



RESEARCH PAPER 02/63
21 NOVEMBER 2002

Communications Data: Access and Retention

Part 11 of the *Anti-terrorism, Crime and Security Act 2001* (chapter 24) deals with the retention of communications data, such as itemised telephone bills and information about emails sent (but not the actual content). This paper covers the relevant debates and concerns that emerged during the passage of the presaging bill, and places the retention of communications data in the context of provisions relating to its *access*. The latter are most notably embodied in the *Regulation of Investigatory Powers Act 2000* (chapter 23).

Data sharing and disclosure are discussed in research paper 02/54.

Grahame Danby

HOME AFFAIRS SECTION

HOUSE OF COMMONS LIBRARY

Recent Library Research Papers include:

02/46	Unemployment by Constituency, June 2002	17.07.02
02/47	The <i>Mobile Telephones (Re-programming) Bill</i> [HL Bill 177 of 2001-02]	18.07.02
02/48	Defence Statistics – July 2002	19.07.02
02/49	Unemployment by Constituency, July 2002	15.08.02
02/50	Regional Development Agencies (RDAs)	22.08.02
02/51	Unemployment by Constituency, August 2002	11.09.02
02/52	Detention of suspected international terrorists – Part 4 of the <i>Anti-Terrorism, Crime and Security Act 2001</i>	16.09.02
02/53	Iraq: the debate on policy options	20.09.02
02/54	The <i>Anti-Terrorism, Crime and Security Act 2001</i> : Disclosure of Information	04.10.02
02/55	Sustainable development and the 2002 World Summit	10.10.02
02/56	Local Government Finance in England: replacing the Standard 11.10.02 Spending Assessment	
02/57	Social Indicators	15.10.02
02/58	Unemployment by Constituency, September 2002	16.10.02
02/59	Economic Indicators	01.11.02
02/60	Unemployment by Constituency, October 2002	13.11.02
02/61	The <i>Health (Wales) Bill</i>	20.11.02

Research Papers are available as PDF files:

- *to members of the general public on the Parliamentary web site,
URL: <http://www.parliament.uk>*
- *within Parliament to users of the Parliamentary Intranet,
URL: <http://hcl1.hclibrary.parliament.uk>*

Library Research Papers are compiled for the benefit of Members of Parliament and their personal staff. Authors are available to discuss the contents of these papers with Members and their staff but cannot advise members of the general public. Any comments on Research Papers should be sent to the Research Publications Officer, Room 407, 1 Derby Gate, London, SW1A 2DG or e-mailed to PAPERS@parliament.uk

Summary of main points

The term communications data, defined in the *Regulation of Investigatory Powers Act 2000* (RIPA), refers to information about the transmission, but not the content, of a communication. Examples include itemised telephone bills, routing information (including sender and recipient) for emails, mobile phone location data, and websites visited.

While the *Data Protection Act 1998* already provides for access to communications data by a variety of public authorities, a new, more regularised, framework is to be provided by Part I Chapter II of RIPA. The wording of the latter explicitly reflects the right to privacy provisions of Article 8 of the European Convention on Human Rights.

The Government aims to implement Part I Chapter II of RIPA in 2003. This is later than originally expected, a delay triggered in part by the withdrawal of associated draft secondary legislation. The draft *Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002* was withdrawn in June 2002 amid concerns over privacy and insufficient consultation. By bringing several additional public authorities within the remit of Part I Chapter II of RIPA, the draft Order focused attention on the ubiquity of existing data access under less formal arrangements.

Publication of a consultation paper on the regulation of access to communications data is expected around the turn of the year. Work is also proceeding apace on a data access code of practice, published in draft during summer 2001.

Part 11 (in force) of the *Anti-terrorism, Crime and Security Act 2001* (ATCSA) provides for the *retention* of communications data by communications service providers, such as telephone companies and internet service providers. Hitherto communications providers have tended to retain data for only so long as it is needed for business purposes.

In pursuit of section 102 of ATCSA, the Government is consulting with communications providers on a voluntary code of practice for data retention. Part 11 also includes provision for authorising the Secretary of State to give directions on data retention to communications providers. Implementation of a voluntary code and authorisation of directions would both take the form of statutory instruments, subject to the affirmative procedure.

This paper summarises the parliamentary debates on Part 11 of the *Anti-terrorism, Crime and Security Act Bill* – focusing on scope and the consequences for privacy of the individual, and the burden on communications providers. It ends with a short bibliography, including articles which comment on the consequences of ATCSA. In one of these, Jason Saiban and John Sykes conclude:

Finally, one should not forget that, authorized or not, it is extremely likely that emails and other communications are being read by the intelligence agencies in any event. 'Echelon' is the CIA's preferred means of access. Will the Act actually make any difference to the way in which our daily lives are monitored?

CONTENTS

I	Access to communications data	7
	A. Regulation of Investigatory Powers Act	7
	B. Draft Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002	13
	C. Comment on the draft Order	16
	D. Withdrawal of the draft Order	18
II	Retention of communications data	20
	A. Anti-terrorism, Crime and Security Act 2001	25
	1. General	25
	2. Part 11	28
	B. Parliamentary debates on the Anti-terrorism, Crime and Security Bill	33
	1. Joint Committee on Human Rights	33
	2. Commons second reading	34
	3. Commons committee stage	35
	4. Lords select committees	36
	5. Lords second reading	36
	6. Joint Committee on Human Rights – further report	41
	7. Lords committee stage	42
	8. Final stages	47
III	Further reading	48

I Access to communications data

Public authorities gain access to communications data, such as addresses and dates of contact, under a variety of statutory powers and codes of practice. For example, according to a written answer of 24 July 2002, the Metropolitan Police had made approximately 127,000 separate requests for communications data under the *Data Protection Act 1998* in the last year.¹

Another written answer covers the Inland Revenue and Customs and Excise:

Harry Cohen: To ask the Chancellor of the Exchequer in relation to communications data as defined in the Regulation of Investigatory Powers Act 2000, how many officials from (a) the Inland Revenue and (b) Customs and Excise he estimates will be authorised to seek access to communications data; and how many times officials have sought access to such data from communications providers such as Internet service providers under the Data Protection Act 1998 in the last year; and if he will make a statement.

Dawn Primarolo: In relation to the Regulation of Investigatory Powers Act 2000, Customs and Excise estimate that the number of authorised officials will be about 200. The Inland Revenue are not yet in a position to estimate a figure, but in any event authorised officials in the Inland Revenue will be restricted to the grades equivalent to Senior Executive Officer and Higher Executive Officer. In the last year, Customs and Excise officials have sought access to such data approximately 35,500 times and Inland Revenue officials approximately 11,700 times.²

The *Regulation of Investigatory Powers Act 2000* makes available a statutory framework for, among other things, access to this data. The Act aims to be compatible with the European Convention on Human Rights, leaving public authorities who adopt its methods and codes less open to successful challenge under the *Human Rights Act 1998*.

A. Regulation of Investigatory Powers Act

Communications data is defined by section 21(4) (Part I Chapter II) of the *Regulation of Investigatory Powers Act 2000*:

In this Chapter "communications data" means any of the following-

(a) any traffic data [defined in section 21(6)] 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;

¹ HC Deb 24 July 2002 c 1497W

² HC Deb 17 October 2002 c 918W

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person-

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

A familiar example of communications data would be itemised telephone bills, detailing the calls made by an individual, but not the contents. A less familiar but highly significant area arises in the context of internet service providers (ISPs) who hold information on individuals' access to websites. For example, a particular user's visits to a website can be tracked if the (computer) server hosting it places an electronic "cookie" in his/her computer. This has benefits both for the internet service provider wishing to target appropriate content and advertising and the user in providing easier, wider and faster access. At the same time it might unfairly implicate an individual who accidentally visits a website with unsuitable content. On 13 November 2001 the European Parliament approved, with amendments, a more general proposal for a European Parliament and Council Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector; reportedly³ one issue was whether cookies violated an individual's right to privacy, enshrined in Article 8 of the European Convention on Human Rights:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such 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.

European Parliament and Council Directive 2002/58/EC concerning the processing of personal data and protection of privacy in the electronic communications sector was adopted on 12 July 2002. Its measures must be transposed into UK law by 31 October 2003. Article 15 allows member states to adopt legislative measures restricting the scope of the rights and obligations on data processing provided "such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to

³ BBC Radio 4, *Today*, 13 November 2001
BBC News Online, *Europe tackles internet privacy*, 13 November 2001

safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.”

Access to communications data and the uses to which it may be put are governed by the *Regulation of Investigatory Powers Act 2000* (RIPA). As its Explanatory Notes⁴ indicate this Act works in conjunction with other key legislation in this area: the *Intelligence Services Act 1994*, the *Police Act 1997* and the *Human Rights Act 1998*. RIPA provides for UK-wide⁵ statutory authorisations and safeguards on the interception of communications, surveillance methods and access to encrypted data. Chapter II of Part I (i.e. sections 21-25) "provides a legislative framework to cover the requisition, provision and handling of communications data. It explains the duties and responsibilities placed upon each party involved in these processes and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights."⁶ Before the withdrawal of a related “additional public authorities” order (see below), this Part was originally expected to come into force on 1 August 2002.⁷ It provides for access to communications data by the following public authorities:

- (a) a police force;
- (b) the National Criminal Intelligence Service;
- (c) the National Crime Squad;
- (d) the Commissioners of Customs and Excise;
- (e) the Commissioners of Inland Revenue;
- (f) any of the intelligence services [Security Service, Secret Intelligence Service, Government Communications Headquarters];
- (g) any such public authority not falling within paragraphs (a) to (f) as may be specified for the purposes of this subsection by an order made by the Secretary of State.⁸

Paragraph (g) above relates directly to the draft *Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002*; the latter was

⁴ Explanatory Notes, RIPA, <http://www.hmso.gov.uk/acts/en/2000en23.htm>

⁵ an exception is Part II of RIPA, not relevant here, which was legislated for separately in Scotland: *Regulation of Investigatory Powers (Scotland) Act 2000*

⁶ Explanatory Notes, RIPA, op. cit.

⁷ Explanatory Memorandum, The Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002, Home Office, May 2002 (unprinted paper 1585 2001/02)

⁸ RIPA, section 25

originally due to come into force on 1 August 2002 but was withdrawn amid concerns over privacy and insufficient public consultation.

Section 22(2) of RIPA imposes a test of "necessity" on the acquisition of data; the designated person within the relevant⁹ authority must believe this necessary:

- (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;
- (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
- (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

These potentially very broad provisions find an echo in Article 8(2) of the European Convention (quoted earlier) and lie at the heart of the Act's human rights compatibility.

The rank required of a designated person will be prescribed by an order made by the Secretary of State. Section 25(2) of RIPA provides for this, subject to restrictions the Secretary of State may impose by virtue of section 25(3). Communications data will be accessible either directly on the "authorisation"¹⁰ of a Superintendent (or equivalent) or by him/her giving a "notice"¹¹ to the postal or telecommunications operator. Inspectors will have powers to authorise access to a subset of communications data, for example account and subscriber information. (It is worth noting that, historically, requests have often been for "low-level" data like subscriber details rather than locations of communications).¹²

Further information on the proposed operation of RIPA Chapter II Part I is given in a draft code of practice, subjected to public consultation during the period 13 August to 2

⁹ A section 25(2) order will stipulate both the ranks and the section 22(2) paragraphs relevant in each case.

