



RESEARCH PAPER 01/98
19 NOVEMBER 2001

Anti-terrorism, Crime & Security Bill, Parts III & XI: Disclosure and Retention of Information

Bill 49 of 2001-02

The *Anti-terrorism, Crime and Security Bill* was introduced in the Commons on 12 November 2001 and is due to be debated at Second Reading on 19 November.

Part 3 contains powers intended to ensure that public authorities, including the Inland Revenue, can disclose certain types of otherwise confidential information where this is necessary for the purposes of fighting terrorism and other crimes.

Communications and traffic data, such as itemised telephone bills and records of emails sent, are retained by service providers for billing and other business purposes. Under Part 11 of the Bill, communications service providers (telephone and internet companies for example) will be able to retain this information for longer than would be normal under the *Data Protection Act 1998*.

A general introduction to the Bill is given in Research Paper 01/101. Other aspects are discussed in Research Papers 01/92, 01/94, 01/96, 01/97 and 01/99

Antony Seely

BUSINESS AND TRANSPORT SECTION

Grahame Danby and Edward Wood

HOME AFFAIRS SECTION

HOUSE OF COMMONS LIBRARY

Recent Library Research Papers include:

List of 15 most recent RPs

01/88	Members' Office Costs – the new system	08.11.01
01/89	The <i>Animal Health Bill</i> [Bill 39 of 2001-02]	08.11.01
01/90	The <i>British Overseas Territories Bill</i> [Bill 40 of 2001-02]	13.11.01
01/91	Unemployment by Constituency, October 2001	14.11.01
01/92	The <i>Anti-terrorism, Crime and Security Bill</i> , Part XII: Anti-Corruption Legislation [Bill 49 of 2001-02]	15.11.01
01/93	The <i>Employment Bill</i> [Bill 44 of 2001-02]	15.11.01
01/94	The <i>Anti-terrorism, Crime and Security Bill</i> , Parts VI & VII: Pathogens, Toxins & Weapons of Mass Destruction [Bill 49 of 2001-02]	15.11.01
01/95	The <i>National Health Service Reform and Healthcare Professions Bill</i> [Bill 47 of 2001-02]	15.11.01
01/96	The <i>Anti-terrorism, Crime and Security Bill</i> , Parts IV & V: Immigration, asylum, race and religion [Bill 49 of 2001-02]	16.11.01
01/97	The <i>Anti-terrorism, Crime and Security Bill</i> , Part X: Police powers [Bill 49 of 2001-02]	16.11.01
01/98	The <i>Anti-terrorism, Crime and Security Bill</i> , Parts III & XI: Disclosure and Retention of Information [Bill 49 of 2001-02]	19.11.01
01/99	The <i>Anti-terrorism, Crime and Security Bill</i> , Parts I, II, VIII, IX & XIII: Property, Security and Crime [Bill 49 of 2001-02]	19.11.01
01/100	The <i>Age Equality Commission Bill</i> [Bill 10 of 2001-02]	16.11.01
01/101	The <i>Anti-terrorism, Crime and Security Bill</i> Introduction and Summary:	19.11.01

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

Part 3 of the Bill would give HM Customs and Excise and the Inland Revenue powers to disclose information held by them for law enforcement purposes and to the intelligence services. Part 3 also clarifies and extends a number of existing powers to disclose information from public authorities to agencies involved in criminal investigations and proceedings. The new powers are intended to ensure that public authorities can disclose certain types of otherwise confidential information where this is necessary for the purposes of fighting terrorism and other crimes.

Provisions similar to those in part 3 of the Bill were included in the *Criminal Justice and Police Bill 2000-01*. On 9th May 2001, the Government agreed to their removal at the Bill's Report stage in the Lords in order to secure the passage of the Bill as a whole, given the proximity to the general election. The debates on part 2 of the former Bill are discussed in part I of this paper. In addition, there is a general introduction which discusses the Performance and Innovation Unit's work on data sharing, and a selection of comments on part 3 of the current Bill.

Communications and traffic data, such as itemised telephone bills and records of emails sent, are retained by service providers for billing and other business purposes. These data do not include the content of the communications, but can provide a map of one's daily life and contacts. The *Data Protection Act 1998* provides enforceable criteria governing the length of time such data may be held.

Under Part 11 of the Bill, communications service providers (telephone and internet companies for example) will be able to retain this information for longer than would be normal under the 1998 Act. A period of 12 months has been suggested in a written answer.

At least initially, the communications industry would be expected to adhere to a system of voluntary codes and agreements on data retention. Access to this data by law enforcement agencies is governed by Part I Chapter II of the *Regulation of Investigatory Powers Act 2000*.

The Bill contains provisions to allow the Secretary of State to issue statutory directions to communications service providers if he considers the voluntary retention system unsatisfactory. These powers are subject to a "sunset" clause in that they must be exercised within an (extendable) initial period, if at all.

Debate on these provisions has centred on the potential violation of individual privacy and the cost to industry. Furthermore, the degree to which they will be effective in fighting serious crime has also been discussed.

The appendix to this paper describes briefly the extension to the powers of GCHQ which is proposed in part 13 of the Bill.

CONTENTS

I	Part III: Disclosure of Information	7
	A. Data Sharing	7
	B. Background to Part III of the Bill	11
	C. Part III of the Bill	23
	D. Reactions to the Disclosure of Information Provisions	25
II	Part XI: Retention of communications data	27
	A. Access to communications data	27
	B. Retention of communications data	31
	C. Anti-terrorism, Crime and Security Bill 2001/02	34
	1. General	34
	2. Part XI of the Bill	36
	Appendix: Amendments of the Intelligence Services Act 1994	39

I Part III: Disclosure of Information

Part 3 of the Bill would give HM Customs and Excise and the Inland Revenue powers to disclose information held by them for law enforcement purposes and to the intelligence services. Part 3 also clarifies and extends a number of existing powers to disclose information from public authorities to agencies involved in criminal investigations and proceedings. The Explanatory Notes state:

The gateways will ensure that public authorities can disclose certain types of otherwise confidential information where this is necessary for the purposes of fighting terrorism and other crimes.¹

A. Data Sharing

In September 2000, the Prime Minister asked the Performance and Innovation Unit (PIU) in the Cabinet office to produce a report on privacy and data issues. The Written Answer announcing the project suggested the Government saw a need to balance respect for the privacy of the individual with the usefulness to government departments and agencies, etc of being able to share data with other such bodies:

Privacy and the protection of personal information has increased in importance with developments in IT. Data-sharing is a key to modernising government, to facilitating seamless electronic delivery of government services, to reducing fraud against government, and to encouraging e-commerce.²

A “scoping note” on the project was more explicit on this point:

It is an important goal for government to strike the right balance between harvesting the benefits offered by data-sharing, and ensuring that sufficient safeguards are in place such that personal information is kept and used in a manner which is responsible, secure, and legal. The promotion of privacy in its own right (and not simply as a perceived constraint on data-sharing) is an equally important objective.³

The sponsor minister for the project was Lord Falconer of Thoroton. The terms of reference were to analyse “a broad range of issues involved in privacy and the use of personal data, including current government, private sector and international practices, structural and technological issues, public attitudes and the current legal framework”.

¹ Para 10

² HL Deb Vol 616, 28.9.00, 196WA

³ *Privacy and Data*, 1.11.00, www.cabinet-office.gov.uk/innovation/2000/privacy/datascope.shtml

The project also examined “a range of issues to do with identification and authentication, including identification numbers and smartcards”⁴.

