RESEARCH PAPER 02/54
4 OCTOBER 2002

The *Anti-terrorism, Crime and Security Act 2000:* Disclosure of Information

Part 3 of the *Anti-Terrorism, Crime and Security Act 2001* is intended to ensure that government departments and agencies can collect and share information required for countering the terrorist threat. The Act was passed very quickly by Parliament in response to the terrorist attacks in the USA on September 11, 2001. Part 3 has proved controversial inside and outside Parliament due to the wide scope of its disclosure powers, which are not limited to anti-terrorist investigations, and the perceived danger of individuals' privacy rights being breached if hitherto confidential information is disclosed to the law enforcement and intelligence agencies. This paper discusses part 3, and the debate about these provisions, in depth.

The paper also discusses similar provisions introduced in (and subsequently removed from) the *Criminal Justice and Police Bill 2000-01*. The paper commences by highlighting relevant issues contained in the Performance and Innovation Unit report, *Privacy and Data Sharing*.

Edward Wood

HOME AFFAIRS SECTION

HOUSE OF COMMONS LIBRARY

Recent Library Research Papers include:

List of 15 most recent RPs

02/39	Unemployment by Constituency, May 2002	14.06.02
02/40	Cross border shopping and smuggling	21.06.02
02/41	Modernisation of the House of Commons: Sitting hours	27.06.02
02/42	Economic Indicators [includes article: Housing market overheating]	01.07.02
02/43	The Burden of Taxation	09.07.02
02/44	Inflation: the value of the pound 1750-2001	11.07.02
02/45	The Euro-Zone: The early years & UK convergence	16.07.02
02/46	Unemployment by Constituency, June 2002	17.07.02
02/47	The *Mobile Telephones (Re-programming) Bill* [HL Bill 177 of 2001-02]	18.07.02
02/48	Defence Statistics – July 2002	19.07.02
02/49	Unemployment by Constituency, July 2002	15.08.02
02/50	Regional Development Agencies (RDAs)	22.08.02
02/51	Unemployment by Constituency, August 2002	11.09.02
02/52	Detention of suspected international terrorists – Part 4 of the *Anti-Terrorism, Crime and Security Act 2001*	16.09.02
02/53	Iraq: the debate on policy options	20.09.02

Research Papers are available as PDF files:

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

ISSN 1368-8456

Summary of main points

Part 3[1] of the *Anti-Terrorism, Crime and Security Act 2001* (ATCSA) is intended to:

> ensure that government departments and agencies can collect and share information required for countering the terrorist threat.[2]

ATCSA was passed very quickly by Parliament in response to the terrorist attacks in the USA on September 11, 2001. The main powers contained in part 3 are described as follows in the Explanatory Notes to the Act:

> Section 17 clarifies and extends a number of existing provisions for disclosure of information from public authorities to agencies involved in criminal investigations and proceedings. The gateways ensure that public authorities can disclose information which is subject to a statutory restriction on disclosure for the purposes of a criminal investigation or criminal proceedings.
>
> Section 19 creates a new gateway giving HM Customs and Excise and the Inland Revenue a general power to disclose information held by them for law enforcement purposes and to the intelligence services for their purposes.[3]

The list of existing powers to which section 17 applies may be extended by statutory instrument.

Part 3 has proved controversial inside and outside Parliament due to the wide scope of its disclosure powers, which are not limited to anti-terrorist investigations, and the perceived danger of individuals' privacy rights being breached if hitherto confidential information is disclosed to the law enforcement and intelligence agencies. This paper discusses part 3, and the debate about these provisions, in depth.

By way of background, the paper discusses similar provisions introduced in the previous Session of Parliament in the *Criminal Justice and Police Bill 2000-01*. These were removed following opposition in the House of Lords, in order to secure the passage of the remainder of the Bill. The paper commences by highlighting relevant issues contained in the Performance and Innovation Unit report, *Privacy and Data Sharing*.

---

1 i.e. sections 17 to 20
2 Explanatory Notes, Para 3
3 Explanatory Notes, paras 10 and 11

CONTENTS

I Background: "Data-Sharing"

A. *Privacy and Data-Sharing*: the PIU Report

In September 2000, the Prime Minister asked the Performance and Innovation Unit (PIU), based at that time in the Cabinet Office, to produce a report on privacy and data issues. The PIU's report, *Privacy and Data-Sharing*, was much delayed, but was eventually published in April 2002.[4] The term "data-sharing" refers to the disclosure of personal information within and between departments, agencies and public bodies, including the sharing of information for purposes other than those for which it was originally collected. This can include:

- case-by-case sharing of information in support of service delivery
- bulk exchange of anonymised or pseudonymised data for policy making and statistical research
- bulk exchange of data, for example for crime prevention, relating to specific, identifiable individuals
- case-by-case sharing of data for investigation of crime or fraud in specific cases.[5]

The legal framework and safeguards applicable to data sharing will vary according to the category it falls under and the circumstances of the case. The policy and legal considerations highlighted by the report are considered in the next two sections of this paper.

1. Public Sector Policy

The PIU report was intended to set out "a new strategic approach to the use of personal data held by the public sector." The motivation for this new approach was:

> - first, an increasing recognition of the importance of effective and intelligent use of the personal data held by the public sector in delivering modern public services which better meet the needs of citizens; and
> - second, an equal recognition that the public has both formal rights and legitimate expectations that personal privacy will be protected.[6]

The issues considered in the report included data-sharing and data-matching across public sector boundaries. There were said to be three main areas where there is considerable potential to make better use of personal information to deliver benefits to the public:

---

4 Privacy and Data Sharing, Performance and Innovation Unit, April 2002, http://www.cabinet-office.gov.uk/innovation/2002/privacy/report

5 Op cit, Chapter 2 (introduction), para 2.07, http://www.cabinet-office.gov.uk/innovation/2002/privacy/report/02.htm

6 Op cit, executive summary, para 1.01, http://www.cabinet-office.gov.uk/innovation/2002/privacy/report/01.htm

- better, more joined-up and more personalised public services - particularly in enabling e-government;
- more effective and better targeted policy making and evaluation; and
- more efficient public services, including using data to improve value for money and streamline services, to help tackle crime and fraud, and improve the effectiveness of the enforcement of civil judgments, criminal court fines and breaches of community penalties.[7]

However, this potential would only be realised if the public trusted the way the public sector handles their personal data and protects their privacy:

> Public trust in the way that public sector organisations handle their personal data - and protect their privacy - is vital to the relationship between the citizen and public services. There are concerns that information technology - with more remote interactions and the greater use of personal information that it allows - could be a threat to privacy and lead to mistaken identity, inadvertent disclosure of private information and inappropriate transfer of data. There are some signs that the level of public concern about privacy is on the rise - for example, with an increasing proportion of people saying that they regard the right to personal privacy as very important. This anxiety has some parallels with shifting attitudes to food safety over the last decade.
>
> The Government made clear in the Modernising Government White Paper that "data protection is an objective of information age government, not an obstacle to it". This report strongly supports that statement, and looks at how to make it a reality. It is clear that if the public does not trust the way that the public sector handles personal information, then it will not be possible to achieve the potential benefits for individuals and for society from better use of data. In particular, this would put at risk the potential gains for the public from the move to the electronic delivery of public services.[8]

The PIU suggested that it was both possible and desirable for Government to achieve the twin objectives of enhancing privacy and making better use of personal data to deliver "smarter" public services. This would require a more strategic approach by the public sector, underpinned by four "high level principles":

- using the data available in the most efficient and effective way possible to achieve goals;
- adopting the least intrusive approach - i.e. where the public sector can achieve improvements in services or efficiency without requiring more data and affecting personal privacy, it should do so, recognising that the protection of privacy is itself a public service;

---

7 Op cit, executive summary, para 1.03
8 Op cit, executive summary, paras 1.07-8

- wherever possible, and where the benefits of better use of personal data are for the person using the service, giving citizens more choice in the management and use of their personal data to deliver public services; and
- ensuring that where data are used or shared without the consent of the individual (for example, in law enforcement), there is openness, transparency and consultation in the policy-making process of striking a balance between individual rights and the wider public interest.[9]

The report suggested that in seeking to apply these principles to decisions about the need for increased data use or data-sharing, public services should systematically:

- assess the benefits of the proposed data use/data-sharing in meeting public policy objectives;
- consider alternative approaches to achieving the objectives which have a lesser impact on privacy;
- identify the costs and risks of increased data use/data-sharing, recognising that many of the risks to privacy will be difficult to quantify;
- assess safeguards that would minimise the risks (for example, using privacy enhancing technologies); and
- use the accumulated evidence to strike a balance between the benefits and the costs and risks.

Where increased data-sharing is proposed after this analysis, policy makers should therefore be in a position to explain why the public interest will benefit and that the proposed action is a proportionate response to the public policy objective.[10]

The PIU identified five key areas for action. These included "building public trust". In order to build greater trust in the way that they handle personal information, public sector organisations would need to:

- adopt clear and consistent principles governing the way personal information is used right across the public sector;
- improve access to personal data, and adopt simple processes for correcting mistakes;
- put in place a named senior manager with clear responsibility for the handling of personal information; and
- ensure citizens are aware of their rights and what the law allows.[11]

---

9 Op cit, executive summary, key points
10 Ibid
11 Op cit, executive summary, para 1.18

The report included for consultation a Public Services Trust Charter setting out the principles that should govern the way personal information is used by the public sector. The charter is intended to set out the Government's commitment to privacy

> as a fundamental human right, underpinned by legislation, and [communicate] the standards of service and care by which the public sector should be judged. It should be backed up for individual services by more specific Privacy Statements and Codes of Practice.[12]

2. The Legal Framework for Data Sharing

The PIU report called for a clearer and better legal framework for data sharing. The report observed that the legal regulation of data-sharing is based on a number of different elements:

- the statutory regulation set out, in particular, in the *Data Protection Act 1998* and the *Human Rights Act 1998*;
- the common law, particularly the duty of confidentiality; and
- the administrative powers that public bodies have to collect, hold, share and use personal data.[13]

These elements, which are also relevant to the data-sharing provisions in part 3 of the *Anti-Terrorism, Crime and Security Act 2001*, are considered in turn below.

a. Existing Statutory Regulation: Data Protection and Human Rights

The *Data Protection Act 1998*

The Data Protection Act (DPA) regulates the processing (collection, use and disclosure) of personal information held on computer, other electronic media and, in certain circumstances, in paper files. "Data controllers" (organisations etc. which process personal information) must comply with eight data protection principles set out in Schedule 1 of the Act.

The Data Protection Principles

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.

---

[12] Ibid
[13] Op cit, chapter 10, summary, http://www.cabinet-office.gov.uk/innovation/2002/privacy/report/10.htm

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

The first principle requires that personal data may not be processed at all unless one of the conditions in Schedule 2 of the DPA is met. These conditions are quite broad. The first condition is that the individual has given his consent, but there are various conditions which would enable public authorities to process personal information without consent. For example, processing may be carried out where:

> The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Another condition is that the processing is necessary for the administration of justice; the exercise of any functions conferred on any person by or under any enactment; the exercise of any functions of the Crown, a Minister of the Crown or a government department; or for the exercise of any other functions of a public nature exercised in the public interest by any person.

The conditions in DPA Schedule 3 for processing "sensitive personal data" are more stringent, as one might expect. Sensitive data includes the racial or ethnic origin of the individual, his political opinions or religious beliefs, whether he is a member of a trade union, his physical or mental health or condition, his sexual life and any information about criminal convictions or any offence he is alleged to have committed. The first condition is that the individual has given his *explicit* consent. Again, there are various

conditions which would enable sensitive data to be processed without consent, including the condition that the processing is necessary for the administration of justice; the exercise of any functions conferred on any person by or under an enactment; or for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

Assuming that a public authority has the necessary authority to process personal information under Schedule 2 and, if necessary, Schedule 3, various data protection principles may place restrictions on the disclosure of such information, or data sharing (unless a relevant exemption applies). For example, it is not normally possible to disclose information if disclosure is incompatible with the purpose for which it was obtained (second principle).

Sections 7 to 9 of the DPA give an individual the right to be told by a data controller, on request in writing, whether they are processing that individual's information and if so, to be given a description of the information, the purposes for which it is being processed and those to whom it is or may be disclosed.

There are various exemptions under part IV of the DPA which may free public authorities from the normal restrictions on the disclosure of personal information. For example, sections 28 and 29 of the 1998 Act provide extensive exemptions relating to national security, crime and taxation. These are discussed in greater detail in part II(B) below.

The *Human Rights Act 1998*

The Human Rights Act (HRA) is designed, as its long title says, to "give further effect to rights and freedoms guaranteed under the European Convention on Human Rights". The HRA requires all public authorities to act in a way which is compatible with Convention rights. "Public authorities" include courts and tribunals, central government, local government, the police and any other "persons certain of whose functions are functions of a public nature" if the nature of the particular act complained of is not private. The term does not include the Houses of Parliament (except the House of Lords in its judicial capacity) or people exercising functions in respect of proceedings in Parliament.

In addition, the HRA:

- requires that, as far as possible, all primary and subordinate legislation is interpreted by the courts and others in a way that makes it compatible with the rights under the Convention;

- enables courts from the High Court upwards (in Scotland, the High Court of Justiciary) to make declarations of incompatibility where they cannot interpret primary legislation in such a way as to make it compatible with the Convention;

- enables the courts to disapply subordinate legislation which cannot be interpreted in a way which makes it compatible with the Convention, unless it is primary legislation which prevents the removal of the incompatibility; and

- enables individuals who believe that their rights under the Convention have been breached by a public authority to seek judicial review or to rely on their rights as a defence in civil or criminal proceedings.

The Convention rights protected under the *Human Rights Act 1998* are set out in Schedule 1 of the Act. The right most relevant to disclosure of personal information by public authorities is Article 8: the right to respect for private and family life:

> **Right to respect for private and family life**
>
> 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.

The right protected by Article 8 is sometimes referred to as a *qualified right*: in other words, the right is not absolute. Interference with qualified rights is permissible if what is done:

a) has its basis in law;
b) is done to secure a permissible aim set out in the relevant Article, for example for the prevention of crime, and
c) is necessary in a democratic society, which means it must fulfil a pressing social need, pursue a legitimate aim and be proportionate to the aims being pursued.

The need for "proportionality" under condition (c) is an important restriction on the interference with an individual's rights by any public authority.