¹⁰ RIPA, section 22(3)

¹¹ RIPA, section 22(4)

¹² EURIM meeting, House of Commons, 19 September 2002

November 2001.¹³ The laying before parliament of a draft of this access code, expected “shortly” in June 2002,¹⁴ may have been delayed by the subsequent withdrawal of related draft orders, i.e. those¹⁵ dealing with additional public authorities.

The suggested balance between authorised direct access and notification procedures reflects a change in policy signalled by the Parliamentary Under-Secretary of State (Bob Ainsworth) in a letter to Lord Lucas (copied to Lord Rooker and the library of both Houses):

...An authorisation allows the relevant public authority to collect the data itself. A notice served on a postal or telecommunications operator requires the operator to collect the data and provide it to the public authority which served the notice.

We believe the suggestion that a notice should be used in preference to an authorisation now needs to be relaxed. This change in policy is due largely to the advent of online databases which the communication service providers make available to the public authorities. (At Report Stage of the RIP Bill and during debate you highlighted police access to the BT database (Official Report, 12 July, Column 328)). Recent developments suggest that this form of accessing communications data will increase significantly...¹⁶

Restrictions "on the circumstances in which, or the purposes for which, such authorisations may be granted or notices given" can be imposed by an order made by the Secretary of State.¹⁷

Under section 57(2)(b) of RIPA, the Interception of Communications Commissioner (Sir Swinton Thomas)¹⁸ will keep under review "the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I."

The Intelligence and Security Committee have also noted:

¹³ Home Office, *Accessing Communications Data Draft Code of Practice*, August 2001 (House of Commons Library unprinted paper 387 2001/02)

¹⁴ <http://www.homeoffice.gov.uk/ripa/pdcpc.htm>

¹⁴ HC Deb 11 June 2002 cc 1238-9W

¹⁵ draft SI on Regulation of Investigatory Powers (Communications Data: Additional Public Authorities)
draft SI on Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources: Additional Public Authorities)
draft SI on Regulation of Investigatory Powers (Designation of Public Authorities for the Purposes of Intrusive Surveillance)

¹⁶ Letter from Bob Ainsworth MP to Lord Lucas, *Regulation of Investigatory Powers Act: Chapter II of Part I - Access to Communications Data*, 18 July 2001

¹⁷ RIPA, section 25(3)(b)

¹⁸ *Report of the Interception of Communications Commissioner for 2000*, Cm 5296, October 2001

19. A key element of public accountability of the Agencies is that individuals who believe that they may have a legitimate grievance against an Agency are able to make their complaint to a Tribunal. We have noted that the Tribunals under the Security Services Act 1989 and the Intelligence Services Act 1994 have been amalgamated with the Interception of Communications Tribunal in the Regulation of Investigatory Powers Act 2000 as the Investigatory Powers Tribunal, which came into being in October 2000.¹⁹

Monitoring internet usage, for example, should be a useful tool against terrorists, paedophiles and other criminals, such as those engaged in fraud – even if it has raised concerns that the powers in RIPA could be misused to compromise the privacy of law-abiding citizens.²⁰ This encapsulates a central issue joined by proponents and detractors of the Act. Some civil libertarians have argued that, when the Government talked of "updating" the legislation on interception, they were in fact assuming far wider powers.²¹ These views are not necessarily inconsistent as technologies such as the internet are providing ever-widening communications options. Indeed, the Act's critics may argue that communications technology has undergone a paradigm shift, rendering obsolete some of the thinking behind RIPA. Of course, the privacy concept may similarly be affected, a "cybervillage" created by the internet resembling its parodical counterpart – a small settlement where everyone knows everyone else's business.

Other concerns were identified in an *Economist* article in August 2000:

Perhaps because of its recondite theme, the law's passage created less of a stir than it deserved to, despite the vigorous opposition it provoked among businesspeople, peers, trade unions and the civil-liberties lobby. Its controversial elements include the ability of the police and others to demand the release of "keys" (ranging from simple passwords to complicated encryption techniques) to electronically encrypted material. The law gives the home secretary an ominous-sounding power to require the installation of interception devices (known as "black boxes") by Internet service providers (ISPs). These will intercept information on e-mail and Internet activity and send it to a government monitoring centre...

...As with many arguments about civil liberties, this one turns on how far governments can be trusted - in this case not to exploit the opportunities for undue surveillance which technology, and the law, will now provide.²²

¹⁹ *Intelligence and Security Committee Interim Report 2000-01*, Cm 5126, March 2001
<http://www.official-documents.co.uk/document/cm51/5126/5126.htm>

²⁰ "Britain: Being watched: Electronic surveillance: Government eavesdropping", *Economist*, 26 August 2000

²¹ *ibid.*

²² *ibid.*

B. Draft Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002

The purpose of the, now withdrawn, draft *Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002* was given in a short accompanying explanatory note:

This Order specifies additional public authorities for the purposes of section 25(1) of the Regulation of Investigatory Powers Act 2000 ("the 2000 Act"). Public authorities specified for the purposes of section 25 are entitled to obtain communications data under the provisions set out in Chapter II of Part I of the 2000 Act.

Subject to affirmative resolution of each House, the Order would have come into force on 1 August 2002. It had also been the Government's intention to commence Part I Chapter II of the 2000 Act (which includes the relevant Order making powers) on the same date.

A copy of the draft *Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002* is available in the House of Commons Library as unprinted paper 1585 2001/02. This includes an explanatory memorandum with legislative and policy background:

Powers exercised

The above instrument is made in exercise of the powers conferred by paragraph (g) of the definition of "relevant public authority" in section 25(1) of the Regulation of Investigatory Powers Act 2000 (RIPA). It cannot have effect until it is approved by resolution of each House of Parliament.

Legislative background

Chapter II of Part I of RIPA (acquisition and disclosure of communications data) introduces a statutory framework to regulate access to communications data by public authorities consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in the process and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights (ECHR).

Section 25(1) of RIPA defines "relevant public authorities" for the purposes of Chapter II of Part I of that Act. Paragraph (g) of the definition of "relevant public authority" in section 25(1) permits the Secretary of State to add further public authorities to this list by means of an Order subject to the affirmative resolution procedure in Parliament.

Section 25(5) of RIPA requires that the Secretary of State shall not make an Order adding public authorities unless a draft has been laid before Parliament and approved by a resolution of each House.

A further Order, made under section 25(2) of RIPA, designating authorising persons for both the new authorities and those already listed in section 25(1), which is subject to negative resolution, will also be required. The attached draft Schedule, which is intended will form the basis of the section 25(2) Order, lists each authority, the authorising officer(s) who can grant authorisations or give notices and the purposes under section 22(2) of RIPA for which communications data may be accessed by that authority. Chapter II is not yet in force and it is intended to commence it on the date this Order will take effect if approved; 1st August 2002.

Policy background

Communications data is information held by communication service providers (eg telecom and Internet companies) relating to the communications made by their customers. This includes itemised billing, routing information and subscriber details. Communications data does not include the content of any communication.

This Order adds additional public authorities to the list of "relevant public authorities" in Chapter II of Part I of RIPA (acquisition and disclosure of communications data).

Chapter II of Part I of RIPA provides that within each relevant public authority only persons holding certain offices, ranks or positions may grant authorisations or give notices requiring communications data. These offices, ranks and positions are to be designated by the Secretary of State in a negative Order to be laid shortly. A strict test of "necessity" must be met before any communications data is obtained under Chapter II. An authorising officer must not only consider the communications data to be necessary but must also consider the conduct involved in obtaining the. communications data to be "proportionate" to what it seeks to achieve. The grounds on which it is necessary, for example, include: in the interests of national security; for the purpose of preventing or detecting crime or of preventing disorder. These measures will be targeted and, in addition, to specifying the authorising officers within each public authority, we intend to restrict the purposes, in section 22(2) of RIPA, for which communications data may be obtained by each authority. This is set out in the draft Schedule. The overall regime will be subject to oversight by the Interception of Communications Commissioner.

The additional public authorities added by the draft order are as follows:

Government departments

- The Department for Environment, Food and Rural Affairs.
- The Department of Health.
- The Home Office.
- The Department of Trade and Industry.
- The Department for Transport, Local Government and the Regions.
- The Department for Work and Pensions.

- The Department of Enterprise, Trade and Investment for Northern Ireland.

Local authorities

- Any local authority within the meaning of section 1 of the Local Government Act 1999.
- Any fire authority as defined in the Local Government (Best Value) Performance Indicators Order 2000
- A council constituted under section 2 of the Local Government etc. (Scotland) Act 1994.
- A district council within the meaning of the Local Government Act (Northern Ireland) 1972.

NHS bodies in Scotland and Northern Ireland

- The Common Services Agency of the Scottish Health Service.
- The Northern Ireland Central Services Agency for the Health and Social Services.

Other bodies

- The Environment Agency.
- The Financial Services Authority.
- The Food Standards Agency.
- The Health and Safety Executive.
- The Information Commissioner.
- The Office of Fair Trading.
- The Postal Services Commission.
- The Scottish Drug Enforcement Agency.
- The Scottish Environment Protection Agency.
- The United Kingdom Atomic Energy Authority Constabulary.
- A Universal Service Provider within the meaning of the Postal Services Act 2000

The explanatory memorandum to the Additional Public Authorities Order also refers to an attached draft schedule (to a further Order – not laid as yet). This identifies both the ranks of the authorising officers for each public authority, and the reasons for which each may have access to communications data. For example, under the original proposals, a police superintendent would be able to require access, by authorisation or giving notice, to the communications data defined by section 21(4) of RIPA (above). A police inspector would have authority solely in respect of a subset of communications data specified in section 21(4)(c) of RIPA (this would refer to general account and subscriber information²³ like the name and address and payment method associated with a telephone number, but

²³ <http://www.homeoffice.gov.uk/ripa/pdcpc.htm> (Accessing Communications Data Draft Code Of Practice)

not the detailed billing information).²⁴ The purposes for which the police could require access would be those given in section 22(2) of RIPA, with the exception of paragraphs f (tax assessment) and h (further purposes which could be specified in a future order).

By way of further example, the Head of Security (in a Business Unit) in Consignia plc would only be able to require access for the reason given in RIPA section 22(2) paragraph b - preventing or detecting crime or of preventing disorder.

These proposals could well be modified in the light of public consultation following withdrawal of the draft *Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002*.

C. Comment on the draft Order

On 10 June 2002, the Foundation for Information Policy Research ("a non-profit think-tank for Internet and Information Technology policy, governed by an independent Board of Trustees with an Advisory Council of experts")²⁵ published the following in a press release:

The Regulation of Investigatory Powers (RIP) Act is to be amended before it even comes into force to dramatically increase the number of official bodies that can access personal details of phone calls and emails. The Act was hugely controversial when it went through Parliament in 2000, with defeats for the Government in the Lords and significant changes being made to prevent its complete rejection.

Now the powers that were originally only given to the police, customs, secret services and the taxman are to be made available to a huge range of Government departments, local authorities, the NHS and even to Consignia (the Post Office).

Ian Brown, Director of FIPR commented, "I am appalled at this huge increase in the scope of Government snooping. Two years ago, we were deeply concerned that these powers were to be given to the police without any judicial oversight. Now they're handing them out to a practically endless queue of bureaucrats in Whitehall and Town Halls."

