a serious arrestable offence which has been retained longer than the normal business purpose period? Such potential confusions are of 'real concern' to the Information Commissioner.[102] The decision in *R. (on the application of NTL Group Ltd) v Ipswich Crown Court* [103] suggests that access to data (content data in this case) under section 9 and Schedule 1 of the PACE 1984 is a possibility to be borne in mind by a CSP. Therefore, pending the making of an order under

NILQ page 177

101 All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, at http://www.apig.org.uk/APIGreport.pdf, para.39.

102 Information Commissioner, Annual Report 2001-02 (2001-02 HC 913) 18.

paragraph 4 of Schedule 1 to the PACE 1984, the relevant material (or data) could be preserved in accordance with the terms of paragraph 11 of Schedule 1. If and when an order is made under paragraph 4, the CSPs would be required to disclose the data retained in their system. According to the judgment, retention of such data by a CSP (NTL in this case), would not amount to an offence under section 1 of RIPA 2000.

As already mentioned, the dangerous overlap of purposes is recognised by the Home Office draft Code of Practice, but it offers no solutions. One suitably restrained approach would be to adopt 'data preservation' (storing only data of suspects identified to CSPs) rather than blanket 'data retention', thus providing clearer proportionality in balancing the law enforcement needs with privacy concerns. Under a data preservation regime, upon the request of appropriate authorities, data relating to named suspects could be ordered to be preserved for possible later access following a further disclosure order. Such a case by case basis approach is rejected as futile by the Home Office consultation paper on a Code of Practice for Voluntary Retention of Communications Data, though the arguments about not being sure who might become suspects and therefore not being sure about which data to retain for the future really does sound like the pleadings of a paranoid police state.[104] Even the strongly criticised Council of Europe CyberCrime Convention does not include data retention provisions[105] and instead opted for measures involving data preservation.[106] Though data preservation itself represents an 'entirely new legal power or procedure in domestic law'[107] for most European countries, nevertheless, these measures 'do not mandate the collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities.'[108] They are also limited 'for the purpose of specific criminal investigations or proceedings'.[109] Such data would be preserved for a period of time as long as necessary, up to a maximum of 90 days.[110]

---

103 *R v Ipswich Crown Court, ex parte NTL Group Ltd* ([2002] EWHC 1585 (Admin).

104 Home Office, Consultation paper on a code of practice for voluntary retention of communications data, at http://www.homeoffice.gov.uk/docs/vol_retention.pdf, 2003, para.12.4.

105 J. Fisher, 'The Draft Convention on Cybercrime: Potential Constitutional Conflicts' (2001) 32 *U. West. L.A. L. Rev.* 339.

106 See further article 16 (Expedited preservation of stored computer data), and article 17 (Expedited preservation and partial disclosure of traffic data) of the Council of Europe CyberCrime Convention, ETS No 185, 2001.

107 See paragraph 155 of the Explanatory Report of the Council of Europe CyberCrime Convention, <http://conventions.coe.int/treaty/en/Reports/Html/185.htm>, 2001. Data preservation as opposed to data retention is also supported as a preferred option by the All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, http://www.apig.org.uk/APIGreport.pdf, para. 189.

108 *Ibid*, at para 152.

109 See article 14(2) of the Council of Europe CyberCrime Convention, ETS No 185, 2001.

110 *Ibid*., article 16(2).

The Convention furthermore enables real-time collection of traffic data 'associated with specified communications'.[111] But these powers do not intrude as far as Part XI:[112]

NILQ page 178

> '… the Convention does not require or authorise the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of 'fishing expeditions' where criminal activities are hopefully sought to be discovered, as opposed to specific instances of criminality being investigated. The judicial or other order authorising the collection must specify the communications to which the collection of traffic data relates.'

