House of Lords
House of Commons
Joint Committee on Human Rights

Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001

Sixteenth Report of Session 2002-03
House of Lords
House of Commons
Joint Committee on Human Rights

Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001

Sixteenth Report of Session 2002-03

Report, together with formal minutes and appendices

Ordered by The House of Lords to be printed 10 November 2003
Ordered by The House of Commons to be printed 10 November 2003
**JOINT COMMITTEE ON HUMAN RIGHTS**

The Joint Committee on Human Rights is appointed by the House of Lords and the House of Commons to consider matters relating to human rights in the United Kingdom (but excluding consideration of individual cases); proposals for remedial orders, draft remedial orders and remedial orders.

The Joint Committee has a maximum of six Members appointed by each House, of whom the quorum for any formal proceedings is two from each House.

**Current Membership**

<table>
<thead>
<tr>
<th>HOUSE OF LORDS</th>
<th>HOUSE OF COMMONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lord Bowness</td>
<td>Mr David Chidgey MP (Liberal Democrat, Eastleigh)</td>
</tr>
<tr>
<td>Lord Lester of Herne Hill</td>
<td>Jean Corsten MP (Labour, Bristol East) (Chairman)</td>
</tr>
<tr>
<td>Lord Parekh</td>
<td>Mr Kevin McNamara MP (Labour, Kingston upon Hull)</td>
</tr>
<tr>
<td>Baroness Perry of Southwark</td>
<td>Mr Richard Shepherd MP (Conservative, Aldridge-Brownhills)</td>
</tr>
<tr>
<td>Baroness Prashar</td>
<td>Mr Paul Stinchcombe (Labour, Wellingborough)</td>
</tr>
<tr>
<td>Baroness Whitaker</td>
<td>Mr Shaun Woodward MP (Labour, St Helens South)</td>
</tr>
</tbody>
</table>

**Powers**

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

**Publications**

The Reports and evidence of the Joint Committee are published by The Stationery Office by Order of the two Houses. All publications of the Committee (including press notices) are on the internet at www.parliament.uk/commons/selcom/hrhome.htm. A list of Reports of the Committee in the present Parliament is at the back of this volume.

**Current Staff**

The current staff of the Committee are: Paul Evans (Commons Clerk), Thomas Elias (Lords Clerk), Professor David Feldman (Legal Adviser), Róisín Pillay (Committee Specialist), Duma Langton (Committee Assistant) and Pam Morris (Committee Secretary).

**Contacts**

All correspondence should be addressed to The Clerk of the Joint Committee on Human Rights, Committee Office, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general inquiries is: 020 7219 2467; the Committee's e-mail address is jchr@parliament.uk.
# Contents

## Report

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td>5</td>
</tr>
<tr>
<td>Background to the Draft Voluntary Code of Practice</td>
<td>5</td>
</tr>
<tr>
<td>The effect of the Draft Code of Practice</td>
<td>6</td>
</tr>
<tr>
<td><strong>Human rights concerns in relation to the Draft Code</strong></td>
<td>7</td>
</tr>
<tr>
<td>Applicability of the Human Rights Act 1998 to service providers holding communications data</td>
<td>7</td>
</tr>
<tr>
<td>Across-the-board standard retention periods for communications data in various categories: necessity and proportionality</td>
<td>9</td>
</tr>
<tr>
<td>Use of retained data for purposes unrelated to national security</td>
<td>10</td>
</tr>
<tr>
<td>The consultation process</td>
<td>12</td>
</tr>
<tr>
<td>The timetable for parliamentary scrutiny</td>
<td>13</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>14</td>
</tr>
</tbody>
</table>

## Formal Minutes

<table>
<thead>
<tr>
<th>Written evidence</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Letter from the Chair to Rt Hon David Blunkett MP, Secretary of State for the Home Department</td>
<td>16</td>
</tr>
<tr>
<td>2. Letter from Rt Hon David Blunkett MP, Secretary of State for the Home Department, to the Chair</td>
<td>19</td>
</tr>
<tr>
<td>3. Letter from the Chair to David Tredinnick MP, Chairman, Joint Committee on Statutory Instruments</td>
<td>23</td>
</tr>
<tr>
<td>4. Letter from David Tredinnick MP, Chairman of the Joint Committee on Statutory Instruments, to the Chair</td>
<td>25</td>
</tr>
</tbody>
</table>
Summary


When we considered the Anti-terrorism, Crime and Security Bill, in 2001, we indicated that the terms of the proposed Code of Practice on the retention of communications data would require further consideration in respect of ensuring compliance with human rights. This report is the result of that further consideration.

The report outlines the background to and effect of the Draft Code (paragraphs 1 to 6). Bearing in mind that the communications data to which the Draft Code and Draft Order relate are in many respects sensitive and personal (paragraphs 11 and 12), the report considers whether the Draft Code and Draft Order include adequate provisions to ensure that the rights to respect for private life and for correspondence under ECHR Article 8 would be properly protected. We note that the Government takes the view that communications providers will not be public authorities subject to the obligation to act compatibly with Convention Rights under the Human Rights Act 1998. It is therefore particularly important to establish the necessity for and proportionality of standard retention of all communications data (paragraphs 10 to 12). However, we have insufficient information which would enable us to satisfy ourselves that those requirements are met (paragraphs 18 and 19).