Guidance produced jointly by the Bar Council and the Home Office defines the proportionality test as follows:

> Even if a particular policy or action which interferes with a Convention right pursues a legitimate aim (such as the prevention of crime) this will not justify the interference if the means used to achieve the aim are excessive in the circumstances.
>
> Any interference with a Convention right should be carefully designed to meet the objective in question and must not be arbitrary or unfair. Public authorities must not use a sledgehammer to crack a nut. Even taking all these considerations

> into account, interference in a particular case may still not be justified because the impact on the individual or group is just too severe. For example, the European Court of Human Rights took this view when it ruled that an outright ban on homosexuals serving in the armed forces was not compatible with the ECHR rights.[14]

b. The Duty of Confidentiality

The disclosure of personal information may give rise, under common law, to a claim in the courts for breach of confidence. For such a claim to succeed, it would be necessary to prove that:

1. the information has the necessary quality of confidence;
2. it was imparted in circumstances imposing an obligation of confidence; and
3. there is an unauthorized use of the information to the detriment of the original communicator of the information.[15]

However, where the public interest in the disclosure of confidential information outweighs the desirability of enforcing the obligation to protect confidence, the disclosure of confidential information will be lawful.[16]

c. Administrative Powers to Disclose Information etc

The PIU concluded that the main legal obstacles to achieving the policy goals on data sharing discussed above were centred around questions of the extent and scope of administrative powers rather than the statutory framework imposed by the *Data Protection Act 1998*. Local authorities and other statutory bodies may be restricted by the requirement that they can do only what statute allows them to: this is known as the doctrine of *ultra vires* (literally, "beyond the powers"). Where no specific data-sharing power exists, consent does not necessarily provide a legal basis upon which to share data:

> Consequently, several data-sharing initiatives - including many of those cited in Chapter 11 - are currently blocked as the bodies concerned cannot share the information necessary to support the service, even if the individual has consented to the data-sharing. For instance:
>
> - the UK Passport Service (UKPS) would like to issue renewal reminders to passport holders six months before their passport is due to expire. For this scheme to be workable, however, UKPS needs up-to-date address information. The address data held by UKPS is usually out of date, as most people move during the ten-year life span of their passport. UKPS would therefore like to get up-to-date address data from the Driver and

---

14 Human Rights Act 1998: Study Guide, paras. 3.8-9, http://www.lcd.gov.uk/hract/study.pdf
15 *Coco v. AN Clarke (Engineers) Ltd* [1968] F.S.R.415
16 Sallie Spilsbury, *Media Law*, 2000, p201

> Vehicle Licensing Agency (DVLA), but legislation would be needed to enable DVLA to disclose this information to UKPS; and
>
> - local authorities would like to use core Council Tax information - mainly name and address - as the basis for customer management databases in supporting one-stop shops, an innovation that can have major benefits for the community by helping to streamline service delivery. However, the Local Government Finance Act 1992 prevents the use of this data for any purpose other than the administration of Council Tax, regardless of the benefits that could be provided to the community.[17]

In some instances, the report observes, it is considered necessary to have power to share data without the individual's consent:

> - for operational concerns - the cost of establishing a system based on consent may be too high or the benefits may be realised only if all data subjects opt in;
> - for policy objectives - for instance, in tackling crime and fraud or improving enforcement of civil judgments. In addition, effective law enforcement relies heavily on intelligence gathering, where information on the suspect and their known associates may be needed for an investigation; or
> - for research, historical or statistical purposes - for instance, the production of anonymised National Statistics. The [Data Protection Act] provides an exemption for secure use in these circumstances.[18]

The PIU concluded that public authorities' administrative powers lacked sufficient flexibility to be able to respond to new needs for data-sharing:

> The sufficiency of powers to share data in each instance is constantly in question. Where consent is given, organisations may still be unable to share data due to the narrow definition of their administrative powers. In the field of crime, criminals are finding new ways of avoiding detection, and gateways need to be expanded to cope with new threats and new forms of crime.
>
> Consequently, public bodies are restricted in their options for taking advantage of new opportunities, even where there is explicit demand for new services or where citizens are willing to give consent for their information to be shared. What is clear is that better data use will be a key enabler for more effective public services.[19]

An earlier PIU report, *Recovering the Proceeds of Crime*, had recommended the creation of a specific power to enable the Revenue authorities to disclose information to the police

---

17 Op cit, chapter 10, para 10.8, http://www.cabinet-office.gov.uk/innovation/2002/privacy/report/10.htm
18 Op cit, chapter 10, para 10.9
19 Op cit, chapter 10, paras 10.10-11

authorities for criminal investigations and proceedings.[20] This proposal, which eventually gave rise to Part 3 of the *Anti-terrorism, Crime and Security Act 2001*, is discussed in section I(B) of this paper, below. *Privacy and Data Sharing*, however, contains three more general recommendations on the legal framework for data sharing:

> **Recommendation 23: The Lord Chancellor's Department should develop guidance on the interpretation of administrative powers and the key principles within the Data Protection Act with regard to how data-sharing can and should operate within the existing legal framework.**
>
> **Recommendation 24: The Government should consult on the introduction of legislation to enable public bodies to share personal data with the consent of the data subject. This power would need to operate without prejudice to existing data-sharing gateways and practices.**
>
> **Recommendation 25: The Government should consult on change to enable data-sharing gateways to be established via secondary legislation, subject to a codified list of tangible safeguards and adequate Parliamentary scrutiny.[21]**

The proposal to enable new data-sharing powers to be created by secondary legislation would appear to be the most contentious of these. The proposal relates to circumstances where it is not considered appropriate to seek the consent of the individual to the disclosure of their information. The PIU's discussion of this issue is reproduced below:

> **Data-sharing without consent**
>
> There are, however, several circumstances in which the individual's consent may not be an appropriate mechanism for enabling data-sharing. In particular, in fighting crime and fraud, in improving civil enforcement, tackling fine-evaders and in providing core services such as health and welfare, operational necessities will often militate against obtaining the individual's consent. In these circumstances, a different model would be necessary.
>
> The move to establishing such data-sharing gateways through secondary legislation would be a substantial step, one which would necessitate clear, codified safeguards to be attached to the enabling legislation. For instance, any or all of the following safeguards could be attached to any possible model:
>
> - the need to ensure effective Parliamentary scrutiny, together with consultation with key stakeholders, such as data subjects and the Information Commissioner;
> - requiring secondary legislation to be passed under the affirmative resolution procedure and/or making each order subject to a sunset clause, requiring orders to be renegotiated after a set period;

---

[20] June 2000, http://www.piu.gov.uk/2000/crime/crime.shtml
[21] Op cit, chapter 10

- specifying which public bodies were covered by enabling legislation, or the types of personal data that could be shared through gateways created under the enabling legislation; or
- requiring public services to set in place adequate safeguards. A Code of Practice, which included standard internal sanctions for abuse, could even be included as one of the requirements within the legislation.

> The move to secondary legislation would, with these safeguards, be a balanced package. The move to secondary legislation is indeed a substantial step, but it should be borne in mind that the courts would have the right to strike down secondary legislation that contravened the Human Rights Act. The onus would therefore be on departments to illustrate proportionality.
>
> Clearly, enabling legislation would be a significant step. There is a careful balance that needs to be struck between enabling public services to establish modern methods of service delivery for the public good, and the need to ensure that Parliament has adequate opportunity to examine such data-sharing proposals in detail.
>
> There are several possible models for change, and the model presented above is one of many that could be envisaged. Possible changes to legislative processes should not be seen in isolation. The recommendations set out in this report should be viewed as a coherent package, designed to enable e-government and a step change in service delivery with public trust and engagement.[22]

The PIU's proposal has similarities to the order-making power created by subsection 17(3) of the *Anti-terrorism, Crime and Security Act 2001*, discussed later at part II(A) of this paper.

The Foundation for Information Policy Research (FIPR), a privacy pressure group, criticised the PIU's proposal to enable compulsory data sharing to be introduced by secondary legislation.[23] The Parliament-Industry Group EURIM[24] made the following comments:

> In exceptional cases, such as in fighting crime, when data is shared without the data subject's consent, more must be done to convince individuals that safeguards will be respected. The recent controversy over the range and variety of bodies covered under Section 22 of the Regulation of the Investigatory Powers Act indicates the scale of the task.

---

22 Op cit, chapter 10, paras 10.28-32

23 FIPR Press Release, "Government Data Sharing Report is Late and Deeply Disappointing", 11.4.02, http://www.fipr.org/press/020411datasharing.html

24 EURIM describes itself as "the all-party, pan-industry "lobby" where the politics of the Information Society and E-Commerce are discussed across political, organisational and national boundaries prior to public debate.

> EURIM's reservations about the use of secondary legislation are most acute in circumstances in which data may be shared without consent. A possible way around the problems of secondary legislation would be to introduce a 'super affirmative procedure' akin to that recently introduced in the Regulatory Reform Orders. The merit in this procedure is that it allows for in-built consultation, and therefore has the affect of operating like primary legislation without its disadvantages in the legislative logjam.
>
> EURIM have also expressed concerns about the way in which data sharing will overlap with the private sector, (including out-source contractors), when processing may be contracted offshore. The report needs to elaborate on this. Increasingly the boundaries between public and private are becoming blurred, and throughout our response we have asked for more detail on which bodies are covered by the term public body, as it is often unclear.[25]

The law firm Nabarro Nathanson, which has a large number of public sector clients, including local authorities, suggested that altering the data-sharing framework through secondary legislation might, paradoxically, increase the level of scrutiny such changes received:

> While this Recommendation has attracted adverse criticism from some commentators, we believe that it may potentially be able to satisfy two aims, namely on the one hand:
>
> **(i)** providing a streamlined route for local authorities (among others) to seek data sharing powers that are otherwise difficult to obtain through existing routes;
>
> and on the other hand
>
> **(ii)** ensuring that creation of such powers is subject to more rigorous scrutiny than would otherwise be the case by use of existing routes.
>
> […]
>
> It has been commented generally that the practice of appending data sharing gateway powers as clauses within more substantive legislation (as for instance with s.60 of the Health and Social Care Act 2001, and various other provisions) perversely means that less attention and scrutiny is paid to it, as part of a wider measure, than might be paid if it were to be a measure of secondary but more self-standing legislation.
>
> We find this argument to be potentially persuasive. However the extent to which this argument succeeds will depend on the level of scrutiny which is actually

---

[25] Response to the PIU Privacy and Data Sharing report by the EURIM Personal Identity Sub-Group, July 2002

> achieved under this route – both in terms of formal scrutiny and in terms of the more coherent attention which it will enable to be given to data sharing in the round.[26]

The Nabarro Nathanson submission went on to outline some of the safeguards which they considered might be appropriate if such a power was introduced. These included:

- requirement for ministerial consultation with the Information Commissioner before issuing the statutory instrument;
- requirement for prior public consultation facilitated by the LCD or Information Commissioner;
- requirement for some form of prior authorisation by the Information Commissioner before commencement of any particular scheme;
- requirement for an authority to state publicly which data sharing powers it may at any time be relying on, and in relation to which operations it relies on such powers;
- requirement for relevant data sharing protocols and codes of practice to be drawn up/ lodged with the Information Commission/ made publicly available and accessible; and
- requirement for authorities to comply with or have due regard to guidance issued by relevant government departments.[27]

The CBI's response to the PIU report did not reach a firm conclusion on whether secondary legislation was the better means of creating new data-sharing gateways. Nevertheless, the Confederation warned that much work was needed to establish public acceptance of data-sharing by public authorities:

> An issue of over-riding concern to Government as a whole is the question of how far people will accept challenges to some individual freedoms in the interest of the public good. This issue is addressed directly in the paragraphs on identification and entitlement towards the end of the report, but it is relevant to all public sector access to and use of personal data. Many individuals, in contrast to most businesses, have a natural suspicion of data sharing by public sector bodies and have to be won over.
>
> Getting individuals to accept, and indeed welcome, data sharing by public sector bodies will have been made more difficult by such experiences as Inland Revenue's exposure of personal data, and more recently the controversy over extensions to the RIP Act[28]. This second example has highlighted (and probably inflamed) strong views not only on access by Government etc to personal data,

---

[26] Response to the Performance and Innovation Unit report on "P*rivacy and Data-Sharing: the way forward for public services*", Nabarro Nathanson, Solicitors, July 2002, paras 4.1.1 and 4.2.1-2.

[27] Nabarro Nathanson, op cit, paras 4.4.3-4.

[28] *Representation of the People Act 2000*

> but also on the ways that it is, can be and should be shared among departments. We believe that Government must learn from recent failures and are willing to help it reconsider what can be done and ways forward.[29]

B. The *Criminal Justice and Police Bill 2000-01*

Data-sharing provisions similar to those now set out in part 3 of the *Anti-terrorism, Crime and Security Act 2001* were included in the *Criminal Justice and Police Bill 2000-01* when it was first introduced in January 2001.[30] The Government agreed to their removal at the Bill's Report stage in the Lords in order to secure the safe passage of the remainder of the Bill. The fate of these provisions is discussed later, but first their origin in an earlier PIU report is described.

1. Background: The June 2000 PIU Report

The data-sharing provisions in the *Criminal Justice and Police Bill* followed a recommendation in *Recovering the Proceeds of Crime* published by the Performance and Innovation Unit in June 2000.[31] The report recommended (amongst other things) that the Revenue authorities should be allowed to disclose information to the police authorities for criminal investigations and proceedings.[32] 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* [1998] *(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

---

29 Data Sharing and Privacy: CBI response to PIU report and consultation document, July 2002, paras 7-8

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

31 http://www.piu.gov.uk/2000/crime/crime.shtml. See No.10 Downing Street press release, *New measures to ensure that crime doesn't pay*, 14 June 2000

32 Many of the other proposals in the report are given effect by the *Proceeds of Crime Act 2002*. For more details see the Library Research Paper on the *Proceeds of Crime Bill* (Paper 01/79, 29 October 2001)

bodies only in the event of murder or treason.[33] 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.[34] 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 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.[35]

2. The Bill

In January 2001 the Government announced that it would implement the PIU proposal, as part of the *Criminal Justice and Police Bill 2000-01*.[36] 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

---

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

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

35 *Recovering the proceeds of crime*, June 2000, pp 94-95

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

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.[37]

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."[38]

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

- 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

---

37 HC Deb 29 January 2001 c 41

38 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).

> 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.[39]

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.
>
> 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,

---

[39] SC F 6 March 2001, c412

> 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.[40]

The amendment was defeated on a division.[41] However, when the *Anti-terrorism, Crime and Security* Bill was published in November 2001, the equivalent provisions contained a definition of "criminal proceedings" designed to ensure that information cannot be disclosed for the purposes of criminal proceedings overseas unless the conduct with which the defendant is charged would constitute criminal conduct in the UK.[42]

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

---

40 Ibid, cc 421-2
41 Ibid, c426
42 Anti-terrorism, Crime and Security Act 2001, Section 20(2)

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.[43]

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.[44]

Following the passage of the Bill from the Commons, Baroness Noakes raised a number of specific concerns about clause 47 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."[45] Lord Bassam of Brighton, Minister of State at the Home Office, responded for the Government, first in his winding up speech on the Second Reading, and second in subsequent correspondence.[46] 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.

---

43 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).

44 SC F 6 March 2001 c 537

45 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.

46 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).

> 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.[47]

In a written briefing, Lord Bassam noted that Revenue departments already disclose information to other public authorities in certain circumstances:

> 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 from passing information to the police about a drug-trafficker or money-launderer.[48]

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 49[49] 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?

---

47 HL Deb 2 April 2001 cc 690-1

48 Home Office, 10 April 2001 p 7

49 [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.]

> 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.[50]

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.[51] 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.
>
> 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.[52]

---

50 HL Deb 2 April 2001 c 691

51 [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.]

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

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.[53]

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 disclosure cannot be made unless there is reasonable evidence that a crime has been committed.[54]

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 were 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

---

53 Home Office, 10 April 2001 p 7
54 HL Deb 2 April 2001 cc 691-2

> 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.[55]

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 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?[56]

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

---

55 Home Office, 10 April 2001 pp 5-6
56 HL Deb 2 April 2001 cc 690-692

> 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.[57]

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 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.[58]

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

---

[57] HL Deb 2 April 2001 c 713
[58] Home Office, 10 April 2001 p 6

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."[59] 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.[60] 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.[61]

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.[62]

As mentioned above, similar provisions were subsequently passed later the same year as part 3 of the *Anti-Terrorism, Crime and Security Act 2001*.