Furthermore, while the Explanatory Report of the CyberCrime Convention claims the privacy interests arising from the collection of traffic data are diminished compared to the interception of content data, it nevertheless acknowledges that

> '...a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context.'[113]

CSPs already co-operate consensually with law enforcement agencies. However, compelled access to traffic data stored for business purposes will become possible under RIPA 2000. Where authorisation is given under RIPA for obtaining and disclosing of the data, then the operator can be compelled (if necessary by civil proceedings) to provide it (section 22(4), though the issuing authority may decide (for example to maintain secrecy or because of superior technical capabilities) to obtain the data itself (section 22(3)). Authorisation will be in writing and must define the conduct authorised and the data to be obtained; the authorisation remains valid for one month (section 23). The issuing authority under chapter 2 is not the Secretary of State but will be an office-holder designated by statutory order within the police, intelligence services, Customs and Excise, Inland Revenue, or any other public authority specified by statutory order.

---

111 *Ibid*., article 20.

112 See para. 219 of the Explanatory Report of the Council of Europe CyberCrime Convention, 2001.

113 *Ibid*, at para 227.

RIPA is an improvement on the previous free-for-all, but it potentially empowers an alarmingly large range of public agencies to snoop and for a rambling array of reasons. And most serious of all, it allows intervention on the basis of standards and procedures which are intentionally lax on the specious grounds that interception of communications content is a much greater intrusion than the collection of traffic data to such an extent that the latter seems hardly to matter.[114] So, speakers who avow the RIP Act as the 'greatest safeguard that exists in any democracy in the world…. for protecting our rights'[115] are simply inaccurate. The Data Protection Commissioner (now the Information Commissioner) was also critical of RIPA, contending that 'access to traffic and billing data should also be made

NILQ page 179

subject to prior judicial scrutiny'[116] and feared that the lack of precision and foreseeability in the legislation might not comply with Article 8 (privacy rights) under the European Convention.[117] The dilution in judicial oversight is also a feature of the US PATRIOT Act 2001[118] in connection with a Pen Register/Trap Trace (PR/TT)[119] authority for Internet data, though even that process does require an application to a court (albeit that it cannot deny the application) and a report back to a judge. PR/TT authority may be used to collect 'addressing' information on the Internet but not the content of communications. The PR/TT authority under section 216 enables law enforcement agencies to install their own monitoring devices such as the FBI's DCS1000, formerly known as Carnivore[120] on computers belonging to a public provider. Systems such as Carnivore are capable of intercepting content of communications and accountability remains difficult with the use of such black-box technology. Moreover, disclosures of either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person to law enforcement agencies by CSPs is now possible under section 212 of the PATRIOT Act 2001.[121]

---

114 See Home Office, *Interception of Communications in the United Kingdom* (Cm.4368, London, 1999) para.10.9.

115 Per David Blunkett, the Home Secretary, House of Commons Debates vol.372 col.935 15 October, 2001.

116 Data Protection Commissioner, Briefing For Parliamentarians on RIP, <http://www.fipr.org/rip/DPCparlRIP.htm>, 2000.

117 News Release, 13 November 2001.

118 Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Pub. L. No. 107-56, 115 Stat. 272 (2001), section 216

119 See 18 U.S.C. s.3122(b)(2).

120 IITRI, Independent Technical Review of the Carnivore System, Final Report, December 8, 2000, at <http://www.epic.org/privacy/carnivore/carniv_final.pdf>.

121 This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers. See generally Computer Crime and Intellectual Property Section (CCIPS), Field Guidance on New Authorities That Relate to Computer Crime and

War is over?

Returning to the thesis at the start of this article that 'War is over', it may be indicative that the legal crisis caused by September 11th has been abating by the slow pace of implementation of Part XI and of Part I, Chapter II of RIPA. As for the latter, when the Home Office issued the draft secondary legislation in June 2002 under section 25 of RIPA, it raised a storm of criticism and was withdrawn. The concern was that the (draft) Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002 would afford powers to a very broad range of official bodies to access communications data, a range well beyond those expressed in the body of the Act itself, such as the police, customs, secret services and the Revenue, and including a wide range of Government departments, local authorities, the NHS and other public authorities.[122] However, the government backed down

NILQ page 180

after a week of vilification,[123] having planned to put the changes for approval before a delegated Legislation Select Committee (on the 19th June 2002) after the Joint Committee on Statutory Instruments had concluded that it was an Instrument to which the Committee did not need to draw the special attention of both Houses.[124] The government's *bona fides* was damaged by the contemporary revelation that a Department of Transport special adviser had sought information about the political affiliation of certain members of the Paddington rail crash survivor's group.[125] The Home Secretary, David Blunkett, said defensively that 'I have no intention that we should be Big Brother'.[126]

Electronic Evidence Enacted in the USA Patriot Act of 2001, at <http://www.cybercrime.gov/PatriotAct.htm>.