The powers contained in RIP Part I Chapter II allow notices to be served on telephone companies, Internet Service Providers (ISPs) or postal operators to obtain information such as the name and address of users, phone numbers called, source and destination of emails, the identity of web sites visited or mobile phone location data accurate to a hundred metres or less.

²⁴ Home Office spokesman 14 June 2002

²⁵ www.fipr.org

However, this part of the Act has proved to be complex to implement. A draft Code of Practice only became available for consultation in Autumn 2001 and is still being rewritten to reflect the poor reception it received. The Government is now suggesting that this process will be completed by August, but this is only the latest date in a long series of missed deadlines.

Ian Brown remarked, "The difficulty that the Government has encountered in getting the right processes in place for the police should make us ultra-cautious in extending these powers to such a wide range of bodies. We don't think that there's been enough resources put into the oversight arrangements for the current proposals, let alone what will be needed for this huge extension. In practice, these bodies are going to obtain this personal data on anyone they wish, without any effective way of checking what they're doing".

He continued, "which websites we visit or where we travel with a mobile phone in our pocket reveals a great deal of personal information. Accessing this information needs to be made more difficult, not opened up to this huge range of new enquirers. I look at this list and wonder not at who they've added, but if I can possibly think of anyone they've left out."²⁶

Among subsequent reports was one published in the *Guardian* (accompanied by a leader) which quoted representatives of Liberty,²⁷ Privacy International, the Society of Editors, Internet Service Providers and the Home Office.²⁸ The report wrote of a "systematic campaign" by ministers "to undermine the right to privacy". It also referred to the European Parliament approval for new communications data retention measures - an important adjunct to the data access measures being discussed here, and since adopted as Directive 2002/58/EC.

The 13 June 2002 *Guardian* published the following response from Bob Ainsworth MP (Parliamentary Under-Secretary of State, Home Office):

You ignore what the provisions of the Regulation of Investigatory Powers Act 2000 allow and the safeguards they put in place. The government is seeking to bring within the regulatory regime of Ripa public authorities which already seek access to communications data, even though some make a small number of requests.

We are not giving these additional public authorities the power to demand the records of every British telephone and internet user. Ripa ensures that access is necessary for specific purposes, such as national security, the prevention and detection of crime, the prevention of disorder and in the interests of public safety

²⁶ <http://www.fipr.org/press/020610snooping.html>

²⁷ The Liberty website includes that organisation's response to the draft Order: <http://www.liberty-human-rights.org.uk/mpress112.html>

²⁸ "Government sweeps aside privacy rights", *Guardian*, 11 June 2002 <http://www.guardian.co.uk/humanrights/story/0,7369,731074,00.html>

and health. Authorities that will use the powers must demonstrate they will need them for the purposes set out in the act. This will help to ensure, more than in the past, that there will be no "fishing expeditions". These provisions are consistent with our Human Rights Act obligations. There will be independent oversight of these powers by the interception of communications commissioner, who is required to report to the prime minister any contravention of the provisions. Anyone who believes data about their communications has been wrongly accessed can complain to the investigatory powers tribunal.

D. Withdrawal of the draft Order

Five days later, the Home Office announced that the draft Order was being withdrawn. The full text of the relevant press release is reproduced here:

NEW TIMETABLE FOR COMMUNICATIONS ACCESS PROVISIONS

Reference: 161/2002 - Date: 18 Jun 2002 12:24

The Home Secretary today responded to public concerns about the regulation of access to communications data.

The draft order, which was due to be debated in the House of Commons next week, has now been withdrawn for detailed consultation over the Summer.

David Blunkett said:

"I recognise there is widespread concern about the current proposals to regulate how public bodies can access phone and internet records.

"It's clear that whilst we want to provide greater security, clarity and regulation to activities that already go on, our plans have been understood as having the opposite effect. Bob Ainsworth and I have therefore decided that it makes sense to withdraw the current proposals to allow calmer and lengthy public discussion before we bring forward new plans in this field. This will not affect the police and security services who will continue to operate in the usual way under current arrangements.

"However, we need a much broader debate about other public bodies involved in this area, particularly given that none of them have joined the debate over the last week to make clear the problems they face without Government legislating.

"Mobile phone and internet usage has grown enormously in the last five years, bringing a whole new world of communications. The reaction to our plans has shown that we need a much broader public debate about how to strike the balance between the privacy of the citizen and society's legitimate need for measures to support the investigation of crime and to protect the public. We must also remember the considerable safeguards provided to the public by the Data Protection Acts.

"Despite being in public life, I value my own privacy and understand these sensitivities. The time has come for a much broader public debate about how we

effectively regulate modern communications and strike the balance between the privacy of the individual and the need to ensure our laws and society are upheld."

Home Office Minister Bob Ainsworth said

"This is an important debate for the country to have. Everyone agrees we need to uphold the law while ensuring communication services providers know where they stand when asked for information. We recognise public concern and are determined to get the balance right."

Note to Editors:

The order that has been withdrawn is the addition of public authorities to Part 1 Chapter 2 of RIPA, (Access to Communications Data).

Shortly after the above announcement, the Foundation for Information Policy Research also issued a press release:

The Home Office is reported to have postponed its proposals to amend the Regulation of Investigatory Powers (RIP) Act to allow a huge increase in the official [sic] that can access personal details of phone calls and emails.

Attention was first drawn to the highly technical Regulations encapsulating this change by an FIPR Press Release on 10th June. The story has since become headline news and the Government has now decided not to proceed with these changes.

Ian Brown, Director of FIPR welcomed this news, "these proposals were poorly considered, poorly justified and over the past week have been condemned by almost everyone outside of Whitehall. The Home Office must now tear them up and start again from first principles."

He continued, "we are as keen as anyone else in seeing wrongdoing investigated, but we don't think that handing out such wide-reaching powers to every bureaucrat in the land is compatible with living in a free society. The Government needs to carefully consider whether self- authorisation can ever be appropriate for this type of invasion of privacy and they need to pay a lot more attention to the oversight regime. An Interception Commissioner who doesn't have the resources to open all his mail is no credible way to ensure that abuse is detected."²⁹

In response to these and similar concerns, the Home Office is preparing a public consultation which, it is anticipated, will include a privacy impact assessment. Publication of a consultation paper is expected "around the turn of the year".³⁰ As part of

²⁹ FIPR press release, *FIPR welcomes Government rethink on snooping powers*, 18 June 2002

³⁰ HC Deb 7 November 2002 c 817W

the preparation for this, a meeting of Home Office officials and EURIM³¹ was held at the House of Commons on 19 September 2002. Debate focused on the issues of privacy of the individual and the cost to the communications providers of passing on communications data. It would seem plausible that public concern over the former could be heightened by a consultation which would inevitably bring into focus the extent of existing and proposed communications data access. Of interest would be: summary information giving the existing provisions under which each of the relevant public authorities currently gain access to information; the number of such requests annually; the anticipated number (or at least whether lower or higher) of such requests that might follow a switch to the RIPA scheme. One advantage of RIPA is that, unlike some statutory provisions emanating from other government departments, it includes some provision³² for the recovery of costs incurred by communications providers in acceding to requests for data. The EURIM meeting debated the extent to which these costs would be met, such as those involving staff training and technical infrastructure. The latter would clearly have to expand to accommodate retention of yet more communications data. In a written answer of 6 November 2002 Lord Falconer of Thoroton said:

Section [sic] 11 of the Anti-Terrorism, Crime and Security Act 2001 allows for the Secretary of State to make "appropriate contributions" towards the costs incurred by the service providers to meet the provisions of the Act. We are in discussion with the industry on a formula which we hope will be concluded shortly.³³

II Retention of communications data

In his statement on 15 October 2001, the Home Secretary said:

We will introduce measures to enable communication service providers to retain data generated in the course of their business, by which I mean the recording of calls made and other data, not the content. We will work with the industry on a code of practice. I wish to thank those who have co-operated so well over the past five weeks in the industry.³⁴

Retention of data is subject to the *Data Protection Act 1998*, at the heart of which lie the following data protection principles (Schedule 1, Part I):

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

³¹ EURIM – European Information Society Group, a UK-based “all-party, pan-industry ‘lobby’ where the politics of the Information Society and E-Commerce are discussed across political, organisational and national boundaries prior to public debate.” <http://www.eurim.org/>

³² section 24, RIPA

³³ HL Deb 6 November 2002 c 109W

³⁴ HC Deb 15 October 2001 c 924

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedule 1 also details how these 8 principles are to be interpreted, by virtue of section 4. In respect of the first principle, schedules 2 and 3 attach conditions to the processing (including retention) of personal data. These include the performance of a contract between the data controller (e.g. the communications service provider) and the data subject (customer) and for the pursuit of other legitimate interests of the data controller. Data can also be kept for other purposes specified in the 1998 Act, including the "administration of justice".³⁵ In general, however, communications service providers are obliged to delete data once it is no longer needed for billing purposes. Enforcement of the 1998 Act lies with the Information Commissioner; prior to 30 January 2001 s/he was referred to as the Data Protection Commissioner. Further information on her/his responsibilities appears on the Information Commissioner website.³⁶ The former Information Commissioner, Elizabeth France, was due to stand down at the end of

³⁵ *Data Protection Act 1998*, schedule 2, paragraph 5

³⁶ <http://www.dataprotection.gov.uk/>

September 2002; her successor, Richard Thomas, takes over at the beginning of December.³⁷

In a letter to the *Independent on Sunday* (28 January 2001), the Ministers Charles Clarke (Home Office) and Patricia Hewitt (Department of Trade and Industry) corrected a misconception at the time concerning the scope of RIPA:

YOU ASSERT that the Government plans to "force companies to retain e-mail records" through the Regulation of Investigatory Powers Act (Ripa) ("Demon sees devil in the detail of RIP Act," 21 January). We do not. Ripa contains no such powers.

There is an important difference between providing for lawful powers to access communications data and legislating to require internet service providers to retain such information for law-enforcement purposes. Ripa is only about the former. It introduces comprehensive statutory controls, for the first time, governing access to billing information or subscriber details. We have no plans to introduce legislation mandating the retention of such data.

In the wake of subsequent terrorist attacks the question of data retention was revisited. Following the Home Secretary's statement³⁸ on 15 October 2001, a consultation exercise (still ongoing)³⁹ with industry was launched; part of this took the form of 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. Welcoming the Government's confirmation that data retention would take the form of a voluntary rather than mandatory code, the ISPA identified some of the "complex issues" that would have to be addressed:

how to develop a code of practice that will relate to the diversity of communications service providers (CSPs)

identification of the types of data law enforcement agencies find useful

the practical aspects of data handover and compliance with data protection law

how CSPs' costs will be recovered

how the code of practice will affect CSPs whose servers are located abroad.⁴⁰

³⁷ Lord Chancellor's Department press notice 305/02, *Government responds to European Commission's Questionnaire on EC Data Protection Directive*, 16 September 2002

³⁸ HC Deb 15 October 2001 c 924

³⁹ HC Deb 11 June 2002 cc 1238-9W;

http://www.ispa.org.uk/html/media/data_retention.html (9 October 2002)

⁴⁰ ISPA Council Statement, *ISPA gives cautious welcome to UK Government's data retention announcement*, 26 October 2001, http://www.ispa.org.uk/html/statement_2510dp.htm

Many of the above points should be covered in the code of practice being drawn up by the Government:

Mr. Allan: To ask the Secretary of State for the Home Department what types of data are included within the code of practice which his Department is drawing up for data retention by communications service providers.