II Part 3 of the *Anti-Terrorism, Crime and Security Act 2001*

In his statement to the House on measures against financing terrorism on 15 October 2001, the Chancellor, Gordon Brown, confirmed that powers would be introduced shortly to allow the tax authorities "where applicable to share information and co-operate more effectively with the police".[63] 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

---

59 HL Deb 8 May 2001 c 2039
60 HL Deb 8 May 2001 c 2055
61 HL Deb 9 May 2001 c 2173
62 HC Deb 10 May 2001 c 303
63 HC Deb 15 October 2001 c 940

> police will have more sources of information from the Inland Revenue about crimes that are being committed.[64]

These provisions, which subsequently became part 3 of the *Anti-Terrorism, Crime and Security Act* 2001, were very similar to those discussed earlier which were removed from the *Criminal Justice and Police Bill*.

According to the Explanatory Notes to the Act, part 3 is intended to

> ensure that government departments and agencies can collect and share information required for countering the terrorist threat.[65]

This part of the Act contains two main provisions, sections 17 and 19, which are described as follows in the Explanatory Notes:

> Section 17 clarifies and extends a number of existing provisions for disclosure of information from public authorities to agencies involved in criminal investigations and proceedings. The gateways ensure that public authorities can disclose information which is subject to a statutory restriction on disclosure for the purposes of a criminal investigation or criminal proceedings.
>
> Section 19 creates a new gateway giving HM Customs and Excise and the Inland Revenue a general power to disclose information held by them for law enforcement purposes and to the intelligence services for their purposes.[66]

The provisions of part 3 are discussed in greater detail below.

A. Extension of Existing Disclosure Powers

Schedule 4 lists various existing information disclosure provisions. Section 17 extends these powers, so that disclosures of information under the Schedule 4 provisions may be made

> to assist any criminal investigation or criminal proceedings being carried out in the UK or abroad or to facilitate determinations of whether or not such investigations or proceedings should begin or end.[67]

The provisions listed in Schedule 4 fall into two main categories. The first covers information obtained by public authorities in the course of investigations into efficiency or compliance with regulatory regimes. For example,

---

64 HC Deb 15 October 2001 c 952
65 Para 3
66 Explanatory Notes, paras 10 and 11
67 Explanatory Notes, para 63

- Trade Descriptions Act 1968, s28(5A), governs the disclosure of trade secrets etc. obtained by local authority trading standards officers in carrying out their enforcement powers under the Act.
- Employment Agencies Act 1973, s9(4), governs the disclosure of information about employment agencies obtained by DTI officials in the course of carrying out inspections under the Act.
- Fair Trading Act 1973, s133, governs (inter alia) the disclosure of information on businesses obtained by the Office of Fair Trading in the course of its consumer protection enforcement powers.
- Health and Safety at Work etc. Act 1974, s28(7), governs the disclosure of trade secrets etc. obtained by the Health and Safety Executive and others in carrying out their powers of inspection under the Act.
- Sex Discrimination Act 1975, s61(1), governs the disclosure of information obtained by the Equal Opportunities Commission in the course of formal investigations under the Act.
- Race Relations Act 1976, s52(1), governs the disclosure of information obtained by the Commission for Racial Equality in the course of formal investigations under the Act.

The other main type of provision listed under Schedule 4 concerns survey-type information obtained from producers etc. by public authorities in connection with their marketing functions (including the issuing of levies to support such functions). For example:

- Agricultural Marketing Act 1958, s47(2), governs the disclosure of information obtained from producers by agricultural marketing boards etc.
- Agriculture Act 1967, s24(1), governs the disclosure of information obtained from producers by the Meat and Livestock Commission.
- Cereals Marketing Act 1965, s17(2), governs the disclosure of information obtained from producers in the course of raising a levy to fund the Home Grown Cereals Authority.
- Fisheries Act 1981, s12, governs the disclosure of information about businesses obtained by the Sea Fish Industry Authority under the Act.

Other provisions include the following:

- National Savings Bank Act 1971, s12, governs the disclosure of information about customers of the bank (now known as National Savings and Investments).
- Energy Act 1976, paragraph 7 of Schedule 2 governs the disclosure of information obtained by virtue of the Act. The Act includes wide-ranging reserve powers enabling the Government to control the sources and availability of energy. Schedule 2 contains extensive powers to obtain information from producers and suppliers of energy in connection with its reserve powers.

The heart of section 17 is subsection 17(2), which lists the purposes for which information to which the section applies may be disclosed:

> a) […] any criminal investigation whatever which is being or may be carried out, whether in the United Kingdom or elsewhere;
> b) […] any criminal proceedings whatever which have been or may be initiated, whether in the United Kingdom or elsewhere;
> c) […] the initiation or bringing to an end of any such investigation or proceedings;
> d) […] facilitating a determination of whether any such investigation or proceedings should be initiated or brought to an end.

This was consequently the focus of much of the controversy over part 3 during its passage through Parliament (considered later). An analysis of parts of the human rights aspects of the *Anti-terrorism, Crime and Security Act 2001* by Helen Fenwick, now Professor of Law of the University of Durham, describes the scope of subsection 17(2) as "extraordinarily wide in a number of respects":

> The immense broadening of the existing disclosure powers is not confined under it to the protection of national security or to the fight against terrorism. It is not confined even to the investigation and prevention of serious crime. It extends to any offence whatever and therefore could include private prosecutions. The powers under (c) and (d) in particular are amazingly broad: section 17(2)(c) speaks of 'for the purpose of initiating any investigation', while section 17(2)(d) provides for disclosure at an even earlier stage – before it has been determined that an investigation should be initiated. Therefore the information sharing requirements can apply even before a suspicion has arisen as to any offence. Section 17(2)(c) and (d) are not qualified by any requirement that there should be certain initial grounds for suspicion.[68]

Ministers argued, during the passage of the Bill through Parliament, that narrowing the scope of the disclosure powers would impede the police and security forces, since neither the public authorities empowered to disclose information nor the police and security forces seeking disclosure would necessarily know whether the information sought related directly or indirectly to terrorism. For example, the Economic Secretary to the Treasury, Ruth Kelly, said in Committee in the Commons:

> If the clause were restricted to terrorist offences, it would be a significant impediment because the public official in each case would have to satisfy himself in advance of any disclosure whether the information was directly related to a terrorism investigation.[69]

---

[68] *Modern Law* Review, September 2002, Helen Fenwick, "The Anti-Terrorism, Crime and Security Act 2001: A Proportionate Response to 11 September?" p758

[69] HC Deb Vol 375, 26.11.02, c793, http://www.publications.parliament.uk/pa/cm/cmvol375.htm

At the Report stage in the Lords, the then Home Office Minister, Lord Rooker, said:

> At the time a public authority chooses to disclose to the police, say, an address which they suspect has been used by criminals, it may have no idea that those who live there are part of a terrorist network. It would not know. Its piece of the jigsaw is not connected to the parts held by other authorities. It is only in the course of the investigation that the situation becomes apparent. Under the Bill as drafted, the police would receive information related to suspect criminal acts. The police are the investigators. It is their job to put the various pieces together to see whether they make a picture. Many times they will not, but it is their job to add those pieces to the jigsaw.[70]

The Treasury may by order add any provision contained in any subordinate legislation to the list contained in Schedule 4. The order must be made by statutory instrument subject to the affirmative procedure: a draft of it must be laid before Parliament and it cannot have effect unless the draft has been approved by a resolution of each House.[71] No such order has yet been made. In the Bill as originally published, the order-making power was subject to the less-exacting negative procedure: the order automatically comes into effect unless either House passes a resolution to prevent it from doing so. In the ordinary course of events, such a resolution is not put before Parliament so the order comes into effect without a great deal of scrutiny. An amendment passed at Report stage in the House of Lords introduced the affirmative procedure, however.[72] The order-making power in subsection 17(3) has similarities to the PIU proposal, considered earlier, to enable new non-consensual "gateways" for the disclosure of information to be created by secondary legislation.[73]

Subsection 17(5) requires public authorities, in determining whether they may disclose information, to ensure that their disclosure is proportionate to that which is intended by disclosing. This subsection, which makes explicit the duty of 'proportionality' which would already seem to required under the *Human Rights Act 1998* by virtue of Article 8, was inserted during the passage of the Bill[74] in response to concerns about the human rights implications of part 3.[75] Helen Fenwick suggests that the insertion of this subsection might provide a limited additional restraint on the use of Section 17 as some disclosures of information:

> might not raise Article 8 issues, in which case the proportionality requirement might have some safeguarding impact. Also the legitimate aims under section 17(2)(a)-(d) might be viewed as going beyond the aims of Article 8(2). Thus

---

70 HL Deb Vol 629, 6.12.01, cc960-1, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

71 Subsections 17(3) and (4)

72 HL Deb Vol 629, 6.12.01, c975, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

73 See part I(A)(2)(c) of this paper.

74 HL Deb Vol 629, 13.12.01, cc 1433-4, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

75 See part I(A)(2)(a) of this paper, above, for a brief description of the Human Rights Act as it applies to the disclosure of information.

> section 17(5) may deter the use of general fishing expeditions, to an extent. However, given that the aims of section 17(2) are so very broad it would be hard to say whether a disclosure was disproportionate to the aim in question given the uncertainty generated by the wording 'any criminal investigation whatsoever' and the lack of a need for any existing suspicion.[76]

The public authorities covered by the disclosure powers in section 17[77] are those covered by the *Human Rights Act 1998*. This includes central government, local government, courts and tribunals, the police and any other "persons certain of whose functions are functions of a public nature", provided the nature of the particular act complained of is not private.

The Government argued during the passage of the bill that the *Human Rights Act 1998* would provide significant safeguards against inappropriate use of section 17. For example, the Economic Secretary to the Treasury, Ruth Kelly, said in Committee in the Commons:

> I guarantee that it provides strong safeguards for the disclosure of information. I emphasise that all the gateways in clause 17 are pre-existing: they have already been approved by the House, and nothing new is being debated today. They refer to specific information covered by existing statutory restrictions on disclosure. Safeguards are provided by the Human Rights Act 1998 and by the Data Protection Act 1984, and they still apply, so any information that is disclosed must be proportionate, necessary and lawful.[78]

A number of Peers, however, suggested that in practice it would be difficult for citizens to protect themselves adequately by using the Human Rights Act. In Committee, Lord Phillips of Sudbury said:

> The noble Lord made the point two or three times that many of the objections to Clause 17 are misplaced because the workings of the clause will have to be consonant with the requirements of the Human Rights Act, and he referred to the aspects of the Human Rights Act which deal with proportionality and reasonableness.
>
> However, although I am a great supporter of the Human Rights Act, both in concept and now, it has always seemed to me—I am not alone in this—that it would be a bad day for Parliament if it resorted to legislation which failed to grapple with the details, particularly as they may affect civil and individual liberties, but in every case fell back on the parrot cry, "Well, don't worry, old son, you've got the Human Rights Act". We on this side of the House feel very strongly—and I know that the main Opposition party concurs—that it is vital that

---

76 *Modern Law Review*, op cit, p760
77 By virtue of section 20(1)
78 HC Deb Vol 375, 26.11.02, cc793-4, http://www.publications.parliament.uk/pa/cm/cmvol375.htm

> the protections which, in our view, should be integral to what the noble Lord, Lord McIntosh, admitted was a huge extension of disclosure, should be clear, practical and useable. Above all, using the Human Rights Act to get at your remedy if the remedy is not on the face of the Act is an extremely uncertain business, not only because the Human Rights Act is couched in the most wide and general terms but because the only way of getting those protections is by court process. I need hardly tell the Committee that going to law to obtain protection against unfair disclosure, or against the denial of a disclosure that should be given, is not practical. There is no legal aid for that sort of case. The costs are way beyond the resources of anyone, other than through an organisation with a strong commitment to the legislative principles.[79]

This argument is developed by Helen Fenwick in her *Modern Law Review* article:

> It is disingenuous to suggest that the citizen can rely on Article 8 as a safeguard since there are both procedural and substantive problems in so doing. There is no mechanism for informing the citizen that disclosure has occurred, and therefore opportunities for raising Article 8 arguments are limited. They would normally have to be raised within a trial where the information disclosed formed part of the evidence against the defendant. However, at present the courts are unlikely to take the view that information obtained in breach of Article 8 is required to be excluded from evidence.[80] The citizen could bring a civil action against the public authority in question, or the investigatory body, under section 7(1)(a) HRA post-trial, relying on Article 8. But the section 17(2) powers are so broad that the body could normally claim that most disclosures satisfied the statutory tests. Thus the plaintiff might have to claim that section 17(2) itself breaches Article 8.[81]

Fenwick argues that it seems plausible that section 17(2) might be found to breach the proportionality test under Article 8. This view echoes that of the Joint Committee of Human Rights. In its second report on the Anti-terrorism, Crime and Security Bill, the Committee said:

> **There remains a significant risk that disclosures will violate the right to respect for private life under Article 8 of the ECHR, because of the range of offences covered, and the lack of statutory criteria to guide decisions and the lack of procedural safeguards to be followed when deciding whether it is necessary and proportionate to make a disclosure of personal information. We publish, as an appendix to this Report, the written evidence of the**

---

79 HL Deb Vol 629, 28.11.01, c385, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

80 [see *Khan v UK* (2000) 8 BHRC 310; *R v Khan* [1997] AC 558; *Attorney-General's Reference (No 3 of 1999)* [2001] 2 WLR 56. For discussion see H. Fenwick *Civil Liberties and Human Rights* (London: Cavendish Publishing, 2002, 3rd ed) at 890-896 and 900-909]

81 *Modern Law Review*, op cit, p761

> **Information Commissioner to the Committee in this regard. We endorse that evidence, and commend it to the attention of each House.**[82]

However, Fenwick suggests that if the citizen's rights under Article 8 had been breached, the best he or she would have a realistic prospect of achieving would be a declaration of incompatibility, since it would be difficult for the courts to interpret section 17(2) in such a way as to make it compatible with the European Convention on Human Rights. This, she suggests, would not provide a practical remedy for the individual citizen.[83]

By virtue of Subsection 17(6), section 17 does not limit any power to disclose that exists apart from that section. In other words, any disclosure power not mentioned in Schedule 4 is not affected, and neither are any of the non-crime related disclosure powers which may already be contained in the Schedule 4 provisions. Subsection 17(7) provides that information obtained before the commencement of section 17 may be disclosed by virtue of that section.

During the passage of the Bill, Members of both Houses drew attention to the fact that section 17 (unlike section 19) contains no specific statement that the power to disclose does not override the *Data Protection Act 1998*.[84] Ministers gave assurances that the DPA did indeed apply to section 17. For example, the Economic Secretary to the Treasury, Ruth Kelly, said:

> Safeguards are provided by the Human Rights Act 1998 and by the Data Protection Act 1984, and they still apply, so any information that is disclosed must be proportionate, necessary and lawful.
>
> **Mr. Grieve**: If the Data Protection Act is supposed to apply to clause 17, why is it cited specifically in respect of clause 19 but not in respect of clause 17?
>
> **Ruth Kelly**: Such provisions could have been included, but it was decided that that would confuse certain other issues—[Interruption]. Not in relation to this clause, but in relation to other measures. I can tell the hon. Gentleman, however—I see that the hon. Member for West Dorset (Mr. Letwin), who is sitting beside him, agrees—that the Data Protection and the Human Rights Acts apply to clause 17. If he disputes that, we can perhaps continue to debate it, but it is the case.[85]

In Committee in the Lords, the Government spokesman Lord McIntosh of Haringey said:

---

82 Joint Committee on Human Rights, *Anti-terrorism, Crime and Security Bill: Further Report*, Fifth Report, HL Paper 51/HC 420 of 2001-02, para. 24.