The scoping note gave further background. The following benefits and risks of data sharing were noted, as well as the benefits of increased privacy:

Benefits of data-sharing

Data-sharing delivers a range of benefits, for both the individual and society. They include:

- ***better public services***: the ability to share personal data means that services can be personalised and more convenient for the citizen.
- ***cutting costs***: significant savings can be made when data-sharing enables electronic delivery (e.g. the ‘Herts connect’ local government initiative delivered an estimated cost saving of £20 million) and when it is used to cut down welfare fraud (DSS estimate that they saved £150 million in 1998/99 through data-sharing; they foresee additional saving with further data sharing);
- ***cutting red tape***: data-sharing can cut down on the amount of information that an individual or organisation has to give to more than one institution (e.g. schools giving the same information to DfEE and OFSTED, as noted in the Better Regulation Task Force report).
- ***cutting crime***: Police use DVLA information to trace suspected criminals, and other data to break organised crime rings.
- ***better policy making***: the recent PAT18 report recommended that better information in a number of areas would enable social exclusion to be tackled more effectively.
- ***economic benefits of e-commerce***: where the re-use of personal data is seen to be a founding principle.

Risks and costs of data-sharing

Data-sharing also carries some risk, such as:

- ***identification***: getting the wrong person when inaccurate data is shared - this risk is exacerbated by the lack of a single identifier since data is therefore shared on the basis of a name, address or date of birth;

⁴ HC Deb Vol 366, 3.4.01, c290W

- **financial costs:** the need to invest in technology that maximises the benefits of data-sharing through a system that provides accountability and security.
- **public concern:** incidents in the private sector and other factors could give rise to increased concerns of privacy and security.

Benefits of increased privacy

Privacy is a fundamental right. It is hard to quantify, which may have the effect that it is accorded less weight than other factors such as financial savings, but it is no less real. Furthermore, it is not simply relevant at the level of the individual, who may trade reduced privacy for improved customer service or cost savings, but it is also a common good for society as a whole.

It is generally assumed that, over time, privacy is inevitably eroded. But technological developments may in fact allow a reduction in the information needed for a given transaction (e.g. electronic pseudonyms and other privacy-enhancing technologies).⁵

The scoping note set out the need for important policy decisions on this issue:

Decisions need to be made in the near future about the sharing of data within government, and between government and the private sector, to maximise the benefits to consumers of e-government, to further reduce fraud (as highlighted in Lord Grabiner's report on the informal economy) and to improve the efficiency of government and effective use of its resources.

Two conditions need to be met for the benefits of data-sharing to be fully realised:

- people need to be informed and accepting of the use to which their data will be put and the purposes for which it will be shared;
- government needs to operate within the legal framework established by the Data Protection Act 1998 and the Human Rights Act 1998, and to be an exemplar in the creation of a secure and transparent process for the use of personal data.⁶

The note observed that although work on data-sharing was going on in government, this was "piecemeal": the PIU project should establish a government-wide framework for the future. The note continued:

A number of factors suggest that a study of the balance between data-sharing and privacy is timely:

⁵ Ibid

⁶ Ibid

- IT developments make it increasingly easy to collect, share and manipulate personal data; and the government will need to address the opportunities and threats posed by technological developments.
- the new opportunities and risks presented by those developments in technology and the public's legitimate desire to have their privacy concerns recognised and protected in the new electronic world, including the possibility of increased privacy which technology may provide.
- consumer expectation for services to be tailored to their individual needs and preferences is extending beyond the private sector to government services;
- there are new prospects of cracking down on fraud through increased data-sharing, and improving government efficiency overall;
- the lack of widespread understanding of the Data Protection Act and Human Rights Act, and the responsibilities they confer on the public and the private sectors.⁷

The PIU's report, which was due to be published in spring 2001, has yet to appear. The privacy advisory group, established to contribute to the data sharing project, identified a lack of clarity in the legal framework governing the disclosure of information by public bodies. The most obvious restriction is provided by data protection legislation:

Under the *Data Protection Act 1998*, electronic personal data cannot be shared between public bodies, including Government departments, unless they are collected for that purpose and the parties which will receive the data are specified in the entry on the Register of Data Users maintained by the Data Protection Registrar⁸. This means that, in general, unless there are statutory sharing arrangements in place, one body cannot inform another of suspicious activity.⁹

Further information on the data-protection aspects of data sharing is set out on the Information Commissioner's website.¹⁰

Other legal constraints might, in fact, prove more fundamental than data protection. Additional constraints on data sharing which may apply include:

- *vires* issues (whether, in terms of its statutory functions, the public body has the power to disclose the information for additional purposes); and

⁷ Ibid

⁸ Now known as the Information Commissioner

⁹ Ibid

¹⁰ www.dataprotection.gov.uk

- confidence issues (whether the public body owes a common law duty of confidence to the subject of the information).

An earlier PIU report had recommended that legislation was necessary to allow the Inland Revenue to disclose information to other law enforcement agencies for the purpose of determining whether to initiate, pursue or bring to an end criminal investigations or proceedings: this recommendation is set out in more detail in the next section.

B. Background to Part III of the Bill

Provisions similar to those now set out in clauses 17-20 (part 3) of the Bill were included in the *Criminal Justice and Police Bill 2000-01* when it was first introduced in January 2001.¹¹ The Government agreed to their removal at the Bill's Report stage in the Lords on 9 May, in the light of specific concerns about the disclosure of information by the Revenue and Customs, as well as the announcement that day that the general election would be held on 7 June.¹² When the appropriate amendments to the Bill were scrutinised in the Commons the next day, Charles Clarke – then Minister of State at the Home Office – said, “given the shortness of time available to complete the parliamentary stages of the Bill, we have decided to give further scrutiny to that part of the legislation. If the Government are re-elected, we will consider the best way to proceed with those useful reforms and how to use other legislative vehicles to do so.”¹³

The Chancellor Gordon Brown confirmed that powers to allow the tax authorities “where applicable to share information and co-operate more effectively with the police” would be introduced shortly, in his statement to the House on measures against financing terrorism on 15 October.¹⁴ He went on to say, “we believe that a range of crimes justify passing information from the Inland Revenue to the police. We will consult on the details of the legislation, but the police will have more sources of information from the Inland Revenue about crimes that are being committed.”¹⁵ The following paragraphs discuss the background to this proposal.

In June 2000 the Performance and Innovation Unit of the Cabinet Office published a report on recovering the proceeds of crime;¹⁶ one of its recommendations was that the Revenue authorities should be allowed to disclose information to the police authorities for

¹¹ specifically part II of the Bill comprising clauses 45-48 [Bill 31 of 2000-01]

¹² HL Deb 9 May 2001 cc 2172-3

¹³ HC Deb 10 May 2001 c 303

¹⁴ HC Deb 15 October 2001 c 940

¹⁵ HC Deb 15 October 2001 c 952

¹⁶ No.10 Downing Street press office, *New measures to ensure that crime doesn't pay*, 14 June 2000

criminal investigations and proceedings.¹⁷ The report's discussion of the use of information held by the Inland Revenue and other public authorities to combat crime is reproduced below:

The amount of financial information held by the Inland Revenue is extensive – records for 32 million individuals and 1.1 million companies or other organisations are currently held. Under the *Data Protection Act 1994* [sic] (*DPA*), electronic personal data cannot be shared between departments unless they are collected for that purpose and the parties which will receive the data are specified in the entry on the Register of Data Users maintained by the Data Protection Registrar. This means that, in general, unless there are statutory sharing arrangements in place, one body cannot inform another of suspicious activity. Tax Inspectors (and Department of Social Security (*DSS*) Investigators) can be liable to prosecution if they breach the confidentiality of tax or benefits records. This can mean that evidence of criminality has to be ignored because it cannot be shared with other investigating authorities.