Mr. Denham [holding answer 26 October 2001]: I will draw up the Code of Practice in consultation with communications service providers and the law enforcement and security and intelligence agencies. The general definition of communications is in Part I, Chapter II of the Regulation of Investigatory Powers Act 2000. The types of data within that category that will be covered by the code will be agreed in the course of consultation. That way we can be sure that both sides are clear about the types of data which are retained.

Mr. Allan: To ask the Secretary of State for the Home Department what plans he has in respect of the retention of communications data by communication service providers; and whether this will be (a) voluntary or (b) mandatory.

Mr. Denham [holding answer 26 October 2001]: I intend to make it clear that communications service providers may retain data for up to 12 months for law enforcement and national security purposes. I will then work with the telecommunications industry to develop a voluntary code of practice on retention of data.⁴¹

While some internet service providers already keep data for a year, others delete it after as little as 48 hours.⁴² The Government has also commissioned a report (by John Horrocks) on data retention; its findings, which include commercially sensitive information, were due to be shared with industry contacts in November 2001.⁴³ It has not been seen by the House of Commons Library.

That the Government is still consulting with industry on a code of practice is one fact to emerge from two written answers. These also illustrate the relationship between data access and data retention:

Harry Cohen: To ask the Secretary of State for the Home Department in relation to communications data, how many Immigration Service officials he estimates will be authorised to seek access to communications data and how many times officials have sought access to such data from communications providers such as Internet service providers under the Data Protection Act 1998 in the last year; and if he will make a statement.

⁴¹ HC Deb 31 October 2001 cc 725-6W

⁴² BBC News Online, *Anti-terror laws raise net privacy fears*, 11 November 2001

⁴³ HC Deb 1 November 2001 c 849W

Beverley Hughes: The Immigration Service has previously accessed communication data under the Data Protection Act 1998 through police Single Points of Contact. The Immigration Service did not retain a central register of the number of inquiries undertaken.

The Immigration Service is seeking to become a prescribed authority under the Regulation of Investigatory Powers Act 2000 Chapter II in order to access communications data. Once approved, any immigration official investigating immigration related crime would be able to submit an application for communication data via a single point of contact.

Harry Cohen: To ask the Secretary of State for the Home Department if he will make a statement on the code of practice in relation to communications data; which public authorities will be able to have access to communications data; if he will make a statement on the support he has obtained from telecommunications companies for the concept of a voluntary code of practice to govern the access to communications data; whether he intends to use statutory powers to place access to communications data on a statutory footing; and if he will make a statement on the collective statement made by Data Protection Commissioners with regard to his proposals for the retention of communications data.

Mr. Blunkett: Communications data may be supplied voluntarily for specified purposes (e.g. investigation of crime) under the Data Protection Act 1998. A more tightly controlled regulatory regime for access to communications data will be provided for under the Regulation of Investigatory Powers Act 2000 (RIPA). Chapter II of Part I of the Act explains the duties and responsibilities placed upon each party involved in the process, and creates a system of safeguards reflecting Article 8 of the European Convention of Human Rights (ECHR). The overall regime will be subject to oversight by the Interception of Communications Commissioner.

The Chapter II provisions are subject to a statutory code of practice, a draft of which was published for public consultation during summer 2001. The code relates to the powers and duties conferred or imposed under Chapter II. It provides guidance on the procedures that must be followed before access to communications data can take place under those provisions. RIPA provides that the code is admissible in evidence in criminal and civil proceedings. We aim to implement the Chapter II provisions in 2003.

I will be bringing forward proposals in relation to any additional public authorities under Chapter II Part I of RIPA following detailed public consultation.

We are still in consultation with the communications service providers on the production of a voluntary code of practice to cover the retention of communications data by them under the Anti-terrorism Crime and Security Act

2001, and have noted the statement by the Data Protection Commissioners with regard to proposals on data retention.⁴⁴

Lord Falconer of Thoroton has more recently stated that the consultation process “is now drawing to a close”.⁴⁵ This, despite earlier reports that the secretary-general of the Internet Service Providers Association had written to Home Office officials to the effect that the ISPA could not “recommend to members that they voluntarily comply with the proposed code of practice”.⁴⁶ The cost of storing large quantities of information, and the possibility of legal challenge under data protection and human rights legislation lay behind these concerns. According to a short report in *Solicitors Journal* (25 October 2002) Nicholas Lansman, secretary general of the ISPA, has said the data retention proposals “fail to provide details of the number of investigations that are currently compromised though [sic] the lack of available data ... the investigations cited refer to cases in which officers sought data older than 15 months and where there was no national security consideration involved.”⁴⁷

A. Anti-terrorism, Crime and Security Act 2001

This section takes as its starting point Part 11 of the *Anti-terrorism, Crime and Security Bill* as originally presented in the House of Commons. Bill 49 of 2001-02 received its first reading on 12 November 2001.

1. General

The *Bill Summary* accompanying publication of the original Bill⁴⁸ asserted that communications data had been “central to the investigation into the terrorist attacks on 11 September.”⁴⁹ A supplemental regulatory impact assessment on the *Retention of Communications Data* indicates how, alluding to the widespread use (if not necessarily under registered ownership) of mobile phones:

Communications data is an important investigative tool: it allows 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).⁵⁰

Relating the Bill's data retention theme with RIPA, the *Bill Summary* stated:

⁴⁴ HC Deb 15 October 2002 cc 742-4W

⁴⁵ HL Deb 7 November 2002 c 161W

⁴⁶ “Blunkett warned on internet plans”, *Financial Times*, 23 October 2002

⁴⁷ “ISPs kick out Blunkett proposals”, *Solicitors Journal*, 25 October 2002 p 948

⁴⁸ Bill 49 of 2001-02

⁴⁹ <http://www.homeoffice.gov.uk/oicd/antiterrorism/index.htm>

⁵⁰ http://www.homeoffice.gov.uk/oicd/antiterrorism/retention_of_communications_data.pdf

The Regulation of Investigatory Powers Act 2000 sets out clear limits on the purposes for which the law enforcement, security and intelligence agencies may request access to data relating to specific communications. Mass trawls or “fishing expeditions” are NOT permitted. The Bill allows for a voluntary code of practice to support this. It has a reserve power to review these arrangements and issue directions if necessary. Reserve power is reviewable every two years. If still needed, it must then be reviewed by an affirmative order. As soon as the power is exercised, there is no need for further review.

We are not alone in seeing the need for such a change. Belgium, France, Germany, Italy and the Netherlands all now have data retention policies in place.

A BBC News Online article published on 11 November 2001 indicates a number of concerns likely to feature in subsequent debates.⁵¹ Privacy and cost, in short. The article cites a “tentative figure of £20m” put on the proposals by the Internet Service Providers Association. This compares with the Government’s regulatory impact assessment which cites industry estimates “upwards from £9m”. The Bill provided for contributing to additional costs, though internet service providers would, and still, increasingly have open to them the option of relocating overseas, avoiding the extra work as well as foreclosing access by UK law enforcement agencies. This option becomes ever more attractive with the increasing availability of international links with higher bandwidth (data carrying capacity).

Of course, were the EU to adopt uniform data retention requirements, then this would lessen the relocation options of ISPs – perhaps to countries establishing themselves as “data havens”. Debate has evidently been joined,⁵² not least in how to reconcile data retention and access with existing directives on data protection and privacy. A Danish EU Presidency press release of 9 October 2002 alludes to this, referring to a Statewatch⁵³ report:

Based on a report from the organisation Statewatch, there has over the past few days been rumours in certain parts of European press of imminent EU-rules on the retention of telecommunication traffic data and the access to such data.

In this connection it has been suggested that the Danish Presidency of the European Union has tabled a proposal for binding rules on such retention, rules that would imply that telecommunication providers would be placed under an obligation to store traffic data for up to two years, that such traffic data would be collected in central databases, and that stored information should be made available to all Member States.

⁵¹ BBC News Online, *Anti-terror laws raise net privacy fears*, 11 November 2001

⁵² http://www.epic.org/privacy/intl/data_retention.html

⁵³ <http://www.statewatch.org/news/2002/aug/05datafd1.htm>

These rumours are based on fundamental misunderstandings, that could have been avoided, in case the media concerned had contacted the Danish Presidency in advance.

In June 2002 the Danish presidency tabled a proposal for Council conclusions on information technology-related measures concerning the investigation and prosecution of organised crime.

The proposal that was made available on the Council website (ue.eu.int) in July contains a request that within the very near future binding rules should be established on the approximation of Member States' rules on the obligation of telecommunications services providers to keep information concerning telecommunications in order to ensure that such information is available when it is of significance for a criminal investigation

The proposal contains no detailed indications as to what the contents of such rules should be, but emphasizes that such regulation must be established taking account of the requirements regarding privacy and the processing of personal data which stem from the European Convention on Human Rights of 4 November 1950, the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The proposal is currently under consideration in the relevant Council expert group and is not likely to be ready for adoption before November 2002 at the earliest.

There are no further proposals on the table regarding retention of traffic data, and the Danish Presidency is not engaged in drafting any such proposals.⁵⁴

On the privacy point, the above-mentioned BBC article⁵⁵ quoted Caspar Bowden, then director of the Foundation for Information Policy Research as fearing widespread use (under RIPA) of large communications databases retained under the *Anti-terrorism, Crime and Security Bill*. He elaborated in a press release, published before the Bill but which, he subsequently asserted,⁵⁶ retained its relevance after:

Sensitive data revealing what you read, where you are, and who you talk to online could be collected in the name of national security. But Mr. Blunkett intends to allow access to this data for purposes nothing to do with fighting terrorism. Minor crimes, public order and tax offences, attendance at demonstrations, even 'health

⁵⁴ http://www.eu2002.dk/news/news_read.asp?iInformationID=21663

⁵⁵ BBC News Online, *Anti-terror laws raise net privacy fears*, 11 November 2001

⁵⁶ Caspar Bowden, Foundation of Information Policy Research, 14 November 2001, personal communication

and safety' will be legitimate reasons to siphon sensitive details of private life into government databases to be retained indefinitely. This would be in flagrant breach of the first and second Data Protection Principles.⁵⁷

In her comments on the Bill, the then Information Commissioner stated that the proposed provisions "could have a significant impact on the privacy of individuals whose data are retained."⁵⁸ She went on:

The Bill pursues the legitimate aims of national security, public safety and the prevention of disorder [or] crime. Article 8(2) imposes a further requirement that any interference be "necessary in a democratic society", i.e. that it fulfils a "pressing social need" and is "proportionate" to the legitimate aim pursued. The scope of the powers proposed to be given to the Secretary of State is immensely broad. The lack of any overt safeguards against abuse of such powers indicate a lack of proportionality such as to render the prospective legislation incompatible with Convention rights.⁵⁹

2. Part 11

With the exception of clause 101, Part 11 of the original Bill emerged largely unamended. The basic requirements of the clause nevertheless found their way into sections 102 and 103 of the *Anti-terrorism, Crime and Security Act 2001*.