83 Under section 3 of the Human Rights Act 1998, the courts must if possible interpret primary legislation in such a way as to make it compatible with the Convention. If this is not possible, section 4 enables courts from the High Court upwards (in Scotland, the High Court of Justiciary) to make a declaration of incompatibility. Parliament can then decide whether and how to amend the law.

84 e.g. HC Deb Vol 375, 26.11.02, c792, http://www.publications.parliament.uk/pa/cm/cmvol375.htm

85 HC Deb Vol 375, 26.11.02, c794, http://www.publications.parliament.uk/pa/cm/cmvol375.htm

> The noble Lord, Lord Phillips, spoke as though the only constraint was the Human Rights Act and the Data Protection Act was not effective for this purpose. The Data Protection Act will apply in most cases, imposing restrictions on disclosure. It also gives the individual the right to ask the data controller what disclosures about them have been made in certain circumstances. The Data Protection Act is policed by the Information Commissioner. Surely that provides an alternative avenue of redress. If we add to that the fact that the duty of confidentiality on public officials towards patients or customers is in no way diminished by the provisions of the Bill, it will be seen that, although this is an extension, it is a justifiable one.[86]

Part I(A)(2)(a) of this paper, above, gives a brief description of the Data Protection Act as it applies to the disclosure of information, and part II(B), below, discusses the crime and national security exemptions under the DPA.

Section 18 governs the use of the section 17 disclosure powers in relation to overseas criminal investigations etc:

> This section enables the Secretary of State to prohibit the disclosure of information for the purposes of overseas criminal investigations or criminal proceedings that would otherwise be permitted by section 17 or without section 17 by the provisions modified by that section. 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 the Secretary of State pursuant to section 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).[87]

Helen Fenwick suggests that section 18 provides "a safeguard of sorts" since it enables the Secretary of State to block disclosure to public authorities or individuals abroad where "the legal system, procedures or integrity of the relevant foreign jurisdiction are not comparable to those of the UK and do not provide comparable protection".[88] She notes that the Secretary of State cannot block disclosure unless it would be more appropriate for the investigation to be carried out by the authorities of the United Kingdom or a third country. Fenwick continues:

---

86 HL Deb Vol 629, 28.11.01, c391, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

87 Explanatory Notes, Paras 64,65

88 *Modern Law Review*, op cit, p760

> Thus [section 18] does not indicate the grounds on which a direction [from the Secretary of State] would be viewed as needed on the grounds of the appropriateness in question. This opaque section provides for the only safeguard introduced under Part 3 against disclosures abroad which could be to a wide range of regimes. Clearly, the safeguard is also dependent on its actually being exercised by the Home Secretary.[89]

Section 20 defines terms used throughout Part 3. In particular, it specifies that "criminal investigation" only refers to the investigation of conduct (including alleged or suspected conduct, etc) which would be criminal if conducted in the UK. A similar restriction is placed on the definition of "criminal proceedings".[90] Thus, the powers granted by section 17 cannot be used to authorise the disclosure of information to public authorities or individuals overseas in relation to conduct which would not be criminal if carried out in the UK.

B. Disclosure of Information held by Revenue Departments

Section 19 enables the Commissioners of the Inland Revenue and Customs and Excise Departments to disclose information to the police and the security services, etc. 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."[91] In addition, information may be disclosed to the intelligence services in support of their functions.

Subsection 19(1) specifies that the power applies to information held "by or on behalf of" (including information held by a person who provides services to)[92] the Commissioners of Inland Revenue or Customs and Excise. As with section 17, the power to disclose information applies equally to information obtained before section 19 came into force. One commentator points to the "immense" volume of information collected by the Inland Revenue in particular:

> For instance, the Inland Revenue use powers in sections 16 to 18 of the *Taxes Management Act 1970* to regularly obtain from local authorities details of: *all* Housing Benefit claimants, *all* individuals on the Council Tax Register, *all* improvement grants, *all* licences (e.g. taxi, street trading) or approvals issued, *all*

---

89 Ibid

90 This restriction was not present in the equivalent provisions which were removed from the *Criminal Justice and Police Bill 2000-01*

91 Explanatory Notes, para 66, http://www.legislation.hmso.gov.uk/acts/en/2001en24.htm

92 Subsection 19(8). Where information is held on behalf of the Inland Revenue or Customs and Excise, it may only be disclosed by or with the authority of the Commissioners of those departments (Subsection 19(4).

> short term leases, *all* foster carers and *all* child minders (*Commons Hansard*, column 582W, 19.4.2000).[93]

Subsection 19(2) lists the purposes for which relevant information may be disclosed:

> No obligation of secrecy imposed by statute or otherwise prevents the disclosure, in accordance with the following provisions of this section, of information to which this section applies if the disclosure is made-
>
> a) for the purpose of facilitating the carrying out by any of the intelligence services of any of that service's functions;
> b) for the purposes of any criminal investigation whatever which is being or may be carried out, whether in the United Kingdom or elsewhere;
> c) for the purposes of any criminal proceedings whatever which have been or may be initiated, whether in the United Kingdom or elsewhere;
> d) for the purposes of the initiation or bringing to an end of any such investigation or proceedings; or
> e) for the purpose of facilitating a determination of whether any such investigation or proceedings should be initiated or brought to an end.

Purposes (b) to (e) mirror those contained in subsection 17(2), but purpose (a) applies to section 19 alone. It enables disclosure to the intelligence services, ie. the Security Service (MI5), the Secret Intelligence Service (MI6) and GCHQ in support of their functions. These functions include the protection of national security and economic well-being and the prevention and detection of serious crime. For example, the activities of the Intelligence Service must be exercised:

> a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
> b) in the interests of the economic well-being of the United Kingdom; or
> c) in support of the prevention or detection of serious crime.[94]

GCHQ has similar purposes. The functions of the Security Service are defined thus:

> The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.

---

93 *Computers and Security*, Vol 21, no. 3, Dr Chris Pounder, "Anti-Terrorism Legislation: The Impact on the Processing of Data", September 2002, p243

94 Intelligence Services Act 1994, s1(2)

> It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.
>
> It shall also be the function of the Service to act in support of the activities of police forces, the National Criminal Intelligence Service, the National Crime Squad and other law enforcement agencies in the prevention and detection of serious crime.[95]

Subsection 19(3) requires that anyone intending to make a disclosure under section 19 must ensure that any disclosure is proportionate to that which is intended by disclosing. This mirrors subsection 17(5). It makes explicit the duty of 'proportionality' already required under the *Human Rights Act 1998* by virtue of Article 8, and was inserted during the passage of the Bill in response to concerns about the human rights implications of part 3. See part I(A)(2)(a) of this paper for a brief description of the Human Rights Act as it applies to the disclosure of information in general, and part II(A) for a discussion of how HRA applies to section 17 in particular.

Once information has been disclosed, subsection 19(5) limits its further disclosure:

> 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 the purposes of criminal investigations or proceedings.[96]

Thus if the police obtain information under section 19 for the purposes of a criminal investigation, for example, they may not subsequently disclose it to MI5 to assist in its more general function of safeguarding the economic well-being of the United Kingdom. The relevant Commissioners' consent to the onward disclosure of information obtained under section 19 may be given in the form of a general consent which specifies the circumstances in which such onward disclosures may be made.[97]

Subsection 19(7) specifically provides that section 19 does not override the *Data Protection Act 1998* (DPA):

> Nothing in this section authorises the making of any disclosure which is prohibited by any provision of the Data Protection Act 1998 (c. 29).

As mentioned above, there is no parallel provision in section 17. Part I(A)(2)(a) of this paper, above, gives a brief description of the DPA as it applies to the disclosure of

---

95 Security Service Act 1989, s1, as amended
96 Explanatory Notes, para 67, http://www.legislation.hmso.gov.uk/acts/en/2001en24.htm
97 Subsection 19(6)

information. To summarise, a number of the data protection principles which govern the 'processing' of personal information under the Act would tend to restrict the scope for disclosure of information collected for entirely separate purposes. However, sections 28 and 29 of the DPA provide extensive exemptions relating to national security, crime and taxation. For example, under section 28, personal information is exempt from the data protection principles if the exemption is required for the purpose of safeguarding national security. Section 29 contains four separate categories of crime and taxation-related exemption. In particular, under subsection 29(3), personal information may be disclosed to a third party even where this would otherwise be prohibited by the "non-disclosure provisions" of the DPA.[98] The purposes for which such disclosures may be made include:

- The prevention or detection of crime
- The apprehension or prosecution of offenders; or
- The assessment or collection of any tax or duty.

The Information Commissioner's legal guidance on the *Data Protection Act 1998* paraphrases the conditions for use of the national security exemption as follows:

> A certificate of exemption, signed by a Minister of the Crown, is conclusive evidence of the fact that the exemption is required for safeguarding national security. Such a certificate may identify the personal data by describing it in general terms and may have effect at a time in the future.[99]

In other words, the national security exemption is a "class exemption". The "non-disclosure" crime and taxation exemption, on the other hand, is only available on a case-by-case basis. The Information Commissioner's legal guidance describes the implications of this restriction:

> In the case of Equifax Europe Limited v The Data Protection Registrar (case DA/90/25/49/7) decided on 28th June 1991, the Tribunal held that in the context of the equivalent provisions in the 1984 Act, "in any case" means "in any particular case" and the provision would only apply, therefore, on a case by case basis.
>
> These three exemptions only apply where there is likely prejudice to one of the crime and taxation purposes. The Act does not explain the meaning of "likely to prejudice". Therefore, this is not to be regarded as a blanket exemption that would justify the withholding of subject access to whole categories of data where in fact those purposes would not be likely to be prejudiced in the case of all data subjects. It would also not justify the withholding of all the personal data about a particular data subject when only part of the personal data would be likely to prejudice those purposes.

---

98 Defined in section 27(3). The non-disclosure provisions include the second data protection principle and the requirement to process fairly and lawfully under the first data protection principle.

99 Para 5.2. Available at www.dataprotection.gov.uk

> The Commissioner takes the view that, for any of these three exemptions to apply there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be noticeably damaged. The data controller needs to make a judgement as to whether or not prejudice is likely in relation to the circumstances of each individual case.
>
> With regard to the first, second and third crime and taxation exemptions, the data controller should note the limitations on the use of this exemption. The data controller must consider each of the provisions in turn and decide which, if any, would be likely to prejudice any of the crime and taxation purposes, if they were applied.
>
> The data controller can only disapply those provisions which would be likely to prejudice one or more of the crime and taxation purposes and then only to the extent to which prejudice would be likely to result.
>
> If challenged, the data controller must be prepared to defend the decision to rely upon the exemption either to the Commissioner or to the Court. It would, therefore, be advisable for the data controller to ensure that each such decision is taken at an appropriately senior level within the data controller's organisation and for the reasons to be documented.[100]

By virtue of subsection 19(10), section 19 does not limit any power to disclose information which the Commissioners of Inland Revenue or Customs and Excise may have apart from under that section.

As pointed out above, section 20 specifies that "criminal investigation" only refers to the investigation of conduct (including alleged or suspected conduct, etc) which would be criminal if conducted in the UK. A similar restriction is placed on the definition of "criminal proceedings".[101] Thus, the powers granted by subsection 19(2)(b) to (e) cannot be used to authorise the disclosure of information to public authorities or individuals overseas in relation to conduct which would not be criminal if carried out in the UK. It would seem, however, that it would in theory be possible to disclose information to public authorities or individuals overseas under subsection 19(2)(a) if this was necessary in order to assist the intelligence services in carrying out any of their functions.

---

[100] Para 5.3.4. Available at www.dataprotection.gov.uk

[101] This restriction was not present in the equivalent provisions which were removed from the *Criminal Justice and Police Bill 2000-01*

III Scrutiny of Part 3

A. Parliamentary Committees

The Home Affairs Committee welcomed the disclosure powers in part 3 of the Bill, but other Parliamentary committees to consider the Bill were less enthusiastic about these powers. Extracts from the reports of the relevant committees are reproduced below.

1. Home Affairs Committee

The Home Affairs Committee reported on 19 November 2001:

> **We welcome the measures designed to improve data-sharing between government agencies which we recommended in our report on Border Controls earlier this year.**[102]

The earlier report had stated:

> **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).**[103]

2. Joint Committee on Human Rights

The Joint Committee first reported on the *Anti-Terrorism, Crime and Security Bill* on 16 November 2001:

> Part 3 of the Bill: Disclosure of Information
>
> Part 3 of the Bill (including Schedule 4) would permit public authorities to disclose information to each other for the purposes of an investigation. These apply in relation to any criminal investigation. They are not framed specifically, or even mainly, to deal with terrorism or security matters. They contain provisions originally introduced to Parliament as Part 2 of the Criminal Justice and Police Bill in January 2001. Information obtained by a very wide range of public authorities under a vast array of legislative provisions (now listed in Schedule 4 to the Anti-Terrorism, Crime and Security Bill) would be entitled to disclose it for the purpose (inter alia) of a criminal investigation into, or criminal proceedings for, any offence, in the United Kingdom or elsewhere, or for the

---

[102] The Anti-Terrorism, Crime and Security Bill 2001, HC 351, para 55, http://www.publications.parliament.uk/pa/cm200102/cmselect/cmhaff/351/35102.htm

[103] Home Affairs Committee, *Border Controls*, HC 163-I of 2000-01, para 12

purpose of 'facilitating a determination of whether any such investigation or proceedings should be initiated or brought to an end'. In addition, provision was made to remove the revenue departments' obligation of secrecy in relation to information if disclosure of the information would advance a wide range of criminal investigations or security functions. The provisions attracted criticism from this Committee, which concluded—

There is a need to introduce adequate safeguards into this legislation. Consideration should be given to amending these provisions to include ... a requirement that there should be reasonable grounds for suspecting that the information in question would be relevant to a criminal inquiry or that the data subject has committed an offence, and a requirement that a pre-disclosure assessment be made of the proportionality of disclosing information on a particular individual in the context of the offence in question. Consideration should also be given to limiting the very wide power to make disclosures "for the purposes of initiating ... any such investigation or proceedings." We draw the attention of each House to these provisions, and consider that necessary safeguards should be provided to ensure that they are compatible with the right to privacy.

The provisions were dropped from that Bill in the face of opposition in the House of Lords, in order to facilitate the passage of the remainder of the Bill before the general election. The provisions reintroduced in the current Bill still contain no express provision for appropriate safeguards to ensure that the powers will be used only in circumstances where their use is proportionate to a pressing social need. The Secretary of State would have power to exclude disclosures to overseas investigators in a limited range of cases, but has no obligation to do so, and could not prohibit disclosures by a Minister of the Crown or the Treasury. The new provisions do not immediately appear to meet the Committee's criticisms quoted above.