The Inland Revenue, in particular, is heavily restricted in its ability to pass financial intelligence to other Government departments and law enforcement agencies. Historically, disclosures have been made to other law enforcement bodies only in the event of murder or treason.¹⁸ Information *can* be exchanged with Customs (under section 127 of the *Finance Act 1972*) or the *DSS* (under the *Social Security Administration Fraud Act 1997* and the *Finance Act 1997*).

Other bodies can obtain specific information on a particular case from the Revenue by means of a production order, but this requires the agency concerned to demonstrate reasonable grounds for believing that the Revenue has useful information in the first place. The Financial Services and Markets Bill plans to allow a discretionary gateway between the Revenue and the Financial Services Authority, recognising the vital role that taxation records can play in investigating all financial activities.¹⁹ The ability of law enforcement agencies to pass information to the Inland Revenue is much greater, with information channels already functioning from the National Criminal Intelligence Service (*NCIS*), the National Crime Squad (*NCS*), immigration and police.

The benefit of increased information flows between Inland Revenue, law enforcement agencies and Government departments is demonstrated by the success of a single secondment from Inland Revenue to *NCIS*. Since March 1999, 248 disclosures were passed from *NCIS*. This information arising from the financial disclosure system within the Economic Crime Unit and passed to the *SCO* has already identified potential tax evasion totalling hundreds of millions of pounds (source: *NCIS*). In addition to the general changes proposed to the

¹⁷ Many of the proposals made in the report were brought forward in the *Proceeds of Crime Bill 2001-02* which received its Second Reading on 30 October 2001. For more details see the Library Research Paper on the Bill (Paper 01/79, 29 October 2001).

¹⁸ [For details see *Royal Commission on Standards in Public Life* Cmnd 6524 July 1976 para 93]

¹⁹ [This provision was made under section 350 of the *Financial Services and Markets Act 2000*.]

confiscation order enforcement system, there is merit in informing the Inland Revenue of all confiscation orders, so that future tax assessments can take account of funds used to satisfy the debt.

Conclusion : Legislation should be introduced to allow the Inland Revenue to disclose information on a case by case basis for the purpose of determining whether to initiate, pursue or bring to an end criminal investigations or proceedings. Consideration should be given to whether this legislation should extend to all public bodies and also to assisting foreign criminal investigations or proceedings.

Consideration should be given to whether this legislation should extend to all public bodies and also to assisting foreign criminal investigations or proceedings.²⁰

In January 2001 the Government announced that it would implement this proposal, as part of the *Criminal Justice and Police Bill 2000-01*.²¹ As mentioned above, part II of the Bill (clauses 45-48) dealt with the disclosure of information by Government departments, and certain public bodies, including the tax authorities, for the purposes of criminal investigations and proceedings; the then Home Secretary Jack Straw summarised the purpose of these provisions on the Bill's Second Reading:

Part II deals with the disclosure of confidential information for the purposes of criminal investigations and procedures. It tidies up disclosure provisions in the 74 measures set out in schedule 1, which are diverse enough to include the *National Savings Bank Act 1971* and the *Diseases of Fish Act 1983*. Part II also provides a statutory power for the Inland Revenue and Customs and Excise to disclose information to other law enforcement agencies. That will allow a reciprocal flow of information between those bodies, the police and the National Criminal Intelligence Service.²²

In her contribution to the Second Reading debate the then Shadow Home Secretary, Ann Widdecombe, suggested that confidential information should be disclosed by the tax authorities "only when it is manifestly required in connection with a serious investigation."²³

At the Committee stage of the Bill, Oliver Heald moved amendments to clause 45 (extension of existing disclosure powers of public authorities) designed to ensure, amongst other things, that

²⁰ Cabinet Office, *Recovering the proceeds of crime*, June 2000 pp 94-95 The report is available on the Cabinet Office internet site at: www.cabinet-office.gov.uk/innovation/2000/crime/crime.shtml

²¹ Inland Revenue/HM Customs & Excise press notice PR JW1, 22 January 2001

²² HC Deb 29 January 2001 c 41

²³ HC Deb 29 January 2001 c 52 This issue was also flagged by Simon Hughes and Oliver Heald at later stages of the debate (*op.cit.* c 72, c 118).

- disclosure of information provided to the authorities under certain statutes was not permitted;
- disclosures could be made only when the subject matter of a foreign investigation amounted to a crime in this country; and
- disclosures could be made only when it would exclude information that was subject to a European Union agreement.

He introduced the amendments as follows:

The background to the amendments is the concern of business that the Government are changing policy in a way that may damage United Kingdom business. It is thought that the purpose of the clause is to allow important, confidential commercial information to be given to the United States anti-trust authorities in order to put UK businesses at peril of criminal action being taken against them for actions that are considered legal and proper in the UK and the EU.

It will also expose businesses that might, under United Kingdom law, have a civil liability for their actions to United States criminal laws. That is a huge departure from the previous consensus that we should protect British business, especially when its actions are entirely proper and legal under United Kingdom law, but also against a criminal liability when only a civil one exists in this country.

The change of policy has not been announced to Parliament; the provision is tacked on to a Bill that is about other matters, without proper consultation with the Confederation of British Industry, and at a damaging time in respect of EU efforts to tackle anti-competitive behaviour in Europe.²⁴

In response, Charles Clarke – then Minister of State at the Home Office – stated that the proposals in clause 45 resulted from a recommendation in the June 2000 PIU report, whose findings were open to consultation over the summer of that year. The CBI's concerns had been addressed in meetings with the Secretary of State for Trade and Industry and DTI officials, he said. Mr Clarke described the main amendment and the Government's reasons for rejecting it as follows:

Amendment No. 204 has three parts. First, it would prevent the disclosure in relation to the 13 provisions in the new schedule. Secondly, it would require that information be disclosed for an overseas investigation only if that investigation related to conduct that is a crime in the UK as well as in the country to which the information was to be disclosed. Thirdly, it would prevent the disclosure of information that related to an agreement, decision or practice that may affect trade between the member states of the EU. I would like to deal with each of those parts in turn.

²⁴ SC F 6 March 2001, c412

The first part of the amendment provides that nothing in clause 45 would permit disclosure in relation to the 13 provisions listed in the new schedule. Those provisions relate to competition law, utilities regulation, company law and financial regulation. Much of the information held pursuant to the statutes that contain those disclosure provisions will be confidential financial information, including information useful for competition inquiries. Nevertheless, it is also possible that information useful for any number of other criminal inquiries into offences such as fraud, tax evasion and money laundering may be held. We believe that the information holder should be free to disclose that information for criminal investigations or proceedings, whether in the UK or overseas.