Clause 101 [with amendments, section 102 of the Act] provides that the Secretary of State shall issue a code of practice on communications data retention; this may be revised from time to time. He will be required to consult relevant communications providers or their representative bodies before doing so. Originally in clause 101, the consultation procedures were moved, significantly enhanced, to a new clause [section 103 of the Act]. The consultation process is in its closing stages:

The Earl of Northesk asked Her Majesty's Government:

Bearing in mind the urgency alluded to by Ministers at the time of the Bill's passage through Parliament, what progress is being made in implementing Section [sic] 11 of the *Anti-terrorism, Crime and Security Act 2001*.

The Minister of State, Home Office (Lord Falconer of Thoroton): Part 11 of the *Anti-terrorism, Crime and Security Act 2001* requires consultation to take place with the Information Commissioner and industry before implementation. The consultation process, which has concentrated on the terms of a draft code of practice, is now drawing to a conclusion.

⁵⁷ FIPR press release, *Emergency powers allow mass-surveillance for non-terrorist investigations*, 16 October 2001

⁵⁸ Information Commissioner news release, *Information Commissioner contributes to scrutiny of anti-terrorism bill*, 13 November 2001 <http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf>

⁵⁹ *ibid.* (attached memorandum)

In the meantime, as indicated during the passage of the Bill, the industry has co-operated, agreeing voluntary compliance in order to help the security and intelligence services in the fight against terrorism.

The Earl of Northesk asked Her Majesty's Government:

Whether they agree with the statement of the European Union Data Commissioners, as contained in their press release of 11 September following the International Conference in Cardiff, that they have grave doubts as to the legitimacy and legality of current proposals by the European Union governments to introduce mandatory systematic retention of data traffic; and what implications this has for the implementation of Section 11 of the Anti-terrorism, Crime and Security Act 2001 whether under a voluntary or compulsory scheme.

Lord Falconer of Thoroton: The recently agreed European Communications Data Protection Directive Article 15(1) amendment struck a careful balance. The directive ensures that governments in Europe are not prevented from using traffic data to fight serious crime, but underlines the need to ensure that any measures should be appropriate, proportionate and respect the European Convention on Human Rights.

Part 11 of the Anti-terrorism Crime and Security Act 2001 allows for the retention of communications data obtained or held by the communications providers—these are data about communications transactions, not the content of those transactions. It is intended that this is delivered by way of agreements between the Secretary of State and the providers through a code of practice. The Act allows for a review of the operation of the code's requirements and for an order to be made by statutory instrument for directions to be given if necessary.

The statement made by the Data Commissioners, who are an independent advisory group, does not affect the consultation on implementation of the provisions of the Act.⁶⁰

Subsection 2 of clause 101 [section 102 of the Act] allows the Secretary of State to enter into "such agreements as he considers appropriate" with providers on data retention practice. This is restricted by the *Telecommunications (Data Protection and Privacy) Regulations* SI 1999/2093; they contain exemptions on national security and other grounds, however.⁶¹ Since the proposed code is voluntary there would be no penalties for non-compliance. Clause 101(7) [section 102(5) of the Act] provides communications providers with a defence against actions brought by data subjects; the explanatory notes to the Act explain:

⁶⁰ HC Deb 29 October 2002 cc 21-2W

⁶¹ SI 1999/2093, regulation 32

Subsection (5) allows the code or any agreement drawn up under this section to be used in legal proceedings brought against a communications provider by a person whose communications data they hold. Adherence to the terms of the code or agreement may be used as evidence that the retention of data is justified for national security or law enforcement purposes. This provision is intended to prevent a communications provider facing civil liability for retaining data in accordance with the code when they have no further need of it for business purposes.⁶²

Responding to the original Bill the Information Commissioner was "particularly concerned that leaving matters to a voluntary code of practice, or to agreements, may pose difficulties for data protection and human rights compliance."⁶³ She commented on the "absence of clarity as to what information is necessary for law enforcement purposes".

In the latter context, it is interesting to note that section 102(3) of the Act incorporates an amendment, identified below in italics:

(3) A code of practice or agreement under this section may contain any such provision as 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.*

In a submission to the Home Affairs Committee inquiry into the Bill, the Foundation for Information Policy Research has even questioned the utility of data retention:

Stockpiling private and sensitive 'traffic data' on the entire population is not effective in tracking organized crime or terrorist cells. Identification is avoided using pre-paid mobile phones and web-based e-mail from public terminals...

...“Traffic data” constitutes a near complete map of private life: who everyone talks to (by e-mail and phone), where everyone goes (mobile phone location coordinates), and what everyone reads online (websites browsed). Current mobile phones track location to a few hundred meters whilst the phone is switched on (not merely when a call is made), and 3rd generation phones will pinpoint location to a few meters.⁶⁴

Law enforcement agencies in the UK have made use of already available communications data in pursuing their inquiries into the 11 September attacks, a point acknowledged by

⁶² <http://www.legislation.hmso.gov.uk/acts/en/01en24-c.htm>

⁶³ Information Commissioner news release, *Information Commissioner contributes to scrutiny of anti-terrorism bill*, 13 November 2001 <http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf>

⁶⁴ FIPR, *Submission to the Select Committee for Home Affairs Inquiry into the Emergency Anti-Terrorism Bill by the Foundation for Information Policy Research (FIPR)*, 3 November 2001

the former Information Commissioner in a memorandum.⁶⁵ The National Criminal Intelligence Service reportedly takes the view that these events have strengthened the case for internet traffic data retention; however, it did distance itself from a leaked⁶⁶ document, *Looking to the Future*, prepared in August 2000 by the NCIS deputy director-general.⁶⁷ Among the recommendations was a “total retention period for non-specific data before mandatory deletion” of seven years.

Clause 102 [section 104 of the Act] allows the Secretary of State to make an order authorising the giving of directions to service providers about the retention of communications data if, as the *Guardian* put it, “they don't volunteer enough.”⁶⁸ Such an order would be by statutory instrument subject to approval by resolution of each House. Subsection 3 requires that the order must specify the maximum retention period for communications data; 12 months seems the likely figure.⁶⁹ Directions could apply to all communications providers or ones selected either by category or by name (subsection 2). The Secretary of State would have to consult the communications providers or their representatives (subsection 4).

When the Bill was published, the scope of consultation in both clauses 101 and 102 was evidently considered too narrow by the Information Commissioner:

Given the Commissioner's role in enforcing legislation affecting the retention of data it is essential that she be included formally in the consultation process. Given that it is individuals whose data will be retained and possibly accessed by third parties then consideration should be given to consulting formally on a Code with appropriate representatives of the wider community. An appropriate model may be found at section 51(3) of the 1998 Act as this requires the Commissioner to consult with both trade associations and representatives of data subjects as appear appropriate prior to production of a data protection code of practice. The final code [clause 101] should also be drawn to the attention of affected parties not just to communications providers...

...The clause [102] provides for consultation with communications providers before the Secretary of State issues a direction. The earlier comments in relation to consultation on codes of practice and agreements are equally relevant here. The Commissioner would expect to be consulted formally about directions applying to communications providers.⁷⁰

⁶⁵ Information Commissioner news release, *Information Commissioner contributes to scrutiny of anti-terrorism bill*, 13 November 2001 <http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf>

⁶⁶ <http://cryptome.org/ncis-carnivore.htm>

⁶⁷ “The net's eyes are watching”, *Guardian Online*, 15 November 2001

⁶⁸ *ibid.*

⁶⁹ HC Deb 31 October 2001 cc 725-6W

⁷⁰ Information Commissioner news release, *Information Commissioner contributes to scrutiny of anti-terrorism bill*, 13 November 2001 (attached memorandum) <http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf>

As mentioned above, the consultation arrangements in the original Bill were expanded, and the Information Commissioner must now be consulted before the publication of a draft code of practice [section 103 of the Act]. A draft Code must now also be laid before Parliament, and approved by affirmative resolution if it is to come into force. Interestingly, clause 102 remained virtually unchanged: the section [104] of the Act it became merely clarifies that directions from the Secretary of State may only be for the purposes identified in section 102(3) – see above. Though the Information Commissioner does not have to be consulted prior to directions to communications providers, the authority for such directions has to be approved by affirmative resolution of each House (an unamended feature of the original Bill).

Clause 102(7) [section 104(7) of the Act] provides for enforcement (civil proceedings) by the Secretary of State.

Clause 103 [section 105 of the Act] is a sunset measure preventing the Secretary of State from issuing statutory directions if no need to do so has arisen during an initial period of two years after the Act has been passed. However, this initial period can be extended, indefinitely,⁷¹ by two years at a time. To do so, the Secretary of State must make an order by statutory instrument, again subject to the affirmative procedure (subsections 4 and 5). Extending the initial period would retain the possibility of making an order under clause 102 [section 104 of the Act].

Compliance either with voluntary codes of practice or agreements, or with any statutory directions, will inevitably be at a cost to many if not most communication providers.

Clause 104 [section 106 of the Act] places a duty on the Secretary of State to make "appropriate" arrangements for contributing to this "in such cases as he thinks fit". The regulatory impact assessment elaborates:

Government will discuss what arrangements might be appropriate to compensate communication service providers for any additional costs under these provisions, particularly since those that will be most affected will be small/niche-market businesses. The Government has given assurances that measures taken in the context of the emergency legislation should not commercially disadvantage UK business or impact on the confidence of users and operators in the UK as the best place to do e-business. Details of the requirements will be covered in the code of practice.⁷²

⁷¹ clause 103(3)

⁷² <http://www.homeoffice.gov.uk/oicd/antiterrorism/index.htm>

B. Parliamentary debates on the Anti-terrorism, Crime and Security Bill

This section presents a chronological account of parliamentary debates and commentary on the communications data retention measures.

1. Joint Committee on Human Rights

On 14 November 2001, the Joint Committee on Human Rights agreed a report on the *Anti-Terrorism, Crime and Security Bill*. Part 11 of the Bill attracted the following:

69. Part 11 of the Bill deals with the retention of communications data. These are data held by communications providers about the use made of their facilities by customers, such as the telephone numbers dialled from a particular line, the times and duration of calls, and equivalent data in respect of Email communications. They currently fall outside the regime for authorizing surveillance under Chapter 2 of Part I of the Regulation of Investigatory Powers Act 2000.

70. Clause 101 proposes that the Secretary of State should issue a Code of Practice and enter into agreements with providers about the retention of such data. Under clause 102, the Secretary of State would then be empowered to issue directions, by statutory instrument, requiring the providers to make specified provision for the retention of communications data. It would be possible to enforce the directions by civil proceedings. These powers are linked to the maintenance of national security, but also detection or prevention of crime more generally.

71. There is no express limit to the scope of the powers. They could be used to secure highly sensitive data for the purpose of investigating very minor offences, or even for monitoring people's communications without any ground for suspecting them of any offence or of threatening national security. **We note that as the Bill is presently drafted, the Code of Practice relating to the retention of communications data will not be subject to any parliamentary procedure. We also have in mind that a Code of Practice may be used as evidence in courts and tribunals, and that a direction given by a Secretary of State may give rise to legal obligations. In the light of these factors, we consider that measures should be put in place to ensure that the Code of Practice and any directions are compatible with the right to respect for private and family life, home and correspondence under Article 8 of the ECHR, and that those measures should be specified, so far as practicable, on the face of the legislation. We accordingly draw these provisions to the attention of each House.**⁷³

⁷³ Joint Committee on Human Rights, *Anti-Terrorism, Crime and Security Bill*, 14 November 2001, HL 37 HC 372 2001-02

It remains the case that the acquisition and disclosure of communications data provisions of RIPA (Chapter II of part I) have yet to come into force. The *Anti-Terrorism, Crime and Security Act 2001* (ATCSA) provides for parliamentary scrutiny in relation to codes of practice.