The matter was raised with the Home Secretary in oral evidence. One of his officials, Mr Harnett, sought to persuade us that the Treasury's intention had been to meet the Committee's concerns in the re-drafting of the clauses—

First of all, as we understood it, the Committee had a concern about limiting this disclosure to public authorities, and we have done that. In clause 20 we have described a "public authority" as that which has the same meaning ... as in section 6 of the Human Rights Act. So we feel that that not only deals with the specific point about disclosure, but the fact that we have anchored this ... to section 6 of the Human Rights Act means that any disclosure that a public authority makes must be compatible with Article 8 of the Convention ... and thereby it has to meet the tests of reasonableness and proportionality which we understand the Committee was concerned about in January. The other protection that we have looked at in drafting this part of the Bill is that which the Data Protection Act will apply, so we have attempted to address, and believe we have addressed, the Committee's concerns in those respects ... we still think that it is necessary that public authorities should be able to disclose information to others in relation to whether criminal investigations or proceedings should be initiated. We think it is extremely important that this Act does enable us to do that. Our view is that we—

> and when I say "we" it is the Treasury primarily that has been responsible for this part of the Bill that you have before you— have sought to take account of your concerns in the way I have described.
>
> We welcome this evidence of willingness to take account of our view, but we may wish to examine the revised provisions further.[104]

The Joint Committee produced a further report on the Bill on 5 December 2001:

> Part 3 of the Bill: Disclosure of Information
>
> We considered in our previous report the provisions of Part 3 of the Bill. We remain concerned about the provisions for sharing of information between agencies for the purposes of an unlimited range of criminal investigations, including potentially investigations by foreign agencies. Having considered the matter further since our Second Report, we are not satisfied that the small changes made to the provisions since their original appearance (as Part 2 of the Criminal Justice and Police Bill earlier in 2001) meet our fundamental concern. **In our view, there remains a significant risk that disclosures will violate the right to respect for private life under Article 8 of the ECHR, because of the range of offences covered, and the lack of statutory criteria to guide decisions and the lack of procedural safeguards to be followed when deciding whether it is necessary and proportionate to make a disclosure of personal information. We publish, as an appendix to this Report, the written evidence of the Information Commissioner to the Committee in this regard. We endorse that evidence, and commend it to the attention of each House.**[105]

3. Delegated Powers and Regulatory Reform

The Lords Select Committee on Delegated Powers and Regulatory Reform reported on 27 November 2001. Annex 3(a) to the report was a memorandum by the civil rights organization Justice on the use of delegated powers in the Bill. It recommended that the power to extend by secondary legislation the list of existing provisions falling under section 17 should be subject to the affirmative procedure, due to "the clear capacity of these powers to significantly intrude upon privacy rights, including the privacy rights of innocent third parties". The Committee recommended that the order-making power should be amended to make it subject to the affirmative procedure.[106] As noted earlier, the Government introduced such an amendment at the Report stage in the Lords.[107]

---

[104] HL 37/HC 372, Paras 53-5, http://www.publications.parliament.uk/pa/jt/jtrights.htm

[105] Joint Committee on Human Rights, *Anti-Terrorism, Crime and Security Bill: Further Report*, HL 51/HC 420, para 24, http://www.publications.parliament.uk/pa/jt/jtrights.htm.

[106] HL 45, para 17, http://www.publications.parliament.uk/pa/ld/lddelreg.htm

[107] HL Deb Vol 629, 6.12.01, c975, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

4. Constitution Committee

The Lords Constitution Committee reported on 23 November 2001. Due to the expedited progress of the Bill, the Committee did not have time to call a minister for evidence. Instead, it wrote to the then Minister of State at the Home Office, Lord Rooker, setting out its concerns and questions about the proper use of emergency legislation:

> Letter from the Lord Norton of Louth, Chairman of the Committee, to the Lord Rooker, Minister of State, Home Office.
>
> The Committee which I chair has been appointed by the House of Lords "to examine the constitutional implications of all public bills coming before the House; and to keep under review the operation of the constitution". We aim to report on bills before their second reading in the House of Lords. In this context we have some questions about the Anti-terrorism, Crime and Security Bill shortly expected to be brought to the Lords from the Commons. Rather than call you for oral evidence at a time when Home Office Ministers have answered on this legislation to several Parliamentary Committees, we would be grateful for a written answer to the following questions, or, if such an answer is not possible before second reading in the Lords, then for the Government to address these points in the debate at that stage. The Committee will today report to the House that I have written to you in these terms.
>
> ***Proper use of emergency legislation***
>
> Our scrutiny of this bill has not been assisted by the tight Parliamentary timetable in which it is sought to be passed. Parliament needs to ensure that adequate time is available to scrutinise complex and controversial measures contained in bills. This does not just relate to hours on the floor of each House, but also requires time for reflection between stages and time before second reading for scrutiny committees to do their work. You have justified the timetable for this bill by arguing that there is an urgent need to put in place measures to counter the threat of terrorism in the wake of the terrorist attacks in the United States of America on 11 September 2001.
>
> The bill however contains a number of measures which appear to us to be unrelated to terrorism, and powers which are not in any way limited to combating terrorism. These include the provisions allowing public authorities to disclose information for the purpose of any criminal investigation in the United Kingdom or abroad which were originally contained in Part 2 of the Criminal Justice and Police Bill but were dropped in the face of criticism in order to facilitate the passage of the remainder of that bill before the General Election; and extending the power of Ministry of Defence Police and British Transport Police to exercise constabulary powers off-site, originally contained in the Armed Forces Bill earlier this year and dropped following criticism.[108]

---

[108] HL 41, http://www.publications.parliament.uk/pa/ld200102/ldselect/ldconst/41/4101.htm

B. The Parliamentary Debates

1. Commons Second Reading

The *Anti-Terrorism, Crime and Security Bill 2001-02* received a second reading in the House of Commons on 19 November 2001. The Home Secretary, David Blunkett, introduced part 3 of the Bill as follows:

> Part 3 will enhance the power of disclosure to law enforcement agencies, with clear guidelines, and allow disclosure to be presented in constrained circumstances, including those that relate to criminal investigation.[109]

The Shadow Home Secretary, Oliver Letwin, expressed concerns about the scope of the powers in part 3:

> Part 3 deals with disclosure and includes strong provisions to increase the amount of disclosure of personal details by Government agencies, including the Inland Revenue and Customs and Excise. We shall try to limit that. The Bill would permit disclosure under the circumstances of any criminal investigation, including that of a minor offence. We want the provision restricted to terrorist-type offences.[110]

The Liberal Democrats' Home Affairs Spokesman, Simon Hughes, took up similar issues:

> Parts 3 and 11 deal with very important matters concerning the rights of the state to interfere in communications, to find out what communications, technological or otherwise, are passing between people and to require people in the communications industry to hold on to that information for much longer. We have only just legislated in that area. If we need more powers, they should be strictly limited to matters to do with terrorism, and they should be much more narrowly drawn. We shall seek to amend parts 3 and 11 to that effect.[111]

Winding up for the Government, the Home Office Minister, Beverley Hughes, answered the criticism that the Bill should have been restricted to anti-terrorist measures alone:

> The second general point was that the Bill's content is not restricted to terrorism. I fail to understand that concern. All the measures are designed to enhance intelligence and information gathering, to restrict people suspected of involvement in terrorism, to prevent abuse of asylum and to give law enforcement and security agencies powers to tackle the problems that we face. We cannot

---

[109] HC Deb Vol 375, 19.11.02, c34, http://www.publications.parliament.uk/pa/cm/cmvol375.htm
[110] HC Deb Vol 375, 19.11.02, c41, http://www.publications.parliament.uk/pa/cm/cmvol375.htm
[111] HC Deb Vol 375, 19.11.02, cc 57-8, http://www.publications.parliament.uk/pa/cm/cmvol375.htm

> draw a firm line between terrorism and crime. Crime funds and fuels terrorism, and the links between serious crime and terrorism are clear.
>
> […]
>
> The Bill will ensure that enforcement agencies, security services and Government Departments are able to detect and prevent terrorist attacks, and improve the security of industries that may be vulnerable. Terrorism's connection with crime means that the Bill covers a wide range of Government measures. It is not only one part out of 14 that deals with terrorism, as the right hon. and learned Member for Sleaford and North Hykeham maintained; all 14 are relevant to the tasks facing us.[112]

Ms Hughes concluded by asserting that the Bill was proportionate to the threat which the nation faced:

> In the aftermath of 11 September, while we do not need a wholesale revision of existing laws, we do need new levels of security and intelligence as well as exceptional temporary measures. The package of measures introduced in the Bill is balanced; it is a proportionate approach to the extraordinary circumstances that we now face. We are all striving to strike the best possible balance between the right of all our citizens to protect their safety, freedoms and liberties and the right of individuals whom we suspect of wrongdoing to due process and fair treatment. I believe that the Bill strikes that balance, and I believe the vast majority of ordinary people in this country think so too.[113]

The House divided, and agreed to give the Bill a Second Reading by 458 votes to 5.

2. Lords Second Reading

The Bill received a second reading in the House of Lords on 27 November 2001. The then Home Office Minister, Lord Rooker, introduced part 3:

> Part 3 deals with the disclosure of information. It widens the existing powers for the Inland Revenue and Customs and Excise to pass confidential information to law enforcement and intelligence agencies. At present, only information regarding murder or treason can be disclosed. That hampers the exchange of information in the fight against terrorism.
>
> Therefore, the Bill, in Part 3, allows for information to be disclosed for the purposes of a criminal investigation; for criminal proceedings; and where it would help decide whether an investigation or proceedings should start or finish. I fully accept that that is a highly sensitive part of the Bill with various government agencies exchanging information. It has been done in other

---

[112] HC Deb Vol 375, 19.11.02, cc 112-3, http://www.publications.parliament.uk/pa/cm/cmvol375.htm
[113] HC Deb Vol 375, 19.11.02, c115, http://www.publications.parliament.uk/pa/cm/cmvol375.htm

> legislation, most recently in last year's Social Security Fraud Bill. There must be good and compelling reasons for such disclosure and we believe that there are good and compelling reasons for the extension in this case.[114]

Lord Dixon-Smith, on behalf of the Official Opposition, drew attention to the effect of part 3 on regulated enterprises in the City of London.[115]

The Liberal Democrat spokesman, Lord Thomas of Gresford, raised a variety of concerns about part 3, including the possible disclosure of medical records, the lack of judicial oversight and the power to disclose Revenue information to the intelligence services:

> There appears to be no judicial control, no tests of reasonable grounds for believing that a crime has been committed, and no suggestion that conditions should be laid down by anyone concerning disclosure. Therefore, disclosure overseas could take place even though the conduct being investigated is not criminal conduct in this country and no charge has been brought.
>
> To illustrate that, the BMA is concerned about the position relating to medical records. Confidentiality has previously been overridden only in cases of serious crime in this country. Now it appears to extend to any criminal proceedings. Will the Minister say whether there are any curbs to that general requirement for disclosure from those various public authorities?
>
> Clause 19 permits the disclosure of all the 32 million tax files and all the VAT records kept in this country not just to the police but, for the first time, to the security services. That provision did not appear in the clauses of the Criminal Justice and Police Bill which were withdrawn in May. Again, the provisions are not limited to terrorism. Clause 19(2)(a) permits the disclosure to the security services,
>
> "for the purposes of facilitating the carrying out by any of the intelligence services of any of that service's functions".
>
> Therefore, the provision is couched in the widest possible terms, is not limited to terrorism and again is not subject to judicial control.[116]

Another Liberal Democrat Peer, Lord Phillips of Sudbury, expressed strong reservations:

> Many organisations are now beginning to realise that the purport of those sections could scarcely be more serious for the whole issue of public information, or private information drawn into the public sphere.

---

[114] HL Deb Vol 629, 27.11.01, c144, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[115] HL Deb Vol 629, 27.11.01, c155, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[116] HL Deb Vol 629, 27.11.01, c219, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

He referred to the concerns set out in the second report of the Joint Committee on Human Rights (on which, see part III(A)(2) above). Lord Phillips continued:

> Public authorities will be required to disclose information to each other in relation to any criminal investigation. As many noble Lords have said, one of the many bones of contention across the House is that a Bill which is rushed through this House in order to deal with an emergency terrorist situation is being used for much wider purposes.
>
> Under Part 3 of the Bill the authorities will be required to provide information in an extraordinarily wide range of circumstances: any criminal investigation; any criminal proceedings; and indeed any decision as to whether or not to investigate or pursue criminal proceedings. Public authorities include banks, health authorities, education establishments, all government departments and all quangos. The provisions will entitle Inland Revenue and Customs and Excise to reveal information about any individual in respect of any criminal matter whereas, as we sit here today, the only situations in which they can do that are those involving treason or murder.
>
> […]
>
> Some will say that the innocent have nothing to fear by disclosure. It is only the wicked and villains who should worry. But that is not true. The right to privacy long predates any human rights legislation. It is not a right in the formal sense but one that citizens of these lands have enjoyed since time immemorial. The Government would misjudge public opinion and anxiety if they were to proceed on an extraordinarily broad front with extraordinarily broad powers.[117]

The Earl of Northesk, a Conservative spokesman, feared that parts 3 and 11 would give public authorities "carte blanche to data-match to their hearts' content",[118] and a Liberal Democrat front-bencher, Lord Goodhart, said that part 3 raised serious questions under data protection laws, the right not to incriminate oneself and the right to privacy under Article 8 of the European Convention on Human Rights. That part of the Bill was "not targeted at terrorism or matters of urgency outside the context of terrorism" and needed "much fuller discussion than [it] will receive here". As such it was "not appropriate for inclusion in the Bill".[119]

Baroness Buscombe wound up on behalf of the Official Opposition:

> Turning to Part 3, at first glance I thought it all looked familiar and quickly realised that these very same proposals were, as we heard from the noble Lord, Lord Phillips of Sudbury, dropped at our insistence from the Criminal Justice and

---

[117] HL Deb Vol 629, 27.11.01, c247, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[118] HL Deb Vol 629, 27.11.01, c255, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[119] HL Deb Vol 629, 27.11.01, cc 268-9, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

> Police Bill earlier this year, because the Government had not allowed Parliament enough time to scrutinise them properly. Indeed, those proposals were not scrutinised at all in another place last time and nor in consideration of this Bill. Incidentally, when the proposals were presented to us in the Criminal Justice and Police Bill, I do not recall any mention of terrorism.
>
> We would not mind so much if the effect of these clauses was to fight terrorism. That is our purpose and should be the purpose of this Bill.
>
> So will the Attorney-General answer concerns that have been expressed both in the media and in another place with regard to these proposals that provide for the disclosure of confidential information across an enormously wide range of government agencies? It is our contention that these proposals will enable all government agencies to share information with police forces from anywhere in the world. That raises concerns in respect of the need for a process to approve the provision of information, especially where the criminal investigation is taking place in a country where there is inadequate data protection legislation.
>
> In addition, Clauses 17 and 19 allow police to trawl through files to consider whether a crime has been committed, even when there is no evidence that a crime has been committed. Also, Part 3 treats all data in the same manner, with no regard to whether it is personal, possibly sensitive data, confidential business information or information requiring less stringent protection.[120]

Winding up for the Government, the Attorney General, Lord Goldsmith, maintained that it was appropriate to include part 3 in the Bill, but noted concerns regarding judicial oversight and the limits on disclosure.[121]