Competition should not be seen as a special case. We believe that the Bill will permit UK authorities to assist countries that have criminal penalties in their anti-trust laws to prosecute criminal activities in breach of those laws that take place in their jurisdiction. Illegal cartels are bad for consumers, and it is in our interests to work against them. Globally, they affect billions of pounds worth of trade, and they must be dealt with.

The second part of the amendment would require that disclosure overseas be permitted only where it relates to conduct that amounts to a criminal offence in both countries. There will be safeguards on overseas disclosure in the provisions, but we do not believe in putting unnecessary obstacles in the way of effective co-operation in the fight against crime, wherever it occurs. The criminal law of many countries does not exactly mirror that of the United Kingdom, and never will do. For example, the Filipino originator of last year's so-called "Lovebug" computer virus was not apparently committing an offence in the country of the virus's origin.

We believe in furthering competition with other countries, irrespective of whether their domestic law contains criminal penalties. The cases for which information is likely to be sought by overseas authorities should relate to hardcore cartel activity, which the UK regards as a serious offence, even if UK competition law does not contain criminal penalties.

On the third part of the amendment No. 204, the Opposition proposal to limit disclosure in cases where it relates to an agreement, decision or concerted practice may affect trade between EU member states. The Government believe that it is important to improve co-operation with other countries in the enforcement of competition laws in respect of offences that take place within their jurisdiction. We do not want to hinder anyone's fight against anti-competitive practices. The safeguards in the clause will ensure that any information that infringes the jurisdiction of the UK or a third country will not be disclosed for the purposes of any criminal investigations or proceedings.

The suggested broad prohibition would prevent disclosure in anti-competitive and other types of agreement. For example, disclosure might be impossible in respect of fraud, theft or smuggling investigations. The proposed prohibition would be

capable of preventing disclosures both overseas and in the UK, which would mean a substantial limitation of the extent to which disclosure is possible under schedule 1.²⁵

The amendment was defeated on a division.²⁶

Simon Hughes moved amendments to the proposed extension of existing disclosure powers of public authorities (clause 45) and the proposed disclosure powers of the Revenue authorities (clause 47). The intended effects of these amendments were to ensure: first, that any decision to disclose information should lie with a circuit judge – not with the authorities holding the information; and second, that a disclosure would only be made if “the judge is satisfied that there is a reasonable suspicion that a criminal offence has been committed and, more importantly, that the disclosure is likely to be of substantial value to the investigation of an offence.” Mr Clarke resisted these amendments, saying:

Onward disclosure of revenue department information will require the authorised consent of that department. There are strict administrative controls on the disclosure of information by the revenue departments and under section 182 of the *Finance Act 1989*, which makes any unauthorised disclosure of information by the Inland Revenue or Customs and Excise staff a criminal offence, punishable by a fine and/or up to two years’ imprisonment. We believe that such matters are appropriate for the Executive and that there is a range of safeguards in the current legislation. We see no advantage either to the citizen or to the operation of our criminal justice policies in bringing in the judiciary as proposed in the amendments.²⁷

The amendments relating to clause 45 were defeated on a division. Mr Hughes withdrew the amendments relating to clause 47, which was agreed to without further debate.²⁸

Following the passage of the Bill from the Commons, Baroness Noakes raised a number of specific concerns about this provision during the Lords Second Reading debate, arguing that the Government had “drafted very wide powers, the exercise of which could easily be injurious to citizens.”²⁹ Lord Bassam of Brighton, Minister of State at the Home Office, responded for the Government, first in his winding up speech on the

²⁵ Ibid, cc 421-2

²⁶ Ibid, c426

²⁷ Ibid, c 428 These amendments were discussed during the debate on clause 45 of the Bill, relating to the extension of existing disclosure powers (*op.cit.* cc 411-429).

²⁸ SC F 6 March 2001 c 537

²⁹ HL Deb 2 April 2001 c 691 The noble Baroness noted her concerns were shared by the Tax Faculty of the Institute for Chartered Accountants, who had issued two short press notices on the matter, on 11 December 2000 and 23 January 2001.

Second Reading, and second in subsequent correspondence.³⁰ The following paragraphs look at each of these concerns in turn.

The first point Baroness Noakes made was that the ability of the tax authorities to pass on information would discourage taxpayer compliance:

Taxpayers have always believed that information given to the tax authorities is given in strictest confidence. This helps to promote a culture of tax compliance. For example, taxpayers whose affairs have got in a mess are positively encouraged to make a clean breast of outstanding issues. Under a procedure known as the “Hansard” procedure, a taxpayer can do a deal with the Inland Revenue. If the taxpayer honestly owns up to past errors and makes a financial settlement—usually a very large financial settlement—the Inland Revenue will agree not to prosecute. This is clearly advantageous to the taxpayer. But it also promotes a culture of compliance, which is one of the linchpins of our tax system, as well as improving revenue collection.

How will this procedure work in future? What a taxpayer sometimes owns up to is a source of income or capital which has its origins in an illegal act. Will the Hansard procedure protect the taxpayer in future from information disclosure as well? If that is not the case, or if the taxpayer does not believe that that is the case, we could well see a diminution in the incidence of voluntary disclosure and settlement of past tax liabilities. That would be bad for individual taxpayers, for the culture of compliance in this country and for tax collection generally.³¹

In response Lord Bassam noted that “Revenue departments already disclose information in a carefully regulated way through an increasing number of existing information gateways to other public authorities and bodies.”³² He provided a longer response in his written briefing:

Under the current “Hansard” procedure with Inland Revenue and similar agreements with Customs, a taxpayer agrees to make a full and frank disclosure about his or her tax affairs as well as settlement of any liability agreed. In return, the Revenue agrees not to prosecute for matters for which it has statutory responsibility and Customs will agree on reduced penalties. The new disclosure provisions will not change this position. The Revenue Departments already disclose information in a number of existing information gateways to other public bodies. There is no evidence that this has affected the willingness of people to be frank with the tax authorities. Even if there were such an effect the public interest in maintaining the confidentiality of tax information has to be balanced against the public interest in combating crime and particularly serious crime. For example, we do not believe that Customs or the Revenue should be prevented

³⁰ Home Office, *Letter from Lord Bassam of Brighton in relation to the Criminal Justice and Police Bill*, 10 April 2001. The full text is held in the Commons Library as a deposited paper (Dep 01/662).

³¹ HL Deb 2 April 2001 cc 690-1

³² HL Deb 2 April 2001 c 713

from passing information to the police about a drug-trafficker or money-lauderer.³³

Baroness Noakes went on to ask whether the administrative controls over disclosure would be sufficient, without the involvement of an independent body to vet decisions:

An area of difficulty under Clause 49³⁴ is that disclosure under the clause requires the authority of the commissioners concerned; namely, the Inland Revenue or Customs and Excise. One problem with this is that in practice disclosure may well be authorised by a much more junior official to whom the commissioners have delegated their powers. I should be interested to hear whether there are any administrative processes planned to provide some protection to taxpayers against the over-enthusiastic use of these new information disclosure powers below the level of the commissioners themselves. I note in particular that, unlike Clause 47, the clause provides no penalty for wrongful disclosure. How will taxpayers be protected against the misuse of these powers?