The Home Affairs Committee also reported on the Bill prior to second reading, though they focused on other measures in the Bill such as detention of suspected international terrorists.⁷⁴

2. Commons second reading

Prompted by Norman Baker, the Home Secretary justified the Bill's data retention measures during second reading.⁷⁵

Norman Baker: I am grateful to the Home Secretary for that clarification. Why will the powers that he proposes to give the authorities require all communications data to be kept and the authorities to have access to them not simply for the purpose of safeguarding national security, which people will understand, but for the purpose of the prevention and detection of crime, which could be any crime whatsoever? Why are the powers so sweeping and far-reaching?

Mr. Blunkett: Because it has become abundantly clear that it is impossible to distinguish the issues when one cannot separate out crime and terrorist funding, crime and terrorist organisation, and crime used to fund terrorist acts. That is why there is a provision allowing data already held by the service providers to be held under the voluntary code that we intend to put in place.

We thank, as I did on 15 October, the service providers for their co-operation, which we expect to continue. We are providing a reserve power only against people who undercut or damage the reputation and work of others by refusing to take part and co-operate with the code. The data will not include content, merely subscriber details already held and itemised billing, and will be renewable after two years.⁷⁶

Simon Hughes was also concerned about the scope of the data retention measures:

Parts 3 and 11 deal with very important matters concerning the rights of the state to interfere in communications, to find out what communications, technological or otherwise, are passing between people and to require people in the communications industry to hold on to that information for much longer. We have only just legislated in that area. If we need more powers, they should be

⁷⁴ Home Affairs Committee, *The Anti-Terrorism, Crime and Security Bill 2001*, 15 November 2001, HC 351 2001-02

⁷⁵ HC Deb 19 November 2001 cc 21-118

⁷⁶ HC Deb 19 November 2001 cc 37-8

strictly limited to matters to do with terrorism, and they should be much more narrowly drawn. We shall seek to amend parts 3 and 11 to that effect.⁷⁷

Dominic Grieve added:

It appears that there is absolutely no reason why the provision on the communication of data should not be confined to offences that relate to terrorism. I do not understand why it should be so difficult to isolate what is a terrorist offence. Those investigating such offences will know exactly what they are, so it should be possible to frame the Bill to ensure that it is confined to those offences and not to general criminal conduct.⁷⁸

Douglas Hogg identified part 11, and others, as having “simply come out of the Home Office’s back lobby” having nothing to do with terrorism.⁷⁹

Following an amendment in the Lords,⁸⁰ the scope of the powers was additionally constrained to those crimes “which may relate directly or indirectly to national security”.⁸¹

3. Commons committee stage

Committee stage began with an unsuccessful attempt to bring in a new clause dealing with the Bill’s duration.⁸² In this context part 11 of the Bill would have been among those which would automatically cease to have effect two years after the passage of the Act. The Act, indeed the original Bill, does contain a sunset provision relating to *directions* about the retention of communications data.⁸³ And the Act as a whole has to be reviewed by a committee of no fewer than seven Privy Councillors within two years of Royal Assent (13 December 2001). The “review of Act” provisions were finally approved by the Lords during consideration of the Commons Amendments on 13 December 2001.⁸⁴

On the second day of committee stage, the communications data retention measures (clauses 101 to 105) were ordered to stand part of the Bill, without debate or division.⁸⁵

Communications data did not feature in the brief report stage⁸⁶ and briefer third reading.⁸⁷

⁷⁷ HC Deb 19 November 2001 cc 57-8

⁷⁸ HC Deb 19 November 2001 cc 110-1

⁷⁹ HC Deb 19 November 2001 c 94

⁸⁰ HL Dec 6 December 2001 c 982

⁸¹ section 102(3)(b), ATCSA

⁸² HC Deb 21 November 2001 c 342

⁸³ sections 104-5, ATCSA

⁸⁴ HL Deb 13 December 2001 cc 1484-5

⁸⁵ HC Deb 26 November 2001 c 789

⁸⁶ HC Deb 26 November 2001 cc 790-801

⁸⁷ HC Deb 26 November 2001 cc 801-4

4. Lords select committees

Prior to the Bill's⁸⁸ second reading debate in the House of Lords, the Select Committee on Constitution had only time to outline its concerns in a letter to Lord Rooker, then Minister of State, Home Office. "Requirements as to the retention of communications data, including the geographical location from which mobile-telephone calls are made" seemed among those "unrelated, or not limited, to the task of combating terrorism and safeguarding national security".⁸⁹

On 26 November 2001, the Lords Select Committee on Delegated Powers and Regulatory Reform highlighted concerns about the "limited restrictions" applying to the issuing of a code under clause 101 of the original Bill.⁹⁰ It endorsed the views of the Joint Committee on Human Rights:

23. The Joint Committee on Human Rights has also considered this Clause and comments that there is no express limit to the scope of the powers, which could be used to secure highly sensitive data for the purpose of investigating very minor offences, or to monitor people's communications without any ground for suspecting them of any offence or of threatening national security. The Joint Committee considers that measures should be put in place to ensure that "the Code of Practice and directions are compatible with the right to respect for private and family life, home and correspondence under Article 8 of the ECHR, and that those measures should be specified, so far as practicable, on the face of the legislation". **We endorse these views, and invite the House to consider the most appropriate way in which this principle should be given effect. A possible method would be for the draft of any Code under Clause 102 to be submitted to the Joint Committee on Human Rights for its scrutiny.**⁹¹

As noted elsewhere in this paper, the procedure for codes of practice was subsequently modified to include consultation with the Information Commissioner and to allow for parliamentary scrutiny.

5. Lords second reading

In the second reading debate, Lord Rooker introduced Part 11 of the Bill as follows:

Part 11 relates to the retention of communications data. Communications data have been central to the investigation into the terrorist attacks of 11th September. This data has been available because of the excellent co-operation shown by communications service providers. But currently, the data should normally be

⁸⁸ HL Bill 29 2001-02

⁸⁹ Select Committee on the Constitution, *Anti-Terrorism, Crime and Security Bill*, 22 November 2001, HL 41 2001-02

⁹⁰ HC Bill 49 2001-02 (clause 102 of HL Bill 29 2001-02)

⁹¹ Select Committee on Delegated Powers and Regulatory Reform, *Anti-Terrorism, Crime and Security Bill*, 26 November 2001, HL 45 2001-02

erased once it is no longer needed for business purposes--that is, once the bill has been sent out.

Effectively, all we are asking for is the retention of the billing detail that any noble Lord would see on a telephone bill; namely, the date a call was made, the number to which it was made, and the time and duration of the call. There is no conversational content in the billing details--indicating that we are not seeking that. We are seeking the billing information. It is possible to tell the locations of the mobile phones from which calls are made. That is extremely useful information. They may be mobile, but they are not so mobile as some of the terrorists might think. This is not an issue of eavesdropping on people's personal correspondence or phone calls, whether they be e-mails or telephone conversations. Effectively we seek only the retention of the billing data.

The plan is that this will work on a voluntary basis. We believe that we can work well with the industry; so far, co-operation has been good. All the powers used will be fully in line with the European Convention on Human Rights and the Regulation of Investigatory Powers Act. There will be no generalised expeditions; they will all be related to specific inquiries and will conform to the terms of the legislation. We shall work with the industry on a voluntary code of practice to support this work. There is a reserve power, in case the voluntary system does not work, to bring in a statutory power.⁹²

In his contribution, Lord McNally alluded to communications data:

As regards the parts of the Bill relating to communications service providers, I believe that some of us will recognise old friends and old arguments from the debate on the Regulation of Investigatory Powers Act. In a brief provided by the CBI on this section of the Bill, a point was made which I believe is a common theme and criticism. It states:

"The CBI believes that a wholly greater set of demands is being made--and one of much greater cost to business freedom and practices--if the Bill introduces new powers for the investigation of minor crimes or crimes which do not relate to terrorist activity".

That is a perfect example of sweeping up and shelf clearing to grab new powers.⁹³

Lord Phillips of Sudbury referred to the Technical Advisory Panel,⁹⁴ established under section 13 of RIPA to advise the Home Secretary on the reasonableness of obligations imposed on communications service providers (in the context of *interception* of communications):

⁹² HL Deb 27 November 2001 c 152

⁹³ HL Deb 27 November 2001 c 161

⁹⁴ <http://www.technicaladvisoryboard.org.uk/index.htm>

Part 11 of the Bill will allow the Government to require "communications providers" to store information for such period as the Minister may require. Initially, there is to be a voluntary code on retention of information but, if the Secretary of State believes that it is necessary so to do, he or she can then make a mandatory order requiring information to be stored for such period as the Minister may require. In this House we struggled to have reference to the Technical Advisory Board inserted in the Regulation of Investigatory Powers Act. That board is not referred to. I think that the Minister will agree that such a provision is a protection against misuse of some of the powers which are provided under the Bill.⁹⁵

Lord Rooker assured the House that the Technical Advisory Board "...will play its role. The procedures on disclosure of information will follow the RIPA rules, and will be ECHR compliant."⁹⁶ The ATCSA makes no mention of the Technical Advisory Board, despite the hope of Lord Phillips of Sudbury that such a reference could be inserted. He went on:

Some will say that the innocent have nothing to fear by disclosure. It is only the wicked and villains who should worry. But that is not true. The right to privacy long predates any human rights legislation. It is not a right in the formal sense but one that citizens of these lands have enjoyed since time immemorial. The Government would misjudge public opinion and anxiety if they were to proceed on an extraordinarily broad front with extraordinarily broad powers.

It is common sense and reality that there are rotten apples even in a well-run police force or security organisation--and rotten apples will use powers given by the Bill perniciously. The more intrusive and secretive the powers, the more pernicious the abuse. It is not paranoid to worry about such matters. Only last summer we discovered that the national databank that is supposed to destroy fingerprints and genetic materials taken from suspects had failed to discharge no fewer than 50,000 sets, which were languishing on the databank long after they were legally there. We should not tempt persons who are corruptible or who are likely to take short cuts by littering the statute book. Even if one only subscribes to the cock-up theory of life, the proposed powers are far too wide. I hope that the Government will listen to all parts of the House as the Bill progresses.⁹⁷

The Earl of Northesk took an especial interest in the Part 11 provisions, which he subjected to four tests: effectiveness, necessity, proportionality and consequence.⁹⁸ He accepted that access to communications data had been central to the investigation of the terrorist attacks on 11 September 2001; its effectiveness lay in its use as an investigative tool after the event. He was concerned that the "stockpiling" of internet and telephone

⁹⁵ HL Deb 27 November 2001 c 247

⁹⁶ HL Deb 27 November 2001 c 248

⁹⁷ HL Deb 27 November 2001 c 248

⁹⁸ HL Deb 27 November 2001 cc 250-5

traffic could provide information overload (a point also made by Baroness Buscombe),⁹⁹ stymieing the law enforcement and intelligence services. Furthermore, terrorists could circumvent the measures by using pre-paid mobile phones or web-based email from public terminals or low-tech communications (the informal money-transfer hawala¹⁰⁰ system was referred to).