3. Remaining Stages in Both Houses

a. The Scope of Section 17

During the passage of the Bill, various amendments to limit the scope of section 17 were debated. In the Commons, an amendment to limit the disclosure of information to cases involving terrorism and terrorist offences was not selected for debate during the Committee stage, but an identical amendment was debated at the Report stage. The Conservative Home Affairs spokesman, Dominic Grieve, introduced the amendment:

> **Mr. Grieve:** Clause 17 provides for the extension of existing disclosure powers to enable the exchange of information between Government agencies and Departments in a way that is unparalleled in our history. There is no restriction or fetter on the exchange of information, […] and the provision can be applied in any criminal investigation from a speeding offence to high treason. Schedule 4,

---

[120] HL Deb Vol 629, 27.11.01, c273, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[121] HL Deb Vol 629, 27.11.01, c287, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

> annexed to it, shows that the information cuts right across Government. Much of that information concerns matters that are, at present, surrounded by specific confidentiality clauses relating to the information imparted to the particular Government agency or Department.
>
> Thus it will now be possible for the Inland Revenue to share information with any other Government agency. Medical information, including the records of individuals, will be capable of being shared. The Health and Safety at Work, etc. Act 1974, with which I am particularly familiar, contains a specific clause which provides that statements may be obtained from individuals—indeed, they are compelled to provide them. That information, too, may now be shared, even though the 1974 Act specifically provided that it could be made available only for legal proceedings relating to the Act or in circumstances in which the individual consented.
>
> The manner in which this measure has been introduced gives rise to considerable concern. Last year, the Government attempted to do exactly this in the Criminal Justice and Police Bill, in which a very similar provision was introduced. It was hotly disputed, and by the time the Bill reached the House of Lords, the level of resistance was so great that, to save the legislation before the election, the Government agreed to drop the provision.
>
> The other place was right to be concerned about this issue, because it concerns such a fundamental shift in the way we conduct our affairs. Historically, we have been self-regulating and that has implied a willingness by the individual to supply information to Government agencies and Departments in the belief that confidentiality would be maintained. Only in exceptional circumstances has interdepartmental confidentiality been broken or agreement been reached for the sharing of information.
>
> Labour Members who may consider this a small matter should bear it in mind that the entire panoply of information sharing will be unfurled as a result of the changes and that we have been given precisely 25 minutes in which to consider them. They will not be considered in major legislation at all.[122]

The Liberal Democrat Spokesman, Simon Hughes, also spoke in support of the ammendment, emphasising the volume of information that would be covered:

> To take one example, the Revenue keeps records on 32 million people, and that information could be transferred as a result of the proposal. We are not told to whom that information could be passed, at whose request, the seniority of the person making the request, to what use it would be put and for what purposes it would thereafter be used.

---

[122] HC Deb Vol 375, 26.11.02, cc 791-2, http://www.publications.parliament.uk/pa/cm/cmvol375.htm

> Even if we were happy that this power should exist, and that it is a proper power for a police Bill, a criminal evidence Bill or a criminal justice Bill, Parliament was not willing to rush this provision through last year in such legislation. I hope that the House will agree that it is entirely inappropriate to rush it through under a guillotine in an emergency anti-terrorism Bill only a few months later.[123]

The Government opposed the amendment. Replying on behalf of the Government, the Economic Secretary to the Treasury, Ruth Kelly, said:

> The hon. Member for Beaconsfield (Mr. Grieve) fundamentally misunderstands the nature of these clauses. Clause 17 is designed to clarify for public officials in what circumstances they may disclose information. I think that many Members will recognise the need for that clarification. If the clause were restricted to terrorist offences, it would be a significant impediment because the public official in each case would have to satisfy himself in advance of any disclosure whether the information was directly related to a terrorism investigation. That does nothing to harmonise requirements or to make it simple for public officials to understand what they are supposed to disclose.
>
> **Mr. Grieve:** We do not want to make it simple. I am sure that the Minister will agree that each of the sections of each of the Acts listed in schedule 4 contain specific protections. She can read them. I quoted section 28(7) of the Health and Safety at Work, etc. Act 1974. Protection exists, but she intends to get rid of it. That is hardly a clarification.
>
> **Ruth Kelly:** I thank the hon. Gentleman for his intervention, but it again shows that he fundamentally misunderstands the nature of the clause.
>
> The hon. Gentleman disputes the fact that the clause contains safeguards. I guarantee that it provides strong safeguards for the disclosure of information. I ephasise that all the gateways in clause 17 are pre-existing: they have already been approved by the House, and nothing new is being debated today. They refer to specific information covered by existing statutory restrictions on disclosure. Safeguards are provided by the Human Rights Act 1998 and by the Data Protection Act 1984, and they still apply, so any information that is disclosed must be proportionate, necessary and lawful.[124]
>
> We see clause 17 as fundamental to the fight against terrorism. It is essential that we use all the means at our disposal to crack down on terrorism. It is absolutely right that information should be disclosed to us by public authorities in that manner.[125]

The amendment was rejected by 330 votes to 213.

---

[123] HC Deb Vol 375, 26.11.02, c793, http://www.publications.parliament.uk/pa/cm/cmvol375.htm
[124] HC Deb Vol 375, 26.11.02, cc793-4, http://www.publications.parliament.uk/pa/cm/cmvol375.htm
[125] Op cit, c796

A number of amendments seeking to restrict the scope of Clause 17 were discussed in Committee in the Lords. On behalf of the Official Opposition, Baroness Buscombe said:

> We are in two minds as to whether disclosure should be permitted to assist criminal investigations or criminal proceedings. We can see that as regards serious crime the balance probably comes down in favour of disclosure. On the other hand, we could not support disclosure for the purposes of minor criminal offences.[126]

She moved an amendment restricting disclosure to terrorist-related investigations, using the definition of terrorism set out in section 1 of the *Terrorism Act 2000*:

> "the use or threat of action where ... the use or threat is designed to influence the government or to intimidate the public or a section of the public, and ... the use or threat is made for the purpose of advancing a political, religious or ideological cause ... [if it] involves serious violence against a person ... involves serious damage to property ... endangers a person's life, other than that of the person committing the action ... creates a serious risk to the health or safety of the public or a section of the public, or ... is designed seriously to interfere with or seriously to disrupt an electronic system".[127]

Lord Thomas of Gresford moved an amendment with a similar purpose:

> My Amendment No. 51 seeks to include the words "involving terrorism". Its purpose is to limit the scope of an inquiry for the purpose of this emergency legislation. Those are broad words, "involving terrorism". We have to deal with the argument that the Minister has put forward; namely, that the Government want these wide powers because investigating bodies will not know whether a case involves terrorism until they decide to investigate and then carry out the investigation. I have used the words, "involving terrorism" in my amendment to enable those who seek such information to say, "We are from the security services and it is our duty to investigate the possibility of terrorism and information you may have which may assist us". That limits the scope of the people who can make that inquiry.
>
> If a local police constable goes down to the fish counting centre and says, "I demand to see your records of anthrax infected salmon that have come into the River Dee in the course of the past few months", I imagine that his application for that information may be resisted as it would not appear from such a request that he was a person involved in investigating, or considering the investigation of, terrorism. It seems to me that this clause attempts to encompass the widest

---

[126] HL Deb Vol 629, 28.11.01, c396, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[127] Ibid

> investigation or disclosure of information when it could be limited to the scope of the emergency provisions.[128]

Lord McIntosh of Haringey replied on behalf of the Government:

> The provisions of Part 3 are designed to clarify to public authorities whether or not they may disclose information. Restricting their disclosure solely to cases of terrorist offences would be a significant impediment to them. In each case it would force them to satisfy themselves, for fear of acting illegally, that the information was directly related to criminal conduct in relation to terrorism.
>
> Under the present drafting, individuals need to satisfy themselves that information would be relevant to a criminal investigation or proceedings. The amendments would limit the provisions and render them significantly weaker—and "weaker" is not meant in an abstract sense. It means weakening the pursuit of terrorism. I come back to that point time and again.[129]
>
> […]
>
> When the anti-terrorist squad, for example, or any other body is looking for terrorism, they are looking for activities that one can discover but which may not themselves be terrorist activities. Those activities involve other criminal activities that could lead one to terrorists. There is no alternative way to start an investigation involving terrorism other than by looking more widely.[130]

The amendments were withdrawn.

Lord Phillips of Sudbury moved amendments seeking to remove the power under sections 17 and 19 to disclose information for "the purpose of facilitating a determination of whether any such investigation or proceedings should be initiated or brought to an end":[131]

> It is apparent to the Minister that everyone in the Chamber bar the Government Front Bench believes that that entitlement to disclosure is far too wide. It means that an individual or body can engage in a pre-review of whether he wants to begin an investigation which may give rise to proceedings. We believe that that is far too wide and it serves no useful purpose. Given everything that has been said, I beg to move.[132]

He was supported by Baroness Buscombe. However, Lord McIntosh of Haringey, on behalf of the Government, said:

---

[128] HL Deb Vol 629, 28.11.01, c398, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[129] HL Deb Vol 629, 28.11.01, c400, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[130] HL Deb Vol 629, 28.11.01, c401, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[131] i.e. subsection 17(2)(d) and 19(2)(e)
[132] HL Deb Vol 629, 28.11.01, c406, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

> The reason that we need the provision is for bringing to an end any investigation of proceedings. It will allow the authorities to clear an individual's name by providing information which shows he is innocent and allows the investigation to be closed. It will also be able to help the police to determine whether an investigation should start by providing information on an individual thought to have left the country or thought to be dead.[133]

The amendment was withdrawn.

Baroness Buscombe moved an amendment which would have required public authorities intending to disclose information under section 17 to carry out a pre-disclosure assessment of the request for information to establish whether there were reasonable grounds for suspecting that the information would be relevant to an investigation into terrorism, or if not, whether the request for disclosure was proportionate to the offence in question.[134] On behalf of the Government, Lord McIntosh of Haringey opposed the amendment on the ground that under the *Human Rights Act 1998* a public authority was already obliged to ensure that any disclosure was proportionate.[135] Again, the amendment was withdrawn.

Lord Thomas of Gresford moved an amendment to remove subsection 19(2)(a), which enables disclosure of information by the Revenue departments "for the purpose of facilitating the carrying out by any of the intelligence services of any of that service's functions".[136] As noted earlier, this power was not present in the otherwise similar provisions contained in the *Criminal Justice and Police Bill*. Lord McIntosh of Haringey defended this power:

> One of the central objectives of the Bill is to assist the Government in combating terrorism. If vital information cannot be passed to the […] intelligence services, that would represent a serious impediment to that effort. I understand the concerns that the noble Lord, Lord Thomas, has in making a comparison with the previous Bill. But I cannot believe, in the specific context of terrorism […] that it would be right to exclude reference to the intelligence services from the provisions of the Bill.[137]

Withdrawing the amendment, Lord Thomas of Gresford indicated that he was not satisfied by this explanation:

> The powers that are being sought are novel and extensive. They mean that the files of all taxpayers in this country will be available for consideration by the

---

[133] Ibid
[134] HL Deb Vol 629, 28.11.01, c407, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[135] Op cit, c410
[136] HL Deb Vol 629, 28.11.01, c419, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[137] HL Deb Vol 629, 28.11.01, cc419-420, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

> security services for any reason whatever. As I have said, the investigation of terrorism need not be involved.[138]

At Report stage, the House of Lords debated a group of amendments narrowing the scope of disclosures under part 3. They would have enabled a public authority to make a voluntary disclosure of information only if it believed or suspected the information to relate directly or indirectly to a risk to national security or to a terrorist. Only a public authority (restricted, broadly speaking, to those regulated by the *Regulation of Investigatory Powers Act 2000*) would have been able to request information under part 3, and then only if it believed or suspected that the information related directly or indirectly to any risk to national security or to a terrorist. On behalf of the Government, Lord Rooker suggested that the group of amendments (which included amendments to other parts of the Bill) could be described as "wrecking amendments".[139] The debate featured the following exchange between Lord Rooker and Lord Thomas of Gresford:

> **Lord Rooker:** I set out a brief response to each of the amendments. Turning to Clause 17, at the time a public authority chooses to disclose to the police, say, an address which they suspect has been used by criminals, it may have no idea that those who live there are part of a terrorist network. It would not know. Its piece of the jigsaw is not connected to the parts held by other authorities. It is only in the course of the investigation that the situation becomes apparent. Under the Bill as drafted, the police would receive information related to suspect criminal acts. The police are the investigators. It is their job to put the various pieces together to see whether they make a picture. Many times they will not, but it is their job to add those pieces to the jigsaw.
>
> **Lord Thomas of Gresford:** My Lords, I have listened on many occasions to this argument from the Minister. He says that we have to have powers to deal with every possible crime because we do not know how it will all fit together and we do not see the picture at the end.
>
> Surely it is possible, as the amendments seek to do, to confine the scope of the inquiry of the investigating authorities, whether the intelligence services or the police, to anti-terrorism. If they act in good faith, as I am sure they do and, for example, say to the public authorities which are required to disclose something, "We are doing this in order to investigate terrorism", that is enough. No one will question it beyond that. However, with great respect, the Minister is instituting a dragnet which covers the whole realm and enables every possible corner of people's lives—their privacy, their tax returns and everything else—to be investigated by the intelligence services. The Minister has failed to answer that argument at each stage of the Bill.
>
> […]

---

[138] Op cit, c420

[139] HL Deb Vol 629, 6.12.01, c959, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

> **Lord Rooker:** My Lords, I accept what the noble Lord, Lord Thomas, says. Clearly, we shall disagree on the issue. He obviously has a different view from the Government on the way the police conduct their investigations. We think that the police should have the power to assemble the pieces of the jigsaw.[140]

The amendments were passed,[141] but were later removed in the Commons.[142] A compromise amendment (subsection 17(5)) to make explicit the duty on public authorities to ensure that disclosure of information is proportionate to that which is intended by disclosing, was then inserted in the Lords.[143]

b. Disclosure to Public Authorities Only

In Committee in the Lords, Lord Phillips of Sudbury moved an amendment designed to explore concerns about the potential recipients of information under part 3:

> The point of the amendment is to confine the right to disclose to all the bodies concerned in accordance with the 66 scheduled pieces of legislation, to other public bodies or, as I have expressed it, to another public authority. As the clause stands, I cannot see any reason for wondering whether or not the disclosure is also to be allowed to an individual who comes within paragraphs (a), (b), (c) or (d) of Clause 17(2); that is, an individual bringing a private prosecution, contemplating bringing a private prosecution or contemplating investigating a private prosecution, as covered in paragraph (d).
>
> There, of course, we enter a very deep and broad sea. One is dealing with the prospect of an individual bringing criminal libel proceedings, which very often are highly personal and acrimonious. One thinks of cases such as that of the late lamented Jimmy Goldsmith against Private Eye. One thinks also of criminal damage prosecutions, of rape or attempted rape prosecutions, of theft or attempted theft prosecutions, perjury prosecutions and a host of others.
>
> […]
>
> Therefore, as I said, the amendment is designed to prevent the clause extending to that whole range of cases. It would also prevent an unfairness in that, if, indeed, private prosecutions were within the scope of this clause, there would be a serious inequality of arms because the defendant in those private prosecutions would not have the same rights of access to disclosed information as the prosecuting individual. On those grounds, I beg to move.[144]

---

[140] HL Deb Vol 629, 6.12.01, cc960-1, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

[141] The amendment of Section 19 was passed on a division, in which 227 Peers voted in favour and 138 voted against. HL Deb Vol 629, 6.12.01, cc975-6, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

[142] HC Deb Vol 376, 12.12.01, c915, http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo011212/debindx/11212-x.htm

[143] HL Deb Vol 629, 13.12.01, cc 1433-4, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

[144] HL Deb Vol 629, 28.11.01, cc365-6, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

For the Government, Lord McIntosh of Haringey confirmed that the provisions would permit disclosure for private prosecutions. As an example, he pointed out that this would have included the private prosecution of those accused of the murder of Stephen Lawrence, prompting the following exchange with the Earl of Onslow.