I believe that the Government should also consider altering the authorisation procedures from within the tax authorities to an external authority. A precedent exists for occasions when the Inland Revenue wishes to obtain information about a taxpayer from external sources. It needs to obtain the permission of either a general or a special commissioner under Section 20 of the *Taxes Management Act*; that is to say, someone outside the Inland Revenue has to authorise the obtaining of information. It seems to me that there should be a similar requirement for the Inland Revenue to seek authority from someone outside the Inland Revenue--perhaps from a general or special commissioner--before information about a taxpayer is revealed.³⁵

In his letter Lord Bassam set out the Government's reasons for resisting this proposal:

The Finance Act provides the 'teeth' necessary to enforce strict administrative controls on disclosure.³⁶ The Revenue Department have considerable experience over many years in managing the processing of very large amounts of sensitive personal information. They have very strict rules on the confidentiality of information about individuals. All staff are required to sign a declaration of secrecy prohibiting them from disclosing information received in the execution of their duties except for the purposes of those duties or in accordance with the Boards' instructions. Information will only be disclosed in clearly defined and carefully controlled circumstances, and all information is held in strict confidence.

³³ Home Office, 10 April 2001 p 7

³⁴ [Following passage of the Bill to the Lords, Part II of the Bill [HL 36] comprised clauses 47-50; clause 49 dealt specifically with the disclosure of information held by tax authorities.]

³⁵ HL Deb 2 April 2001 c 691

³⁶ [As noted above, under section 182 of the *Finance Act 1989* any unauthorised disclosure of information by Customs or Revenue Staff a criminal offence, punishable by up to two years imprisonment and/or a fine.]

We expect that the Revenue Departments will seek Memoranda of Understanding with the police to set out the procedures to regulate and control the disclosure of information. These arrangements will include tests of relevance and security and will provide for requests and disclosures to be channelled through authorised and properly trained staff. Staff will be provided with clear and detailed guidance to ensure that all disclosures they make are in accordance with the law ...

No requirement to seek the authority of the General or Special Commissioners (or a judge) before information can be disclosed will be imposed as we believe this would insert an unnecessary and bureaucratic hurdle to the disclosure of information. If, for example, the Revenue was involved in a large, complex and on-going enquiry which was also of interest to the police, the requirement for Commissioners approval could mean that they needed a continuous, time-consuming and unnecessary series of approvals from the Commissioners for the disclosure of new but related information. This would slow down the disclosure of information substantially, and so undermine the legitimate objective of the Clause.³⁷

The Government also resisted the suggestion by Baroness Noakes that taxpayers should be given the “right of redress” in disclosure decisions:

Both Revenue Departments have well-established and publicised complaints and compensation procedures, in which complaints can be referred to the Adjudicator’s Office for investigation. It would not be appropriate, however, to provide taxpayers an opportunity to make representations prior to disclosure for a criminal investigation — we would obviously not want to tip-off suspects to the existence of a criminal investigation. In particular in cases where an investigation had not been commenced, we would not want to delay an investigation at a critical stage or give an opportunity for the taxpayer to destroy relevant evidence.³⁸

Baroness Noakes also picked up on the concern raised by the Shadow Home Secretary, Ann Widdecombe, on the Bill’s Second Reading in the Commons, that disclosure should only occur where it was ‘manifestly required in connection with a serious investigation’:

The new information disclosure power is not confined to crimes that have definitely been committed. It does not even require criminal investigations or criminal proceedings to be under way. Clause 49(2) refers to criminal investigations which “may be carried out” and to criminal proceedings which “may be initiated”. This is a very wide power. I believe that some protection for taxpayers is necessary. One way of providing protection is to ensure that

³⁷ Home Office, 10 April 2001 p 7, p 6

³⁸ Home Office, 10 April 2001 p 7

disclosure cannot be made unless there is reasonable evidence that a crime has been committed.³⁹

Lord Bassam's written response setting out the Government's opposition to this proposal identified important limits on the disclosure of information power:

The police will not be able to require the disclosure of any information under the provisions as disclosure is permissive rather than mandatory. The Revenue Departments will also not be permitted to provide information unless they are satisfied that it is needed for crime related purposes. Recipients of information will not be permitted further to disclose the information for any purposes other than those stated in clause 49(2) and then only with the permission of the relevant Commissioners.

Our view is that it would not be appropriate to limit disclosures to cases where it is "manifestly required in connection with a serious investigation". It would be difficult for the holder of information about wrongdoing to know either whether the information is manifestly required or the precise seriousness of the offence. This is especially the case where the information itself might be the trigger for bringing an investigation in the first place. It is also very difficult to come up with a definition of a serious offence that is usable at the intelligence-gathering stage of a criminal investigation. The precise seriousness of the suspected offence will not become apparent until the intelligence is gathered. We believe to impose such requirements would prevent or slow down disclosures and impose a difficult to navigate test on information holders who are subject to criminal penalties if it were accidentally misapplied.⁴⁰

Finally Baroness Noakes was concerned about the power to release information to other jurisdictions, and asked if the Government would ensure only signatories to the European Convention on Human Rights – or its equivalent – received material under this provision:

Clause 49 is not limited to disclosure in the UK. It specifically covers criminal proceedings or investigations outside the UK. The provision is not restricted to criminal offences or suspected offences that would be treated as criminal if they were committed in the UK. For example, some acts which in this country are regarded as civil offences are regarded as criminal in other jurisdictions. Are we really creating a power to allow information to be passed outside the UK authorities for acts that we should not regard as criminal? ...

I am told that a relatively common source of taxpayer disclosure under the Hansard procedures that I referred to earlier is from individuals who have brought money or other assets into this country from their former countries in breach of local laws. Many still have relatives in those countries and would fear for their own or their relatives' safety if disclosure were made. Ethnic minorities

³⁹ HL Deb 2 April 2001 cc 691-2

⁴⁰ Home Office, 10 April 2001 pp 5-6

persecuted overseas may well be particularly affected by the application of these powers ... Would the Minister, who has signed the usual declaration on the European Convention on Human Rights for the Bill, confirm that disclosure of information could not be made under the Bill to a foreign jurisdiction where that jurisdiction does not itself comply with an equivalent of the convention? If he is unable to confirm this, will the Government consider amending the Bill to achieve that protection?⁴¹

In his Second Reading speech Lord Bassam responded to this point as follows:

[The noble Baroness] ... said that disclosure overseas should be permitted under Clause 49 only if it is in relation to conduct which is a criminal offence in the UK. If that were to be the case, it would prevent government bodies from making a disclosure overseas in cases where the United Kingdom had decided not to criminalise the behaviour. That would prevent disclosure in cases where we have made a policy choice to provide civil penalties because of the desirability of avoiding the higher burden of proof rather than because the activities were considered to be less serious ...

[She also ...] asked whether disclosure under Clause 49 will be prohibited to a country that does not comply with the standards as set out in the ECHR. The Inland Revenue and Customs are public authorities within the meaning of the *Human Rights Act*. That means that they will have to exercise their disclosure powers in a way that is compatible with the ECHR. That means that a balancing act has to be carried out and that the disclosure should be made only where the circumstances make the disclosure necessary and--my favourite word--proportionate.⁴²

Lord Bassam discussed the tax authorities' responsibilities under the *Human Rights Act 1998* at more length in his written response:

The Revenue Departments are public authorities within the meaning of section 6 of the *Human Rights Act 1998* ("HRA"). This means that they will be legally required to exercise the new disclosure provisions in a way that is compatible with the European Convention on Human Rights ("ECHR"). They will have to undertake a balancing exercise to ensure that disclosures are only made in circumstances that make the disclosure necessary and proportionate. They will need to check each individual piece of information to ensure that its disclosure satisfies these requirements. The balancing exercise for overseas disclosure will be done on a case-by-case basis, and will include an examination of the gravity of the alleged offence and the potential penalty. This case-by-case test is more appropriate than a threshold test of whether the foreign state is a signatory to the ECHR. The balancing exercise places an important limitation on the exercise of

⁴¹ HL Deb 2 April 2001 cc 690-692

⁴² HL Deb 2 April 2001 c 713

the powers provided by the disclosure clauses and is unlikely to favour disclosure to countries with poor human rights standards.