The Earl of Northesk quoted Jonathan Bamford, Assistant Commissioner to the Information Commissioner: “Part 11 isn’t necessary, and if it is necessary it should be made clear why”. The UK National Hi-Tech Crime Unit had evidently submitted a request to ISPs and telcos¹⁰¹ (who complied) for the retention of communications logs for 11 September 2001 – a request the Information Commissioner had considered lawful and proportionate.

Moving to proportionality, the Earl of Northesk commented that the Bill was “not limited to providing data retention in respect of the current terrorist threat.”¹⁰² He cited an article in *Tribune* where the Home Secretary had given “apparent assurances” to the contrary. The relevant section of David Blunkett’s article is quoted here:

There is another area of proposed change which I can understand raises concerns; namely our work with telecommunications companies to ensure retention of records and access by law enforcement agencies to them.

Our measures will not give the police or anyone else the power to read e-mails or routinely monitor phone calls or e-mails between individuals. However, we do need – strictly in the case of a criminal investigation against suspected terrorists – to have access to more information than we have at present. That is why we are working with companies on a code of practice with the result that they will keep billing records for longer than at present, to allow access in relation to anti-terrorist activity.¹⁰³

Lord Goodhart later asserted that “Unless Part 11 is limited to terrorist crimes, it should not be in the Bill.”¹⁰⁴

Finally, the Earl of Northesk’s contribution on Part 11 dealt with consequence: both for the privacy of the individual and the compliance costs to industry:

The data retention regime promoted in the Bill will effectively transform our communications infrastructure--or may do--into a form of mass domestic

⁹⁹ HL Deb 27 November 2001 c 275

¹⁰⁰ “Hawala system under scrutiny”, *BBC News Online*, 8 November 2001
<http://news.bbc.co.uk/1/hi/business/1643995.stm>

¹⁰¹ internet service providers and telecommunications companies

¹⁰² HL Deb 27 November 2001 c 252

¹⁰³ “Democracy must be vigorously defended”, *Tribune*, 26 October 2001 p 21

¹⁰⁴ HL Deb 27 November 2001 c 269

surveillance. That represents an unwarranted invasion of privacy because it creates a regime where details of the personal life of all citizens will be available to public authorities with inadequate checks and balances...

...There will be a not inconsiderable financial cost to ISPs and telcos, albeit that the Bill makes allowance for appropriate moneys to be paid out of public funds. None the less there is a real risk that,

"Extra costs arising from retention could increase overheads to the point where cheap transatlantic bandwidth makes it attractive to locate servers in offshore subsidiaries where requirements are less onerous".

The Government may seek to defuse this by highlighting the voluntary nature of the scheme--ISPs will not be obliged to retain data. But, in so far as it is argued that this is a key component of the efforts to counter terrorism, it suggests that the scheme is redundant even before its implementation. The consequence is that, in very short order, the Home Secretary is likely to use the reserve powers granted to him under the Bill to introduce a mandatory scheme that will be subject to a dearth of parliamentary scrutiny or accountability.

That said, my impression is that the industry is less concerned about financial aspects than technical ones. As I said, the volumes of data that will be subject to retention are vast. The consequence for most telcos and ISPs will be that management of compliance with the data retention regime will become so time consuming and routine that it impacts seriously on the successful running of their businesses. Inevitably, those various factors will compromise the competitiveness of the IT industry. As recognised by the CBI, the proposed data retention regime could damage consumer confidence in e-commerce and commercial exploitation of IT in the UK. I merely speculate how those consequences can reasonably be squared with the Government's stated policy of making the UK the best place in the world for e-commerce.¹⁰⁵

Digressing briefly to express a particular concern over the "data matching or data sharing" provisions in Part 3, the Earl of Northesk returned to Part 11:

I have detained your Lordships for longer than I might have wished, albeit that I have barely scratched the surface of the complexities of these parts of the Bill. I apologise on both counts. In my defence, these are very serious issues that merit proper examination and explanation. Because public opinion and the attention of parliamentarians are so unsighted on the substance of these issues, it could be argued that Part 11 is one of the more insidious elements of the Bill.¹⁰⁶

¹⁰⁵ HL Deb 27 November 2001 cc 253-4

¹⁰⁶ HL Deb 27 November 2001 c 255

6. Joint Committee on Human Rights – further report

The Joint Committee on Human Rights returned to the Bill, agreeing a further report on 3 December 2001. Among the more general comments, were the following:

We share the view of the House of Lords Select Committee on the Constitution that the inclusion of many non-emergency measures was inappropriate in emergency legislation which was required to be considered at such speed.[13] Even with the best efforts of the committees of the two Houses to subject the Bill to some degree of scrutiny, this is not a proper or sensible way to make legislation.¹⁰⁷

Part 11 also received specific consideration in the report:

Part 11 of the Bill: retention of communications data

29. Part 11 of the Bill would give wide discretion to the Secretary of State to issue a code of practice relating to the retention of communications data by communications providers. These data include very detailed information about geographical locations from which telephone calls are made, as well as other information relating to individual communications. The Secretary of State would also be able to enter into agreements with communications providers about practices to be followed, and to take power by statutory instrument to give directions to communications providers.

30. In our Second Report, we expressed concern about the lack of express limits to these powers, which 'could be used to secure highly sensitive data for the purpose of investigating very minor offences, or even for monitoring people's communications without any ground for suspecting them of any offence or of threatening national security.' In view of the absence of safeguards for the principle of proportionality, we took the view that—

... measures should be put in place to ensure that the Code of Practice and any directions are compatible with the right to respect for private and family life, home and correspondence under Article 8 of the ECHR, and that those measures should be specified, so far as practicable, on the face of the legislation.[46]

We note that the House of Lords Delegated Powers and Regulatory Reform Committee, with its immense experience in scrutinizing provisions in Bills which would confer power to make subordinate legislation, has endorsed this view, and has recommended that we should be responsible for scrutinizing a draft of any code of practice to be issued under clause 102.[47]

¹⁰⁷ Joint Committee on Human Rights, *Anti-Terrorism, Crime and Security Bill: Further Report*, 3 December 2001, HL 51 HC 420 2001-02

31. We regard this as an appropriate way forward to ensure that Parliament can satisfy itself that any Code plays its part in securing adequate safeguards for rights under Article 8 of the ECHR. **We recommend that clause 102 should be amended to require parliamentary scrutiny of any such code of practice in draft. We accordingly draw this once more to the attention of each House.**¹⁰⁸

At this stage there had been no amendments to part 11, bar the shifting of the relevant clause numbers (upwards, by one). Clause 102 here (HL Bill 29) is identical to clause 101 of the original Bill (HC Bill 49). Ultimately, the Act did address the Committee's recommendation and make reference to national security.

7. Lords committee stage

Committee stage in the Lords saw the first clause¹⁰⁹ in part 11 amended to include a requirement that the Secretary of State consult the Information Commissioner when issuing or revising a code on communications data retention. The relevant amendment¹¹⁰ was moved by the Earl of Northesk and supported by Lord Goodhart. For the Government, Lord Rooker said:

I ask Members opposite not to fall over because I am going to accept it. The parliamentary draftsman produced a better form of wording, but I asked what difference it would make. The answer was: none. It is much easier to make it abundantly clear—I hope that this meets the noble Lord's point about the Information Commissioner—that we have no intention of cutting out the Information Commissioner in any way, shape or form. He has a statutory function to perform and will be consulted fully beforehand.

What we do not consider to be a good idea is a joint code issued by government, industry and the Information Commissioner. That would be wholly impractical. The buck stops with the Home Secretary.¹¹¹

The latter paragraph was a reference to another amendment calling for the Secretary of State to issue a draft code jointly with business representatives and the Information Commissioner. Lord Rooker did go on to assure the House that “No one will be excluded from making a representation” before the issue of a final code.¹¹² One amendment,¹¹³ subsequently withdrawn, would have required the Secretary of State to publish the voluntary code or, as the case may be, the terms of an agreement with communications providers. Lord Rooker anticipated being able to publish the “more general” code but not

¹⁰⁸ *ibid.*

¹⁰⁹ clause 102, HL Bill 32 (clause 101, HC Bill 49)

¹¹⁰ Amendment No. 164D

¹¹¹ HL Deb 4 December 2001 cc 756-7

¹¹² HL Deb 4 December 2001 cc 758-9

¹¹³ Amendment No. 165

the full agreements, the latter likely containing “detailed, commercially sensitive and confidential information about individual service providers.”¹¹⁴

The Earl of Northesk also moved, and subsequently withdrew, an amendment aimed at securing that the provisions of the data retention code be proportionate – constrained by considerations of national security. Lord Phillips of Sudbury made the proportionality point in the following way:

Enough was said at Second Reading for the Minister and the Government to be aware of the widespread concern about this part of the Bill. The effects of the warehousing arrangements that these provisions will allow will create a source of potential information for the state which, frankly, has been contemplated only in the novels of George Orwell. We, like the Conservative Front Bench, feel as strongly as we can that the Bill has been introduced for entirely legitimate reasons; namely, national security in the face of an emergency threat. However, we do not and will not accept that it is legitimate to go beyond that and “piggyback” on that legitimate purpose the complete range of criminal offences, at whatever level.

I remind the Committee of a report by the National Criminal Intelligence Service, which was leaked last year and is now available in full on the Internet. The report was publicised in the Observer. The memorandum proposes the creation of a “national traffic data warehouse” on grounds that are found in this and the succeeding clause. The unease that that creates on these Benches is added to because the memorandum is also the fruit of MI5, MI6, GCHQ, ACPO and Customs and Excise. One need not dwell in the lands of paranoia to believe that a fundamental issue of basic and traditional liberty is involved, and that that makes this group of amendments not only necessary but essential.