> **Lord McIntosh of Haringey:** […] Is that so terrible? I am not sure that I agree that it is.
>
> **The Earl of Onslow:** In the context of this Bill, yes, it is terrible. We are dealing with terrorism, terrorism and terrorism. We are not dealing with the murder of Stephen Lawrence; we are not dealing with brothel keeping; and we are not dealing with parking on a double yellow line. We want to confine the Bill to what the Government say it is about. Many of us have made that complaint. Yesterday, I and many other noble Lords around the House made that very complaint. We must confine the Government. No one is saying that they should not have these powers if they want them; but they must get them by proper legislation and proper means. That is the complaint that runs through the whole core of this argument.[145]

Lord McIntosh also observed that the provisions would enable disclosure to a defendant in a private or public prosecution, but that would not be possible if the amendment were carried.

The amendment was withdrawn, but a similar amendment was passed at the Report stage, as part of the group discussed above, following a division.[146] The amendment was removed later in the Commons, however.[147]

c. Duty to Disclose?

During the Lords Committee and Report stages, Peers considered whether part 3 imposed a duty to public authorities to disclose information rather than just giving them power to do so. In Committee, Lord McIntosh of Haringey, for the Government, said:

> There is no question of public officials being obliged to make disclosures. It is up to them to decide whether to do so. There is certainly no question of the police or anyone else trawling records. There will be no investigatory access to the records covered by the Acts in Schedule 4. Public officials will have to determine on a case-by-case basis whether they may disclose the information.[148]

---

[145] HL Deb Vol 629, 28.11.01, c366, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

[146] Amendment passed by 227 votes to 145. HL Deb Vol 629, 6.12.01, c972, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

[147] HC Deb Vol 376, 12.12.01, c915, http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo011212/debindx/11212-x.htm

[148] HL Deb Vol 629, 28.11.01, c367, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

However, Lord Phillips of Sudbury disagreed with the Minister's assertion:

> There is no doubt that a public authority to which a request for disclosure is made under Clause 17 will be unable to refuse it without good reason. That would be a judicially reviewable decision. The Minister is indicating that that is not true, but a public authority to which a request for disclosure was properly made under Clause 17 could not simply refuse to comply. It would be a reviewable decision according to Wednesbury principles and it represents a right on the part of those requesting the disclosure.[149]

Lord McIntosh replied:

> […] That is simply untrue. Nothing is provided either here or anywhere else which forces public officials or public authorities to disclose any information. What is given in this clause is the power to give information. I have already described the safeguards in place. I have already commented on the fact that a large amount of public debate on this issue has been on the basis of serious misconceptions about the provision.[150]

Later, he said:

> I respond only to the single new point that was made; namely, the possibility of a refusal to disclose on request being reviewed. In theory that is the case and it is possible. But how would it succeed? The public authority does not have, and is not given, a duty to disclose. It is only in the unlikely circumstances that it could be said that a public authority was unreasonable—and unreasonable, as the noble Lord, Lord Phillips, said himself in the Wednesbury sense—in refusing to disclose that there could be any question about it. It is a power and not a duty. I am sorry if I am being repetitive, but the public authority will be subject to the Human Rights Act and the Data Protection Act. The Human Rights Act does not require somebody else to pursue the public authority to secure that the human rights provisions are complied with. It is a duty on every public authority to comply with that Act. It would be an offence not to do so.[151]

d. Prior Authorisation

Lord Phillips of Sudbury moved a group of amendments which would have made it necessary to obtain prior judicial authorization before information could be disclosed under section 17:

> Perhaps I may turn briefly to the particular proposal. In relation to subsection (1), it requires a judge to determine the applications made for disclosure. In relation to

---

[149] HL Deb Vol 629, 28.11.01, c414, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[150] HL Deb Vol 629, 28.11.01, c415, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[151] HL Deb Vol 629, 28.11.01, c417, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

> subsection (2), if he makes an order it must specify the information to be disclosed—that is surely helpful to all concerned—and the purpose for which the order is made; namely, whether it is made under sub-paragraphs (a), (b), (c) or (d). The authorisation will make the disclosure subject to such requirements as the judge thinks fit. That is an extremely useful provision. It will allow a judge to make necessary conditions in all the circumstances, one of which may be that the order is brought to the attention of the person whose confidential information is at stake. Then the order must be served on the public authority in respect of which the disclosure request is made. We go on to prescribe evidence on oath. There must be reasonable grounds for believing that the public authority holds the information, that the information is not liable to disclosure by other means, and the whole is to be heard in secret.
>
> Such provision may seem cumbersome, but it provides a clear framework within which all of this could function. It would reduce at a single stroke the widespread public concern over Clause 17 as drafted. On those grounds, I commend the amendment to the Committee. I beg to move.[152]

Opposing the amendment, Lord McIntosh of Haringey argued that judicial control would introduce delays and impede the "free flow of information" that was necessary for the effective co-ordination of agencies:

> It is important that we should realise the practical effect of the amendments. It would be to transform the aim that I have described in this part of the Bill into a form of judicial control over disclosure which might well prevent some of the most important pieces of information being disclosed in time. The noble Earl, Lord Onslow, buries his head in his hands. He has a continuing complaint about our argument that it is not possible always in advance and in time to define what is a terrorist offence because there is no proper definition and, therefore, we have to include criminal investigations and criminal proceedings. But if we are investigating someone who is a potential terrorist, we have to act on the spot; we have to act at the time. The effect of the amendments would be that an authorisation would have to be sought from a judge by the person seeking the information. That information would have to specify what is being sought and it is not always possible to know what is being sought. That procedure would have to take place before the request for information could even be put to the public official who has to decide whether to give the information.
>
> […]
>
> If we have delay of the kind involved in prior judicial control, we will lose the scent; we will lose the information; we will lose the opportunity to deal with potential terrorists. It has to be done immediately. [153]

---

[152] HL Deb Vol 629, 28.11.01, c386-7, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[153] HL Deb Vol 629, 28.11.01, c389-390, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

> I wish that the noble Baroness, Lady Park, was in the Chamber, because this is about intelligence. All that we know about the prevention of terrorism has highlighted the need for the co-ordination of agencies, particularly when there is a clear case for the free flow of information and a need for clear and effective channels. All that is implicit in the Bill. The prior judicial control required by the amendments would put at risk the intelligence work that is essential for that incredibly difficult task.
>
> The provisions will mean that public officials understand their obligations better, especially thanks to the publicity that has been given to the matter in the past few days. That means that they are more likely to respect the safeguards.[154]

These arguments were rejected by Lord Phillips of Sudbury, who compared his proposals with the authorization framework contained in the *Regulation of Investigatory Powers Act 2000* (RIPA):

> It has been made clear in interventions that the law as it stands, and as it has always stood, requires that citizens whose houses are to be searched or whose possessions are to be confiscated should be subject to the protection of a magistrates' warrant or order to allow the police to proceed. That action can be carried out with the greatest rapidity. Applications to a judge under the procedure provided for by the amendment could be done virtually instantaneously. A duty judge would be available at a moment's notice to deal with the matter, which can be done entirely orally. We totally reject the notion that the proposal is defective.[155]
>
> I remind the Minister that the Regulation of Investigatory Powers Act that his Government introduced only last year has all the protections for which we are calling in the amendment. It has an Interception of Communications Commissioner; it requires authorisation for every directed surveillance, it has a warrant for all sorts of interventions; it has appeals by Surveillance Commissioners. All that framework is presently contained in the RIP Act. This is a more potentially important piece of legislation than RIPA.[156]

The amendment was withdrawn.

e. Overseas Disclosures

In Committee in the Lords, Lord Hylton moved an amendment designed to prevent disclosure to an overseas authority under section 17 "unless the law of that country or territory provides, in relation to the use, retention and disclosure of the information in question, equivalent safeguards to those applicable under the law of the part of the United

---

[154] HL Deb Vol 629, 28.11.01, c391, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[155] HL Deb Vol 629, 28.11.01, c394, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[156] Op cit, c395

Kingdom in which the information is held".[157] This mirrors the eighth data protection principle:

> 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.[158]

Supporting the amendment, Lord Phillips of Sudbury said:

> If foreign public authorities are to have the advantages of our legislation, they must provide comparable protections and that must go beyond mere law to practice because, as we know, the manner in which some judicial processes are carried on in other jurisdictions is not such as would give real protection to our citizens and public authorities.[159]

For the Government, Lord McIntosh of Haringey replied that under the Data Protection Act,

> Before making disclosure for the purposes of an investigation where no proceedings are immediately in prospect, the data controller must usually ensure that the country has an adequate system of data protection in place.[160]

The amendment was withdrawn. At the Report stage, Baroness Ludford asked the then Home Office Minister, Lord Rooker, about data protection in respect of criminal justice matters:

> The proposed framework decision on terrorism, which is being discussed today by the Justice and Home Affairs Ministers in Brussels, provides for exchange of information including where there is suspicion of a terrorist offence. What is the data protection regime which applies to that? Under the third pillar the normal EU directive on data protection does not apply. There are ad hoc data protection regimes for different parts of the third pillar. Can the noble Lord explain to me what is the regime for data protection and the exchange of information under the framework decision on terrorism?[161]

---

[157] HL Deb Vol 629, 28.11.01, c418, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

[158] *Data Protection Act 1998* Schedule 1

[159] Deb Vol 629, 28.11.01, c418, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

[160] Ibid

[161] HL Deb Vol 629, 6.12.01, c962, http://www.publications.parliament.uk/pa/ld/ldvol629.htm. Lord Rooker undertook to obtain advice on the matter (c963).

f. Schedule 4

Schedule 4 lists 66 existing, specific powers to disclose information. As explained above, section 17 expands these powers, or "gateways". During the passage of the Bill, various Members and Peers raised specific provisions listed in Schedule 4.

At Report stage in the Commons, the Conservatives' spokesman, Dominic Grieve, referred to the *Health and Safety Act 1974*, section 28(7):

> Thus it will now be possible for the Inland Revenue to share information with any other Government agency. Medical information, including the records of individuals, will be capable of being shared. The Health and Safety at Work, etc. Act 1974, with which I am particularly familiar, contains a specific clause which provides that statements may be obtained from individuals—indeed, they are compelled to provide them. That information, too, may now be shared, even though the 1974 Act specifically provided that it could be made available only for legal proceedings relating to the Act or in circumstances in which the individual consented.[162]

A number of Peers and Members raised concerns about the effect on patient confidentiality of the inclusion of section 24 of the *Health Act 1999*. In Committee in the Lords, Baroness Buscombe, the Conservative frontbencher, read from a briefing produced by the General Medical Council:

> The General Medical Council states:
>
> "We are concerned that this Bill may introduce measures that could require the disclosure of identifiable patient records held by the Commission for Health Improvement and the Audit Commission as part of criminal investigation anywhere in the world".
>
> The GMC continues:
>
> "Currently, we advise doctors that they may disclose information in order to 'assist in the prevention, detection or prosecution of a serious crime', usually a crime which will put someone at risk of death or serious harm (such as terrorism). That is because only serious matters will expose third parties to a risk so serious that it outweighs the patient's privacy interest. Disclosure of medical records in relation to non-serious crimes may seriously undermine the trust that is central to the doctor-patient relationship. The Bill does not appear to place any restrictions, or conditions on disclosure of data and it is possible that a police force could simply require records to be disclosed without any justification. [For example, say] we are looking for people who have had 'X' condition or shown 'Y' symptoms). A criminal investigation in this context is defined by the Bill as 'an

[162] HC Deb Vol 375, 26.11.02, c791, http://www.publications.parliament.uk/pa/cm/cmvol375.htm

> investigation of any criminal conduct, including an investigation of alleged or suspected criminal conduct, and an investigation of whether criminal conduct had taken place'. We are, therefore, keen to establish the possible extent and purpose of disclosure of identifiable patient records under the Bill. The Audit Commission has access to records and does demand patient information for some investigations. CHI also holds copies of patient records and we are seeking to establish their position on this issue."
>
> "The Bill also gives the Treasury, by Statutory Instrument, the ability to add provisions contained in subordinate legislation to the list given in the schedule (4) to the Bill. If there are confidentiality provisions contained in subordinate legislation (and we believe there may be) then it is possible that they might be added in the future".
>
> Perhaps I may also refer very quickly to a transcript of an interview on Radio 4 yesterday, which was included in the "Today" programme, with Beverley Hughes MP. She stated:
>
> "Schedule 4 of the Bill lists all of the pieces of legislation that at the moment regulate that and the only thing Clause 17 is doing is simply making it clear to officials that they can give the specified information earlier on in an investigation and as regards to the NHS the only provisions that are included are the disclosure of the price of medical supplies and information relating to the Audit Commission's financial enquiries into the NHS. There is nothing at all to do with patient records or the doctor/patient relationship whatsoever and as I've said it is an example of the kind of scare mongering we had in relation to parts of the Bill which is very misleading".
>
> The General Medical Council and a fair number of other bodies have been in touch with us in the past 24 to 36 hours on this point. They all say that they cannot agree that the Bill, as currently drafted, reads like that at all.[163]

The Government spokesman, Lord McIntosh of Haringey, replied to concerns about the inclusion of the *Health Act 1999*:

> I turn briefly to the General Medical Council. Under the Health Act 1999 and health legislation there is some information held by the health service which fulfils the qualifications in this legislation. In other words, it is covered by the existing statutory restrictions on disclosure and is information collected under the statutory powers. It is true that under certain circumstances under statutory powers the Audit Commission can demand certain patient records. However, I understand that they are demanded in statistical form rather than that which is identifiable to individual patients. To the very limited extent that health information is collected under statutory powers it is covered by this legislation. It does not cover doctors. Whatever may be the case for other purposes, I give the

[163] HL Deb Vol 629, 28.11.01, cc396-7, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

> assurance that doctors are not public officials for this purpose. The information that they hold on medical records is not covered.
>
> At present individual patient records can be disclosed if they are required for criminal proceedings. The noble Baroness, Lady Buscombe, fairly read out the ruling of the General Medical Council about what can be disclosed for serious crime. She defined that clearly. Terrorism is a serious crime. The GMC's agreement and the ethical standards that it applies to medical staff will be extended from criminal proceedings, which it accepts at the moment, to criminal investigations.
>
> If there is some doubt about the role of the Audit Commission's work we shall look at that between now and later stages of the Bill. Even in the event of medical records in the hands of the Audit Commission becoming subject to one of the statutory restrictions which we are modifying, that does not necessarily mean that disclosure will be permitted. The Data Protection Act, the Human Rights Act and the duty of confidence will apply. If the information in question is confidential then disclosure will be difficult. This is not a question of the police coming and asking for records and trawling for whatever they want to know even if they do not know what they want to know.[164]