The ECHR requirements are reinforced by the provisions of the *Data Protection Act 1998* (“DPA”). This Act provides a detailed framework for the disclosure of personal data. If a disclosure cannot be made in accordance with the data protection principles, the disclosure can only be made if an exemption applies. Section 29 of the DPA provides an exemption to the ‘non-disclosure provisions’ where the disclosure is for the prevention or detection of crime or the apprehension or prosecution of offenders, and the application of the provisions would be “likely to prejudice” any of those purposes. This means that the DPA operates as a filter on the type of information which can be disclosed and provides for a pre-disclosure assessment of the proportionality of disclosing the information. In addition, the DPA provides that personal data is not to be transferred outside the European Economic Area unless the country in question ensures an adequate level of protection for the rights and freedoms of people in relation to the processing of personal data about them. Taken together, the HRA and the DPA should ensure that information disclosure overseas is not permitted in inappropriate cases.⁴³

Concerns about Part II of the Bill were reiterated at the Bill’s Committee stage on 8 May, which coincided with the announcement that the Dissolution of Parliament would take place on 14 May, prior to the general election on 7 June. Lord Cope of Berkeley, Opposition Spokesman on Home Office matters, commented, “it is extremely important that these potential powers--given not only to the police but also to other authorities--are properly controlled and looked at ... Unless we have a proper opportunity to debate the Bill ... we would not want to see Part II of the Bill proceed.”⁴⁴ Speaking for the Liberal Democrats, Lord McNally agreed with the sentiment; consequently Lord Williams of Mostyn, then Attorney General, announced that a suitable amendment would be put down for this purpose.⁴⁵ Introducing this amendment at the Bill’s Report stage the following day, Lord Bassam said:

Given the short amount of time available to complete the parliamentary stages of the Bill, we have jointly tabled the amendment seeking to remove Part II of the Bill. This will provide a period of time in which, no doubt, we can improve the quality of the legislation, if that is what is required, and perhaps undertake further consultations. If the Labour Government are re-elected, we shall consider carefully the best way to proceed with what we believe are very useful reforms.⁴⁶

⁴³ Home Office, 10 April 2001 p 6

⁴⁴ HL Deb 8 May 2001 c 2039

⁴⁵ HL Deb 8 May 2001 c 2055

⁴⁶ HL Deb 9 May 2001 c 2173

C. Part III of the Bill

Clause 17 clarifies and extends a number of information disclosure provisions available to individuals working in public authorities. The relevant statutes, 66 in all, are listed in schedule 4; further powers contained in subordinate legislation may be added by the Treasury, by statutory instrument. The clause permits disclosure to assist any criminal investigation or criminal proceedings being carried out in the UK or abroad or to facilitate whether or not such investigations or proceedings should begin or end. The clause does not limit any power to disclose that exists apart from this clause. Subsection (6) provides that:

The information that may be disclosed by virtue of this section includes information obtained before the commencement of this section.

Clause 18 enables the Secretary of State to prohibit the disclosure of information for the purposes of overseas criminal investigations or criminal proceedings which are being carried out under any of the provisions listed in Schedule 4. This power may be exercised where it appears to him that the overseas investigation or proceeding relates to a matter in respect of which it would be more appropriate for any jurisdiction or investigation to be exercised or carried out by the authorities of the United Kingdom or a third country.

Any person who knowingly makes a disclosure prohibited by a direction under clause 18 will be guilty of an offence. The person will be liable on conviction on indictment to imprisonment for a term of up to two years or a fine or to both, and on summary conviction to imprisonment for a term of up to three months or a fine of up to the statutory maximum (which is currently set at £5000).

Clause 19 applies to information held by or for the Commissioners of the Inland Revenue and Customs and Excise Departments. The clause provides that no obligation of secrecy, excepting the *Data Protection Act 1998* requirements, prevents the voluntary disclosure of information on the authority of the relevant Commissioners made for the following purposes: to assist any criminal investigation or criminal proceedings being carried out in the UK or abroad or to facilitate whether or not such investigations or proceedings should begin or end. In addition, the clause allows for disclosure to the intelligence services (the Security Service, the Secret Intelligence Service and GCHQ) in support of their functions. These functions include the protection of national security and the prevention and detection of serious crime.

Disclosed information cannot be further disclosed by the recipient except for the purposes permitted for original disclosures and with the consent of the relevant Commissioners. Bodies who receive information from Customs and the Inland Revenue may not further disclose that information to the intelligence services except for criminal investigations or proceedings. The clause does not limit any power to disclose that exists apart from this clause.

Under section 29 of the *Data Protection Act 1998*, personal information may be disclosed to third parties in ways which might otherwise contravene various data protection principles⁴⁷ provided the disclosure is for any of the following purposes-

- (a) the prevention or detection of crime,
- (b) the apprehension or prosecution of offenders, or
- (c) the assessment or collection of any tax or duty or of any imposition of a similar nature.

A disclosure under section 29 is only permissible where the application of the data protection principles to the disclosure would be likely to prejudice any of the purposes listed above.

As mentioned above, part III of the *Anti-Terrorism, Crime and Security Bill 2001-02* materially replicates part II of the *Criminal Justice and Police Bill 2000-01* as was, prior to those clauses being dropped from the Bill at its Report stage in the Lords. However, the wording of part III of the *Anti-Terrorism, Crime and Security Bill* differs in some respects from its predecessor (specifically, from Part II of Bill 31 of 2000-01).

Clause 45 of the earlier Bill provides that

Nothing in this section authorises the making of any disclosure which is prohibited by any provision of the Data Protection Act 1998.

Clause 17 of the current Bill does not contain a similar provision.

Clause 19 of the *Anti-Terrorism, Crime and Security Bill* differs in two respects from the wording used in Clause 47 of the *Criminal Justice and Police Bill*. As before, the tax authorities are empowered to disclose information:

- for the purposes of any criminal investigation whatever which is being or may be carried out, whether in the United Kingdom or elsewhere;
- for the purposes of any criminal proceedings whatever which have been or may be initiated, whether in the United Kingdom or elsewhere;
- for the purposes of the initiation or bringing to an end of any such investigation or proceedings; or
- for the purpose of facilitating a determination of whether any such investigation or proceedings should be initiated or brought to an end.⁴⁸

⁴⁷ part of the first principle, and principles 2,3,4 and 5, contained in Schedule 1 to the Act

⁴⁸ Clause 19(2)(b)-(e) to Bill 49 of 2001-02 which replicates the wording previously used in clause 47(2) to Bill 31 of 2000-01

However, under this provision in the current Bill disclosure may now be made for a ‘new’ fifth purpose: that is, “for the purpose of facilitating the carrying out by any of the intelligence services of any of that service’s functions.”⁴⁹