122 A total of 24 were listed, but only two (Scottish Drugs Enforcement Agency and UK Atomic Energy Authority Constabulary) could be said to be primarily criminal justice related. The Government later averred that the extension would have been less startling that first appeared because the rank of authorising officer would have been set by a further draft statutory instrument (Regulation of Investigatory Powers (Communications Data: Prescription of Officers, Ranks and Position) Order 2002) at a level higher than attainable by some organisations - an example might be a parish council: All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, <http://www.apig.org.uk/APIGreport.pdf>, para.76. The variable authorisation level might in turn create the need for one public agency acting for others: *ibid*. para.91.

123 *The Times* 18 June 2002 4, 19 June 4.

124 Thirty-First Report 2001-02 HL 128, HC 135-xxxi.

125 House of Commons Deb. vol.386 col.856 12 June 2002; P. Lewis, 'Is big brother getting even bigger?' (2002) *The Times Law* 18 June 3.

126 *Daily Telegraph* 19 June 2002 23.

Admitting that they 'got it wrong', the Home Office published a consultation paper entitled *Access to Communications Data: Respecting Privacy and Protecting the Public from Crime* in March 2003.[127] The government accepted that there must be further limits as to the range of empowered authorities and that the types of data which can be accessed must be limited in most cases.[128] Though some further safeguards are suggested – especially prior scrutiny by the Office of the Interception Commissioner[129] - prior judicial authorisation, the channelling of all access through the police, or the confinement of the empowered authorities to a select handful are all rejected.[130]

Yet, even without the full activation of RIPA, Chapter 1 Part II, it should not be assumed that the government has been wholly defeated in its intentions. The powers under RIPA already require extensive data collection through 'black boxes' to record internet traffic data under RIPA section 12, which provides that:

> 'The Secretary of State may by order provide for the imposition...on persons who...are providing...public telecommunications services...of such obligations as it appears...reasonable to impose for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with'

NILQ page 181

For this purpose the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order came into force in August 2002.[131] This order sets out the obligations which it appears to the Secretary of State reasonable to impose on the CSPs for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with. The obligations include the provision of 'a mechanism for implementing interceptions within one working day of the service provider being informed that the interception has been appropriately authorised,'[132] and 'to enable the simultaneous interception of the communications of up to 1 in 10,000 of the persons

---

127 Home Office, Consultation paper on *Access to Communications Data: Respecting Privacy and Protecting the Public from Crime*, March 2003, at < http://www.homeoffice.gov.uk/docs/consult.pdf>, Foreword, para.5.

128 *Ibid*. para.3.22. For most of the relevant public authorities, there would be no access to traffic data: para.3.46, 3.48.

129 *Ibid*., para.3.49.

130 *Ibid*. paras.3.32, 3.38, 3.44.

131 2002 SI no.1931.

to whom the service provider provides the public telecommunications service, provided that those persons number more than 10,000.'[133]

A necessary component of the surveillance network being created is the Government National Technical Assistance Centre, a mass surveillance facility in the Security Services London headquarters which it is hoped will become operational during 2002.[134] Potentially all United Kingdom internet traffic data could find its way to the Security Service, and it will in particular perform decryption services for law enforcement.[135] Beyond this facility there is the even more uncontrolled UKUSA spy network known as ECHELON, based on the sharing of signals intelligence between the United States, United Kingdom, Canada, Australia and New Zealand.[136]

The implementation of Part XI of the Anti-Terrorism, Crime, and Security Act 2001 is in much deeper trouble and progress has been remarkably slow. The draft code of practice was published for consultation in March 2003, 15 months after the 2001 Act was enacted. Important questions such as whether investigative work has improved, how many requests have been made, whether a voluntary structure is sufficient, and market impacts will need to be answered when the code will be reviewed within three months from the date it receives parliamentary approval.[137]

Further details of the problems created by the measures within the 2001 Act and the related draft code of practice were set out in a report by the All Party Parliamentary Internet Group (APIG) in January 2003.[138] Based especially upon concerns about the legality under European Convention jurisprudence of acting under voluntary codes, APIG recommended that the Home Office

---

132 *Ibid*. para 5.