At the Report stage in the Lords, Lord Phillips of Sudbury examined the effect of section 17 on section 87 of the *Companies Act 1989*:

> It is instructive briefly to look at the precise effect of Clause 17 in relation to the 66 scheduled statutes, as that has not been done so far. For example, the Companies Act 1989 provides a strict regime of confidentiality, to which Section 87, as mentioned in Schedule 4, will be excepted. However, the exceptions in the Bill as drafted are strictly limited to enabling a relevant authority to discharge a relevant function, for example, the Treasury, if interests of investors or public interests are involved, and the police in respect of information needed in pursuance of European Union obligations. The only other exception in the Companies Act to breach of confidentiality is in respect of relevant proceedings, but not, I emphasise, investigation of those proceedings—I refer to paragraph (a) of Clause 17(2)—let alone for the purposes of initiating such investigations—I refer to paragraph (b)—and certainly not in respect of facilitating a decision as to whether or not to proceed to investigate as a prelude to any criminal proceedings—I refer to paragraph (d).
>
> Furthermore, Section 87 of the Companies Act gives a highly detailed description of what are relevant authorities and relevant functions by which to judge whether or not disclosure falls within the general rule of confidentiality, or rather within exceptions to the general rule of confidentiality.[165]

---

[164] HL Deb Vol 629, 28.11.01, c403, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[165] HL Deb Vol 629, 6.12.01, cc949-950, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

The Duke of Montrose discussed section 24(1) of the *Agriculture Act 1967*:

> My Lords, the measures to which the extended powers will apply are listed in Schedule 4 and include Section 24(1) of the Agriculture Act 1967—which lies behind the agricultural census that is undertaken twice a year and discloses details of all farming businesses. That information is collected for general statistical purposes but details of individual businesses have until now been kept confidential. It is a major worry to me and, I should think, to many other farmers that Clause 17 might permit the disclosure of such information generally. If it does, I shall certainly support my noble friend's amendment.[166]

g. Lords Committee: Other Issues

In Committee in the Lords, Lord Goodhart moved a probing amendment addressing the question of whether part 3 breached "the privilege against self-incrimination which has been held to be part of Article 6 of the European Convention on Human Rights.[167] Replying on behalf of the Government, Lord McIntosh of Haringey observed that disclosure powers already existed in relation to criminal proceedings. However, some of the Acts listed in Schedule 4 already contained provision preventing information obtained through compulsory powers being used as evidence against the person who provided it. Those restrictions would continue to hold good for information disclosable under part 3.[168] Lord Goodhart accepted that "broadly my inquiries have been answered satisfactorily" and withdrew the amendment.

Baroness Buscombe moved an amendment suggested by the Law Society of Scotland requiring consultation with Scottish Ministers over provisions in the Bill affecting a devolved area of competence, Scottish criminal law and procedure. For the Government, Lord McIntosh of Haringey replied that the Bill itself was the subject of a Sewell memorandum (a memorandum by Scottish Ministers seeking the agreement of the Scottish Parliament for Westminster to legislate on a devolved matter). Baroness Buscombe accepted the Minister's reply and withdrew the amendment.[169]

Baroness Buscombe moved another amendment suggested by the Law Society of Scotland, exempting information which is subject to legal privilege from disclosure under section 17. Lord McIntosh of Haringey replied that

> the relevant Acts in Schedule 4 already contain provisions that prevent people being compelled to produce information that is subject to legal professional privilege. Nothing in the Bill will extend those duties or possibilities. It is very unlikely that information that is subject to legal professional privilege will be

---

166 HL Deb Vol 629, 6.12.01, c957, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
167 HL Deb Vol 629, 28.11.01, cc363-4, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
168 Op cit, c364
169 HL Deb Vol 629, 28.11.01, cc411-2, http://www.publications.parliament.uk/pa/ld/ldvol629.htm. The Sewell Memorandum on the Bill is at: http://www.scotland.gov.uk/library3/law/sewel_memo.pdf

> obtained under the provision listed in the schedule. Information subject to legal professional privilege will certainly not be obtained by compulsion under the existing enactments. Only information that is required by statute is covered.[170]

Again, Baroness Buscombe accepted the Minister's reply and withdrew the amendment.

Finally, Peers debated in Committee whether to remove Clause 17 from the Bill. Lord Phillips of Sudbury, moving the Question, said:

> I am also tempted to reflect again on the fact that not a single speaker—beyond the Ministers involved—has defended the clause as it stands.[171]

He concluded:

> All in all, we feel that this clause disfigures an already problematic Bill. It is offensive to our traditions and to the real but limited needs giving rise to it, and indeed to common sense. It is condemned by Liberty, Justice, the Law Society, the Bar Council, the BMA and the General Medical Council. We have all been showered with representations soberly made by sober organisations which fear for the extent of this measure.
>
> Finally, there is no sunset provision in the legislation. If it was truly a measure that related to terrorism, a sunset clause would be added here as it has been added elsewhere in the Bill.
>
> I do not intend to reiterate what I said less than 24 hours ago at Second Reading on the background to this. But we believe strongly—I think I can speak for both Benches on this side of the Chamber—that it should be withdrawn and resubmitted in a fair and sensible form. At this hour of the night I do not intend to press for a vote.[172]

The Conservative spokesman, Baroness Buscombe, supported Lord Phillips' view. However, the Government spokesman, Lord McIntosh of Haringey, returned to the Government's central contention that Clause 17 was "a significant help in combatting terrorism":

> I have set out the safeguards that are in place. I have made it clear that the measure is aimed at terrorism but that it will help with criminal investigations. I recognise that the responses which have been made to Clause 17 are sincerely felt although I believe them to be misconceived. If there is anything we can do between now and Report to remove misconceptions and to narrow the distance between us, we are, of course, willing to try to do that.[173]

---

[170] HL Deb Vol 629, 28.11.01, cc412-3, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[171] HL Deb Vol 629, 28.11.01, c414, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[172] HL Deb Vol 629, 28.11.01, c415, http://www.publications.parliament.uk/pa/ld/ldvol629.htm
[173] HL Deb Vol 629, 28.11.01, c417, http://www.publications.parliament.uk/pa/ld/ldvol629.htm

As noted earlier, amendments significantly limiting the scope of Clause 17 were made at the Report stage, but these were overturned in the Commons.

C. Extra-Parliamentary Opinion

Helen Fenwick, Professor of Law at Durham University, made the following overall assessment of section 17:

> In essence therefore it may be said that in a startling fashion section 17(2) destroys the balance created by a large number of existing carefully considered, and often highly detailed schemes permitting disclosure and preserving confidentiality. Together with section 19 and the associated part 11 […], it provides a new regime allowing the police, the Security Services and other public authorities to obtain a vast range of personal and other information."[174]

Since the part 3 powers were "not confined to use against those involved in serious crime or suspected terrorists or even to those already suspected of criminal offences", there was "no justification for including them in a Bill which was presented to parliament as a response to an emergency"[175]:

> It is clearly unwarranted to use the brief Parliamentary timetable [to which the Bill was subject] for provisions which could have been included in ordinary criminal justice legislation. Moreover, they are not subject to sunset clauses. If they are justified now, after 11 September, although they were not previously, one might have considered that a sunset clause was essential since such wide-ranging powers could hardly have been passed, (at least without amendment in the Commons) had they not been viewed as special powers warranted by the exigencies of the situation. They are now likely to remain on the statute book indefinitely, long after the 'emergency' has subsided.[176]

During the passage of the Bill, 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.

---

[174] *Modern Law* Review, September 2002, Helen Fenwick, "The Anti-Terrorism, Crime and Security Act 2001: A Proportionate Response to 11 September?" p760
[175] Op cit, p758
[176] Ibid

> If powers on these lines are to be included in this Bill, they should be restricted to cases where terrorism is an issue.[177]

Liberty (formerly the National Council for Civil Liberties) 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.
>
> 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.[178]

Liberty has recently published a pamphlet entitled *Terrorism Legislation in the United Kingdom*.[179] It is intended to provide an account of the counter-terrorist powers introduced by the Terrorism Act 2000 and the Anti-terrorism, Crime and Security Act 2001, and to assess the impact of these powers on human rights and civil liberties in the United Kingdom. The pamphlet includes an analysis of part 3 of the 2001 Act, in which Liberty contends:

> The police and security services are now authorised to go through personal information held by public authorities (such as medical records, bank statements, school records, tax returns or inland revenue), even though no crime has been committed or suspected.[180]

Liberty believes that part 3 may lead to breaches of the European Convention on Human Rights:

> It is highly likely that the provisions will give rise to violations of the right to privacy enshrined in Article 8, as the circumstances in which directions can be made are extremely wide and their limits extremely loosely designed. This may mean that it falls foul of the 'prescribed by law' requirement in that it does not

---

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

[178] 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/mparl8.html

[179] October 2002, http://www.liberty-human-rights.org.uk/Anti-TerrorNew.pdf

[180] Op cit, page 26

> respect the principle of legal certainty. The legal and procedural safeguards to counter this vulnerability are insufficient, as are the defined criteria to determine the reasonableness and proportionality of requests. The onus should be on those requesting disclosure to make a sufficiently compelling case in favour of such, rather than on the accused.[181]

During the passage of the Bill, Justice, the independent all party law reform and human rights organisation, submitted a memorandum to the Joint Committee on Human Rights. The memorandum started with a number of general points about the Bill:

> General Principles
>
> JUSTICE accepts, in principle, the justification for special measures to safeguard against terrorist activity. In particular, there may be a need to take certain measures in response to the terrible events of 11 September. However, it is also important that any response should safeguard the rule of law.
>
> Any new measures to safeguard against terrorist activity should also be considered within the framework of the Human Rights Act 1998 (HRA). The HRA, and the European Convention on Human Rights (ECHR) provide a valuable and workable framework under which appropriate and targeted action can be taken in response to the events of 11 September and their aftermath.
>
> Within this human rights framework, the measures in this Bill, which is designed as a response to the post-11 September terrorist threat, must satisfy two key principles:
>
> - They must be necessary and proportionate in the context of the existing powers available, and must, at minimum, incorporate procedural safeguards, to ensure that the powers they allow are not open to abuse; and
>
> - They must be carefully targeted at the exceptional situation that justifies them so as to ensure that the rights of innocent parties are protected to the fullest possible extent.
>
> The need to guard against terrorist action must not, therefore, become the pretext for the erosion of rights in matters unrelated to that threat.
>
> As presently drafted, many elements of this Bill fail to satisfy these principles. JUSTICE has a number of broad concerns with the Bill:
>
> - Many of the measures are not subject to sufficient safeguards.

---

[181] Op cit, page 27

- Many of the measures are not confined to the investigation of terrorist offences, but allow for significant extension of police investigatory powers in relation to even minor criminal offences. Such measures are not warranted in emergency legislation designed to respond to a terrorist threat.

- The majority of powers in this Bill are intended to be permanent and are not subject to a time-limiting sunset clause. This is unacceptable in emergency fast-track legislation. Additional powers beyond those related to the current state of emergency should be closely scrutinised through the usual parliamentary procedures. Given the nature of this legislation, the Bill as a whole should be subject to a sunset clause.

- Several elements of the Bill provide for over-extensive delegated powers, which diminish even further the parliamentary scrutiny that can be given to the significant new measures proposed.

> The measures proposed in this Bill must be seen in the context of the permanent anti-terrorist powers in the Terrorism Act 2000, which came into force only last February. This Act placed permanent anti-terrorist legislation on the statute books for the first time and contained a comprehensive range of powers exercisable on the basis of a very broad definition of terrorism. In addition, the Regulation of Investigatory Powers Act 2000 has created significant statutory powers of surveillance and interception of communications. Any addition to these recent and significant Acts in this present Bill needs to be closely justified by the government.[182]

Justice commented at some length on part 3 of the Bill:

PART 3: DISCLOSURE

Clause 17 of the Bill allows for very extensive disclosure and exchange of information as between public bodies and investigating or prosecuting authorities, both within and outside the UK. Information may be disclosed for the purposes of "any criminal investigation whatever" or any criminal proceedings, and under clause 17(d), for "the purpose of facilitating a determination of whether" an investigation should be initiated. There is a presumption that information will be exchanged, subject to a direction by the Secretary of State to the contrary under clause 18, which may be made only in specified circumstances. Clause 19 makes similar provision for disclosure of information by the Commissioners for Customs and Excise, and the Commissioners of Inland Revenue, and allows for an additional power of disclosure "for the purpose of facilitating the carrying

---

[182] Joint Committee on Human Rights, *Anti-terrorism, Crime and Security Bill: Further Report*, 5.12.01, HL 37/HC 372, paras 1.2-6, http://www.publications.parliament.uk/pa/jt200102/jtselect/jtrights/51/51ap01.htm

out by any of the intelligence services of any of that service's functions." (clause 19(2)(a)).

Disclosure may be made for these purposes by any public authority, under a range of legislation listed in Schedule 4 to the Bill. Under clause 17(3) additional legislation can be added to the list in Schedule 4 by order. Public authority is broadly defined, in the same way as under section 6 of the Human Rights Act, to include quasi-public authorities as well as "pure" public authorities such as government departments and the police.

Disclosure under these powers may interfere with privacy rights under Article 8(1) ECHR. The Court of Human Rights has stressed that the protection of personal data is fundamental to the right to respect for private life. Powers of disclosure such as those extended by Part 3 therefore need to be closely confined, and subject to safeguards, in order to ensure that such interference can be justified under Article 8(2). Under Article 8(2), interference with privacy is permissible only where it is sufficiently prescribed by law, is necessary in a democratic society and proportionate to a legitimate aim.

It will also need to be ensured that disclosure to law enforcement authorities complies with data protection principles. Issues are raised in relation to the data protection principle that data should not be used for a purpose different than that for which it was collected. In particular, it should be ensured that, in accordance with data protection principles, there are appropriate safeguards against abuse in relation to the transfer of information to law enforcement authorities outside the UK, particularly in jurisdictions where data protection laws may not afford adequate protection.

In JUSTICE's view, there must be doubts as to whether the scope of Part 3, as presently drafted, is sufficiently clear or confined to meet the "prescribed by law" standard in Article 8. This requirement reflects the principle of legal certainty, which is fundamental to the Convention as a whole and to its protection of the rule of law. Article 8.2 requires that an individual should be able to ascertain, with a reasonable degree of accuracy, how and in what circumstances a restriction on privacy rights should apply to him or her.

The sweeping powers of disclosure in Part 3, applicable in any criminal investigation, or in order to initiate any criminal investigation, cannot, in JUSTICE's view, be justified as a response to a terrorist threat. JUSTICE therefore proposes that the powers under clauses 17 and 19 be confined to the investigation and prosecution of terrorist offences, and to cases where there are reasonable grounds to suspect that the person on whom information is sought has been involved in the commission of such an offence.

Disclosure under clause 17(2)(d) raises particularly serious privacy concerns, since it would allow information about an individual to be disclosed to investigating authorities abroad at a stage when no investigation against that person has yet begun. Clause 19(2)(a) would also allow for unduly wide powers of disclosure. JUSTICE therefore proposes the deletion of clause 17(2)(d) and clause 19(2)(a).