Second, as before, the *further* disclosure of information that has been provided under this provision may only be made “for a purpose mentioned in [clause 19(2)]; and with the consent of the Commissioners by whom or with whose authority it was initially disclosed.”⁵⁰ However, under the Bill the intelligence services, or “any person acting on behalf of any of those services”, may only obtain information in this manner, provided it is for one of the ‘original’ four purposes set out above.⁵¹

It is worth noting a minor amendment to clause 20 of the Bill - concerning the interpretation of Part III – from the equivalent provision as it appeared in the *Criminal Justice and Police Bill*,⁵² as this has a bearing on the concerns raised during the passage of the Bill concerning disclosure to aid criminal proceedings undertaken outside the UK. As noted, under clauses 17(2)(b) and 19(2)(c), disclosures may be made for “the purposes of any criminal proceedings whatever which have been or may be initiated, whether in the United Kingdom or elsewhere.” This is now qualified by Clause 20(2), which states:

proceedings outside the United Kingdom shall not be taken to be criminal proceedings for the purposes of this Part unless the conduct with which the defendant in those proceedings is charged is criminal conduct or conduct which, to a substantial extent, consists of criminal conduct.

The definition of criminal conduct in this context, however, is unchanged: that is “any conduct which

- (a) constitutes one or more criminal offences under the law of a part of the United Kingdom; or
- (b) is, or corresponds to, conduct which, if it all took place in a particular part of the United Kingdom, would constitute one or more offences under the law of that part of the United Kingdom.”⁵³

D. Reactions to the Disclosure of Information Provisions

As already noted, provisions similar to those in part III of the Bill were included in the *Criminal Justice and Police Bill 2000-01*. On 9th May 2001, the Government agreed to

⁴⁹ Clause 19(2)(a) to Bill 49 of 2001-02. In this context, “‘intelligence service’” has the same meaning as in the *Regulation of Investigatory Powers Act 2000* (c. 23)” (Clause 19(8) to Bill 49 of 2001-02).

⁵⁰ Clause 19(4) to Bill 49 of 2001-02 which follows clause 47(4) to Bill 31 of 2000-01

⁵¹ ie, for a purpose mentioned in clause 19(2)(b)-(e)

⁵² Clause 48 to Bill 31 of 2000-01

⁵³ Clause 20(3) to Bill 49 of 2001-02, which replicates the definition of crime provided in clause 48 to Bill 31 of 2000-01

their removal at the Bill's Report stage in the Lords in order to secure the passage of the Bill as a whole, given the proximity to the general election. The debates on part II of the former Bill were discussed in section B above.

The Home Affairs Committee published its report on the Bill on 19th November 2001.⁵⁴ It welcomed the measures designed to improved data sharing between government agencies, and noted that such measures had been recommended in its first report of 2000-01, on border controls. The earlier report stated:

12. We recommend that the continuing barriers to effective data collection and sharing between the border agencies should be urgently reviewed jointly by Home Office and Treasury (for Customs) Ministers. The Border Control Working Group should agree a joint information requirement to avoid duplication of demands for commercial information from carrying companies (paragraph 107).⁵⁵

However, responses to the Bill by the Law Society and the civil liberties pressure group Liberty objected to the re-introduction of these measures. The Law Society said of part 3:

This Part is a carbon copy of Part 2 of last year's Criminal Justice & Police Bill, which was previously dropped in the face of fierce criticism.

While it is understandable that the Government would wish to find an opportunity to reintroduce these provisions, an emergency bill on terrorism is not the place to do so. This Bill should not be used as a convenient way to 'mop-up' other Home Office issues, particularly those of a controversial nature.

If powers on these lines are to be included in this Bill, they should be restricted to cases where terrorism is an issue.⁵⁶

Liberty made stronger comments:

This Part of the Bill appears to be unconnected with terrorism or the events of 11th September. It must be assumed these new powers have been requested by the authorities and this is seen as [a] suitable vehicle for delivering them. This part should be removed from the Bill or restricted to terrorist related activities.

These measures allow personal and private information to be obtained by the police and others without any controls checks or safeguards. It will allow the police to trawl through the files held by other government departments.

⁵⁴ HC 351 of 2001-02

⁵⁵ *Border Controls*, HC 163-I of 2000-01

⁵⁶ Law Society: Parliamentary Brief, Anti-Terrorism, Crime & Security Bill. Second Reading – House of Commons 19 November 2001

The police will not need reasonable suspicion that the file contains evidence of a crime merely that it is useful in an investigation. The police will not need to go to a magistrate [or] court for authorisation and they will be able to access files without subsequent checks or audits. The subject of these investigations is unlikely ever to be told the police have rifled through their files and there will be no real remedy if the police are mistaken, over-zealous or plain malicious.⁵⁷

II Part XI: 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.⁵⁸

A. Access to communications data

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;
- (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.

⁵⁷ Anti-Terrorism, Crime And Security Bill 2001 Briefing For The Second Reading In The House Of Commons. Liberty, November 2001. www.liberty-human-rights.org.uk/mpar18.html

⁵⁸ HC Deb 15 October 2001 c 924

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 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. 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; reportedly⁵⁹ 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.

While the present Bill deals with the retention of communications data, access to it and the use to which it may be put are governed by the *Regulation of Investigatory Powers Act 2000* (RIPA). As its Explanatory Notes⁶⁰ 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-wide⁶¹ 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."⁶² This Part is due to come into force shortly.⁶³ It provides for access to communications data by the following public authorities:

- (a) a police force;

⁵⁹ BBC Radio 4, *Today*, 13 November 2001

BBC News Online, *Europe tackles internet privacy*, 13 November 2001

⁶⁰ Explanatory Notes, RIPA, <http://www.hms0.gov.uk/acts/en/2000en23.htm>

⁶¹ an exception is Part II of RIPA, not relevant here, which was legislated for separately in Scotland: *Regulation of Investigatory Powers (Scotland) Act 2000*

⁶² Explanatory Notes, RIPA, op. cit.

⁶³ Implementation timetable, RIPA, <http://www.homeoffice.gov.uk/ripa/imptable.htm>

- (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.⁶⁴

Section 22 of RIPA imposes a test of "necessity" on the acquisition of data; the designated person within the relevant 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.

The rank held by a designated person will be prescribed by an order made by the Secretary of State.⁶⁵ Communications data will be accessible either directly on the "authorisation"⁶⁶ of a Superintendent (or equivalent) or by him/her giving a "notice"⁶⁷ to

⁶⁴ RIPA, section 25

⁶⁵ RIPA, section 25(2)

⁶⁶ RIPA, section 22(3)

the postal or telecommunications operator. Inspectors will have powers to authorise access to a subset of communications data, for example account and subscriber information. 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 November 2001.⁶⁸ 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...⁶⁹

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.⁷⁰

Under section 57(2)(b) of RIPA, the Interception of Communications Commissioner (Sir Swinton Thomas)⁷¹ 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."

Furthermore, in the words of the Intelligence and Security Committee:

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 2000.⁷²

⁶⁷ RIPA, section 22(4)

⁶⁸ Home Office, *Accessing Communications Data Draft Code of Practice*, August 2001
<http://www.homeoffice.gov.uk/ripa/pcdpc.htm>

⁶⁹ 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

⁷⁰ RIPA, section 25(3)(b)

⁷¹ *Report of the Interception of Communications Commissioner for 2000*, Cm 5296, October 2001

⁷² *Intelligence and Security Committee Interim Report 2000-01*, Cm 5126, March 2001
<http://www.official-documents.co.uk/document/cm51/5126/5126.htm>

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.⁷³ 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.⁷⁴ 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.