On the national security question, Viscount Goschen, while prepared to accept additional measures for this purpose, argued that the face of the bill allowed for investigation of a wide range of crimes.¹¹⁵ Lord Elton:

It is easy to anticipate the Minister's response. It will be, as it has been so often, that any crime is potentially a terrorist crime, whether it is shoplifting, breaking the speed limit or blackmail. For that reason we are hesitant about giving the Government the emergency power procedure for the processing of this Bill.¹¹⁶

Lord Peyton of Yeovil wondered if difficulties in defining terrorism could really account for the apparently wide powers in the Bill:

¹¹⁴ HL Deb 4 December 2001 c 761

¹¹⁵ HL Deb 4 December 2001 cc 766-7

¹¹⁶ HL Deb 4 December 2001 c 767

But I cannot think of any other reason why the Government should want so obstinately to bring down on their head such a degree of very deeply entrenched opposition. There is no party ingredient in it at all. It is an opposition from people who would willingly arm the Government with any powers that are plainly necessary or desirable to secure the defeat of terrorism. But to give them such powers “just for good measure” to perform a much wider function is quite intolerable.¹¹⁷

Lord Rooker prefaced his response by reminding the House not to confuse retention of data with access to it. He dismissed proposals to restrict access provisions to national security as betraying “a misunderstanding of how the terrorists operate. We cannot draw a distinction between terrorist activity and other crimes; that would be incredibly difficult.”¹¹⁸ He went on:

Removing the second purpose of the code and agreements, which is to prevent and detect crime and to prosecute offenders, would make no sense in practice. It would not affect requests to access the data, which will be regulated not under the Bill but under the Regulation of Investigatory Powers Act 2000 and overseen by the Interception Commissioner. However, it would undermine the operational efficiency of the police in combating crime because their wider responsibilities could not be taken into account in drawing up the code. The provision will rely heavily on the code, which, I repeat, is voluntary.¹¹⁹

He argued there was no need for an explicit proportionality clause:

The code must comply with the principles set out in the 1999 telecommunications regulations and the Data Protection Act 1998. Both of those pieces of domestic legislation implement EC directives that were designed to be compliant with Article 8—the right to privacy—of the European Convention on Human Rights. Proportionality and necessity are key principles of the ECHR.¹²⁰

Another concern during committee stage was the potential legal liabilities that communications providers might find themselves exposed to – for example in respect of the *Data Protection Act 1998*. The Earl of Northesk moved, and later withdrew, an amendment to give communications providers more explicit protection than the Bill (and the subsequent Act):

The amendment in this context seeks to provide a clear and unambiguous statement that in relation to the retention of data the Act we are debating today overrides conflicting legislation so that CSPs who comply with a code, agreement or direction can do so secure in the knowledge that they cannot be made legally liable in so doing. The Minister should be under no illusions as to the importance

¹¹⁷ HL Deb 4 December 2001 c 769

¹¹⁸ HL Deb 4 December 2001 c 772

¹¹⁹ HL Deb 4 December 2001 c 773

¹²⁰ HL Deb 4 December 2001 cc 773-4

of that. Without absolute certainty about liability, the voluntary code simply cannot work.¹²¹

Lord Rooker countered:

Removing the possibility of legal challenge to service providers' retention practices would undermine the Government's commitment to ensuring that personal data are treated fairly and responsibly in line with the Data Protection Act. These protections work only if subject to a challenge in the court.

In any event, we intend to draw up a code of practice that is compliant with data protection and human rights legislation and to consult fully with the Information Commissioner to ensure that the drafting reflects that. It is, therefore, entirely unnecessary and, indeed, bordering on the unhelpful, to introduce any kind of immunity clause.¹²²

Another amendment, also withdrawn after debate, sought to place on the Secretary of State a duty to avoid placing an unreasonable burden on communications providers. A code of practice or agreement would not expect or require them to retain any class of data not already obtained or held in the normal course of business. Lord Rooker provided reassurance on this:

The provisions are flexible enough to distinguish data that are of use to law enforcement and should be kept, and data that are of no interest to national security or the detection of crime. Records of standard operational procedures or the product of the functioning of computer systems, for example, should not be kept because that has nothing to do with the purpose for which the codes allow data to be kept. The provisions apply only to communications data that are already held by providers. We have no intention of asking them to retain data that are not collected in the normal course of their business. They are being asked to do nothing new.¹²³

Debate on the next clause¹²⁴ of part 11, covering directions about retention of communications data, focused on two amendments: the first was designed to restrict the clause's purpose (safeguarding against terrorism) and to limit its duration (until a revised voluntary code could be put in place); the other debated amendment sought to ensure directions applying generally were restricted to *public* communications providers. Both were subsequently withdrawn. Other amendments, not moved, sought to ensure greater demonstration that any statutory directions were more fully justified and proportionate. Lord Rooker acknowledged these concerns:

¹²¹ HL Deb 4 December 2001 cc 790-1

¹²² HL Deb 4 December 2001 c 791

¹²³ HL Deb 4 December 2001 c 796

¹²⁴ clause 103, HL Bill 32 (clause 102, HC Bill 49)

I take the point behind the amendments. I can make one commitment that may answer the Committee's suspicion. I cannot read out a list of criteria by which we would decide, if necessary, to switch from a voluntary to a mandatory scheme. However, during consultation on the code of practice, an objective set of criteria to determine its success or failure will be drawn up.¹²⁵

The debate's emphasis on public communications providers related to the growing popularity of private networks and of direct communications between individual computers (peer-to-peer, or P2P, networking). Elaboration by Lord Phillips of Sudbury¹²⁶ was underlined by the Earl of Northesk:

In terms, therefore, the Bill potentially requires private computers, perhaps even down to the level of the individual user, to log arbitrary data. If it applies at that level and users are required to log traffic and report usage upon government request, not only will it be an unwarranted intrusion upon the individual but it could also severely impair research and development of a number of P2P software applications.¹²⁷

Lord Rooker gave the following response:

Although the provisions in the Bill and those in the RIP Act will bite in the main where they are intended to do so—namely, on providers who provide a service to the public, such as BT, Orange and Vodafone—we do not wish to rule out the possibility—I put it no more strongly than that—of ensuring that communications data relating to private networks are retained where they might be necessary for national security or crime prevention purposes.¹²⁸

Lord Rooker went on to emphasise that talk of mass surveillance was “extravagant and extreme”, and that “mass trawls of thousands of people” were not on. “That is not what this legislation is about. It is not what the code of practice will cover.”¹²⁹ He added:

Several times I made it absolutely clear that the code of practice will conform to all necessary legislative safeguards, including—and I mentioned this twice—Article 8 of the European Convention on Human Rights. I specifically put that on the record.¹³⁰

Lord Thomas of Gresford questioned the “handing of powers of considerable potential to the executive”, accepting it was not the present Government's intention to embark on mass surveillance.¹³¹

¹²⁵ HL Deb 4 December 2001 c 800

¹²⁶ HL Deb 4 December 2001 cc 801-2

¹²⁷ HL Deb 4 December 2001 cc 802-3

¹²⁸ HL Deb 4 December 2001 c 804

¹²⁹ HL Deb 4 December 2001 c 809-10

¹³⁰ HL Deb 4 December 2001 c 813

¹³¹ HL Deb 4 December 2001 cc 811-4

Committee stage deliberations on Part 11 ended with the Earl of Northesk moving an amendment to give communications service providers a right of appeal against requests for data retention. The Tribunal set up under RIPA was nominated. While a voluntary code would not, Lord Rooker noted, require an appeal mechanism, in so far as directions were concerned he pointed out that judicial review would be available.¹³²

8. Final stages

Most of the amendments to Part 11 came after the Lords Committee Stage. These included subjecting the codes of practice on data retention to parliamentary scrutiny – by requiring a draft code to be laid before parliament, and for its bringing into force to require approval of a statutory instrument, by affirmative resolution. Another change was highlighted and discussed by Michael Zander in *New Law Journal*:

The House of Lords qualified these [data retention] powers by an amendment, moved by Lord Phillips and passed by 228 to 133, limiting them to criminal activity directly or indirectly related to national security (HL, Dec 6, col 982). Again, the Government rejected the amendment but, where a little earlier the Tories had bottled out on this issue, here, illogically, they stood firm. At 7.15 pm on the final day the Opposition motion moved by Lord Phillips carried the day by 196 to 145 (HL, Dec 13, col 1479) and at the last gasp, at 10.30 pm the Government conceded the point in the Commons (HC, Dec 13, col 1121).¹³³

As the commentary above indicates, amendments relating to data retention, whether by voluntary code or statutory direction, were initially agreed to during the first day of the Lords report stage. Speaking to these amendments, The Earl of Northesk said:

None of us disputes that law enforcement should have adequate powers to counter the threat of global terrorism. We all share that aspiration. But those powers should not overreach themselves unnecessarily. As our debates on this issue have demonstrated so visibly, there is widespread concern that that is precisely what the Bill does.

Moreover, as I have argued consistently, there is a very real risk that the vast accumulations of data that the Bill currently envisages could prove counter-productive in terms of providing the type of focused intelligence that is required to combat terrorism. By making the powers too broad, the Bill could have the perverse effect of hampering our law enforcement agencies and intelligence services in their admirable work; nor should we underestimate how great a problem that would present in terms of data subjects' right of access to information about them under the Data Protection Act.¹³⁴

¹³² HL Deb 4 December 2001 cc 816-7

¹³³ “The Anti-terrorism Bill – what happened?”, *New Law Journal*, 21 December 2001 pp 1880-1

¹³⁴ HL Deb 6 December 2001 c 954

The amendments agreed to required that data retention codes, agreements or directions *may* relate at least indirectly to national security.

During the debate, Lord Rooker also announced¹³⁵ that the Government would be bringing forward an amendment to ensure the code of practice on data retention would be subject to the affirmative resolution procedure of both Houses. The relevant amendments were agreed to, without division, during third reading.¹³⁶ Speaking to these, Lord Rooker said:

I shall be brief because we debated the matter last Thursday when I promised to bring forward an amendment to introduce parliamentary approval of the voluntary data retention codes of practice. It will provide a further safeguard to ensure that data protection and human rights legislation is complied with. Together with the duty to consult the Information Commissioner and the industry, it will, I hope, ensure that an appropriate balance is struck between security and civil liberties.

The practical effect of the amendment is to split the process of drawing up the code of practice into two stages. First, there will be a consultation with the parties directly involved: the service providers, the law enforcement agencies and the Information Commissioner. That will lead to the publication of a draft code. The next stage is a period of public consultation when comments will be welcomed from any quarter, irrespective of whether people were consulted in the first place. Following that consultation, the code will be laid before Parliament for approval by the affirmative resolution procedure.¹³⁷

III Further reading

House of Commons Library Research Paper 00/25, *The Regulation of Investigatory Powers Bill*, 3 March 2000

House of Commons Library Research Paper 01/98, *Anti-terrorism, Crime & Security Bill, Parts III & XI: Disclosure and Retention of Information*, 19 November 2001

House of Commons Library Research Paper 02/54, *Anti-terrorism, Crime and Security Act 2001: Disclosure of Information*, 4 October 2002

Parliamentary Office of Science and Technology, *Electronic Privacy*, postnote 183, October 2002

¹³⁵ HL Deb 6 December 2001 c 963

¹³⁶ HL Deb 11 December 2001 cc 1282-8

¹³⁷ HL Deb 11 December 2001 c 1282

Home Office, *Regulation of Investigatory Powers (RIPA) Act 2000*, homepage
<http://www.homeoffice.gov.uk/ripa/ripact.htm>

Home Office, *Anti-terrorism, Crime and Security Act 2001*, homepage
<http://www.homeoffice.gov.uk/oicd/antiterrorism/index.htm>

Performance and Innovation Unit, *Privacy and data-sharing: The way forward for public services*, April 2002
<http://www.cabinet-office.gov.uk/innovation/2002/privacy/report/>

“Privacy on the internet”, *Guardian Unlimited Special Report*
<http://www.guardian.co.uk/netprivacy>

Foundation for Information Policy Research, *Surveillance and Security*
<http://www.fipr.org/surveillance.html>

Jason Saiban and John Sykes, “UK Anti-Terrorism Act 2001 & ISP’s”, *Computer Law & Security Report*, Vol. 18 no. 5 2002 pp 338-9

Chris Pounder, “Anti-Terrorism Legislation: The Impact on The Processing of Data”, *Computers & Security*, Vol. 21 no. 3 2002 pp 240-5

Philip Westmacott, “Anti-Terrorism Legislation – UK: Big Brother never forgets – the data retention provisions of the Anti-Terrorism, Crime and Security Act 2001”, *Computer Law & Security Report* Vol. 18 no. 3 2002 pp 205-7

Michael Zander, “The Anti-terrorism Bill – what happened?”, *New Law Journal*, 21 December 2001 pp 1880-1

Jane Swann, “One year on”, *Solicitors Journal*, 25 October 2002 p 963