133 *Ibid*, para 11.

134 <http://www.homeoffice.gov.uk/oicd/ntac/ntac.htm>.

135 See BBC News, Questions over net snooping centre, 6 June, 2002, at <http://news.bbc.co.uk/1/hi/sci/tech/2027377.stm>.

136 See generally <http://www.echelonwatch.org/>. Note the European Parliament resolutions on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI), dated 5 September 2001, and 7 November, 2002 (B5-0528/2002).

137 Home Office, Consultation paper on *Access to Communications Data: Respecting Privacy and Protecting the Public from Crime*, March 2003, at < http://www.homeoffice.gov.uk/docs/consult.pdf>, para.33.

NILQ page 182

immediately drop their plans to introduce a voluntary scheme for data retention under Anti-Terrorism, Crime, and Security Act 2001.[139] An even more stark verdict from APIG was that the Government equally should not invoke its powers under section 104 to impose a mandatory data retention scheme; the concerns include costs, incompatibility with data protection and surveillance provisions as well as conflict with foreign regimes which have adopted different stances and which would come into play when data is processed or warehoused abroad.[140] Given the publication of the draft code of practice in March 2003, it now seems less likely that the whole scheme will be allowed to lapse on 14 December 2003 without firing any legal shot in anger. Nevertheless, instead of an oppressive scheme of blanket data retention,[141] greater attention should be paid to targeted data preservation, even if the target is at times defined in rather wide and wooly terms.[142]

In conclusion, we are getting back to 'normal' by the standards of security laws in the United Kingdom. On the surface, the normal decencies of debate and scrutiny are observed, and the laws are maintained, subject to the blemish of a derogation under Article 15 of the European Convention in respect of powers of detention of suspected foreign terrorists, though even the validity of that notice has now been attacked by some judges.[143] A move away from a war model is to be welcomed, for, like the 'war on drugs' or the 'war on crime', that approach is conducive to a lack of accountability and proportionality - the application of overwhelming rather than sufficient force and finances - and it also threatens an endless departure from civil society.[144] But the shift is by no means secure - threatened armed action against those governments which the President of the United States accuses of being part of an 'axis of evil' – Iraq can now be deleted from the list, but Iran and North Korea remain and Syria seems close

---

138 All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, at <http://www.apig.org.uk/APIGreport.pdf>.

139 *Ibid*. para.141.

140 *Ibid*. para.178.

141 Of course, as pointed out earlier, regard must be had to the capabilities under RIPA s.12.

142 The preservation of all data for 'the period around the attacks' on September 11, which was undertaken on a voluntary basis and resulted in data being preserved until February 2002, is so wide as to amount to blanket retention. See All Party Parliamentary Internet Group, Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003, at <http://www.apig.org.uk/APIGreport.pdf> para.182

143 The discriminatory nature of Part IV of the Anti-terrorism, Crime and Security Act 2001 convinced Mr Justice Collins in a Special Immigration Appeals Commission hearing to declare the derogation to be in breach of Article 14 but the Court of Appeal reversed that judgment: *A v Secretary of State for the Home Department*, [2002] EWCA Civ 1502.

144 See F.A. Allen, *The Habits of Legality* (Oxford University Press, New York, 1996) 37-40.

to candidate status - could quickly change the atmosphere.[145] Furthermore, the alternative to the war model is still an extensive security state. 'War is over', but state surveillance is gathering pace.

Terrbook\ptIX\nilq04

[145] <http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html>, 2001.