Other concerns were identified in an *Economist* article:

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.⁷⁵

B. Retention of communications data

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-

(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.

⁷³ "Britain: Being watched: Electronic surveillance: Government eavesdropping", *Economist*, 26 August 2000

⁷⁴ *ibid.*

⁷⁵ *ibid.*

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".⁷⁶ 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 she (Elizabeth France) was referred to as the Data Protection Commissioner. Further information on her responsibilities appears on the Information Commissioner website.⁷⁷

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

⁷⁶ *Data Protection Act 1998*, schedule 2, paragraph 5

⁷⁷ <http://www.dataprotection.gov.uk/>

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 statement⁷⁸ on 15 October, a consultation exercise 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.⁷⁹

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

⁷⁸ HC Deb 15 October 2001 c 924

⁷⁹ 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

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.⁸⁰

While some internet service providers already keep data for a year, others delete it after as little as 48 hours.⁸¹ The Government has also commissioned a report on data retention; its findings were due to be shared with industry contacts in November 2001.⁸²

C. Anti-terrorism, Crime and Security Bill 2001/02

1. General

The *Bill Summary* accompanying publication of the Bill asserted that communications data had been "central to the investigation into the terrorist attacks on 11 September."⁸³ A regulatory impact assessment indicates how, alluding to the widespread use (if not necessarily under registered ownership) of mobile phones:

In particular communications data is an important investigative tool: allowing 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).⁸⁴

Relating the present Bill's data retention theme with RIPA, the summary goes on:

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.

⁸⁰ HC Deb 31 October 2001 cc 725-6W

⁸¹ BBC News Online, *Anti-terror laws raise net privacy fears*, 11 November 2001

⁸² HC Deb 1 November 2001 c 849W

⁸³ <http://www.homeoffice.gov.uk/oicd/antiterrorism/index.htm>

⁸⁴ *ibid.*

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 indicates a number of concerns likely to feature in subsequent debates.⁸⁵ 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 makes provision for contributing to additional costs, though internet service providers will increasingly have open to them the option of relocating overseas, avoiding the extra work as well as foreclosing access by UK law enforcement agencies.

On the privacy point, the article quotes Caspar Bowden, director of the Foundation for Information Policy Research as fearing widespread use (under RIPA) of large communications databases retained under the present Bill. He elaborates in a press release, published before the Bill but which, he has since asserted,⁸⁶ retains 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 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.⁸⁷

In her comments on the Bill, the Information Commissioner has stated that the proposed provisions "could have a significant impact on the privacy of individuals whose data are retained."⁸⁸ She goes 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

⁸⁵ BBC News Online, *Anti-terror laws raise net privacy fears*, 11 November 2001

⁸⁶ Caspar Bowden, Foundation of Information Policy Research, 14 November 2000, personal communication

⁸⁷ FIPR press release, *Emergency powers allow mass-surveillance for non-terrorist investigations*, 16 October 2001

⁸⁸ Information Commissioner news release, *Information Commissioner contributes to scrutiny of anti-terrorism bill*, 13 November 2001 <http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf>

lack of proportionality such as to render the prospective legislation incompatible with Convention rights.⁸⁹

2. Part XI of the Bill

Clause 101 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. This latter process is already in train. Subsection 2 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.⁹⁰ Since the proposed code is voluntary there would be no penalties for non-compliance (subsection 6). Clause 101(7) provides communications providers with a defence against actions brought by data subjects; the explanatory notes:

*Subsection (7) 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.*⁹¹

The Information Commissioner is "particularly concerned that leaving matters to a voluntary code of practice, or to agreements, may pose difficulties for data protection and human rights compliance."⁹² She comments on the "absence of clarity as to what information is necessary for law enforcement purposes". 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 co-ordinates), and what everyone reads online (websites browsed). Current mobile phones track location to a few hundred meters whilst the phone is switched on

⁸⁹ *ibid.* (attached memorandum)

⁹⁰ regulation 32

⁹¹ Bill 49 - EN

⁹² Information Commissioner news release, *Information Commissioner contributes to scrutiny of anti-terrorism bill*, 13 November 2001 <http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf>

(not merely when a call is made), and 3rd generation phones will pinpoint location to a few meters.⁹³

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 the Information Commissioner in her memorandum.⁹⁴ The National Criminal Intelligence Service reportedly takes the view that these events have strengthened the case for internet traffic data retention; it has, however, recently distanced itself from a leaked⁹⁵ document, *Looking to the Future*, prepared last year by the NCIS deputy director-general.⁹⁶

Clause 102 allows the Secretary of State to make an order giving directions to service providers about the retention of communications data if, as the *Guardian* puts it, "they don't volunteer enough."⁹⁷ 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 would seem likely.⁹⁸ 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).

The scope of consultation in both clauses 101 and 102 is 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

⁹³ 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

⁹⁴ Information Commissioner news release, *Information Commissioner contributes to scrutiny of anti-terrorism bill*, 13 November 2001 <http://www.dataprotection.gov.uk/dpr/dpdoc1.nsf>

⁹⁵ <http://cryptome.org/ncis-carnivore.htm>

⁹⁶ "The net's eyes are watching", *Guardian Online*, 15 November 2001

⁹⁷ *ibid.*

⁹⁸ HC Deb 31 October 2001 cc 725-6W

Commissioner would expect to be consulted formally about directions applying to communications providers.⁹⁹

Clause 102(7) provides for enforcement (civil proceedings) by the Secretary of State.

Clause 103 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,¹⁰⁰ 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.

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** 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.¹⁰¹

⁹⁹ 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>

¹⁰⁰ clause 103(3)

¹⁰¹ <http://www.homeoffice.gov.uk/oicd/antiterrorism/index.htm>

Appendix: Amendments of the Intelligence Services Act 1994

The *Intelligence Services Act 1994* places on a statutory basis the activities of both the Secret Intelligence Service¹⁰² and Government Communications Headquarters (GCHQ). It also established the Intelligence and Security Committee, comprising senior parliamentarians appointed by the Prime Minister. Countering domestic threats to security, be they from terrorism or other serious crime, is the provenance of the Security Service;¹⁰³ this is governed by the provisions of the Security Service Acts 1989 and 1996. All three intelligence and security agencies¹⁰⁴ are also subject to the *Regulation of Investigatory Powers Act 2000*, which provides for oversight by the Intelligence Services Commissioner (Lord Justice Simon Brown).¹⁰⁵

Clause 114 of the present Bill recognises the blurring demarcation between overseas and internal threats to national security. It does so by extending the powers of GCHQ, and SIS, to act in the UK in relation to apparatus believed to be outside the British Islands. The term apparatus means any equipment, machinery or device, or any wire or cable. This measure would extend the authorisation mechanisms in section 7 of the *Intelligence Services Act 1994* to include interception of communications between terrorists in the UK and their accomplices overseas.

¹⁰² also known as MI6

¹⁰³ MI5

¹⁰⁴ For further background see Library Standard Note, *Intelligence and Security Agencies*, 16 November 2001

¹⁰⁵ *Report of the Intelligence Services Commissioner for 2000*, Cm 5297, October 2001