While concerned about the accessibility of retained data to investigators inquiring into matters unrelated to national security, we are satisfied on balance that available arrangements are likely to provide adequate safeguards against inappropriate disclosure (paragraphs 20 to 26) and that the consultation arrangements before publication of the Draft Code were sufficient to meet the Secretary of State’s obligations under the 2001 Act (paragraphs 27 and 28).

In view of the very important issues relating to the rights to respect for private life and for correspondence raised by the retention of communications data, and access to them, we consider that more time should have been allowed for Parliament to examine the far reaching provisions of the Draft Code and its relationship to the Regulation of Investigatory Powers Act 2000 (paragraphs 29 and 30).
1 Introduction

Background to the Draft Voluntary Code of Practice

1. Part 11 of the Anti-terrorism, Crime and Security Act 2001 provides for arrangements to be put in place whereby communications service providers retain information about communications sent by their customers for longer than would be required for business purposes. These “communications data” are said to be valuable sources of information for the police and other agencies in combating terrorism. Section 102 of the Act requires the Secretary of State to issue, and allows him to revise from time to time, a code of practice relating to the retention of such data by communications providers. It also allows him to enter into agreements with providers in relation to the retention of communications data. Failure to comply with a Code of Practice or agreement is not to give rise to criminal or civil liability, but the Code or agreement is admissible as evidence in legal proceedings in relation to any question as to whether or not the retention of communications data is justified on the ground that failure to retain the data would be likely to prejudice national security, the prevention or detection of crime or the prosecution of offenders.

2. Before issuing a Code of Practice, the Secretary of State is required by section 103 to consult the Information Commissioner and the communications providers to whom the Code will apply, then to prepare and publish a draft of the Code. Thereafter he must consider any representations made to him about the draft, and may modify the draft in the light of them. After a draft has been laid before and approved by resolution of each House of Parliament, the Secretary of State is to bring the Code into force by statutory instrument.

3. The Secretary of State has now laid before each House a Retention of Communications Data under Part 11: Anti-terrorism, Crime & Security Act 2001 Draft Voluntary Code of Practice (hereafter “the Draft Code”), together with a draft Retention of Communications Data (Code of Practice) Order 2003, and now seeks the approval of each House for them.1

4. When the Anti-terrorism, Crime and Security Bill was before Parliament in November and December 2001, the Joint Committee on Human Rights reported on the human rights implications of Part 11. We took the view that “measures should be put in place to ensure that the Code of Practice and any directions are compatible with the right to respect for private and family life, home and correspondence under Article 8 of the ECHR, and that those measures should be specified, so far as possible, on the face of the legislation”.2 Subsequently, we endorsed the suggestion of the House of Lords Delegated Powers and Regulatory Reform Committee that the Joint Committee should scrutinize any draft Code laid before Parliament under what is now section 103(4) of the Act.3 The Committee is

---

1 The Draft Voluntary Code of Practice on the Retention of Communications Data and the Draft Retention of Communications Data (Code of Practice) Order 2003 were laid before Parliament under the Anti-terrorism, Crime and Security Act 2001 on Thursday 11 September 2003


now undertaking that scrutiny, although we were disappointed that the Home Office did not explicitly seek our views before laying the draft order bringing the Draft Code into effect. The Joint Committee on Statutory Instruments has written to the Home Secretary to ask him not to proceed further until we have reported.4

The effect of the Draft Code of Practice

5. The Draft Code would provide for communications providers to retain communications data for longer than would be required for the communications providers’ ordinary business purposes. Appendix A to the Draft Code sets out the periods for which, in the Secretary of State’s view, it is necessary for communications data to be retained for the purpose of national security. The Draft Code specifies different periods for different classes of data: four days for Web activity logs, six months for SMS, EMS and MMS data, E-mail data and ISP data, and 12 months for personal information about subscribers and telephony data. In addition, there are other types of data in relation to which the period of retention would vary relative to the service provided or the data to which they are related. The essential point is that highly personal data (including data which could be used to identify individuals and track their use of the Internet, and their credit card numbers) would have to be held, without their permission or knowledge, for a standard period of 12 months, and other similarly sensitive data would be held for shorter standard periods.

6. During these periods, retained data could be lawfully obtained by or disclosed to a range of official agencies. While the justification for retention of data under the Draft Code would be a need to retain it for national security purposes, data in the possession of a communications provider would apparently be accessible to agencies for wider purposes: a wide range of agencies have access to such data under the Regulation of Investigatory Powers Act 2000 for the purposes of criminal investigations, and the range of such agencies would be considerably extended by the Draft Regulation of Investigatory Powers (Communications Data) Order 2003 for which the Secretary of State is currently seeking approval by resolution of each House.5 This is a matter to which we return below.

4 Joint Committee on Statutory Instruments, Thirtieth Report, Session 2002-03, HL Paper 177, HC 96-xxx, para 1.8.
5 See Appendix 3
2 Human rights concerns in relation to the Draft Code

7. When we first examined the Draft Code, it seemed to us to give rise to four matters of concern on human rights grounds.

a) The nature of the communications data affected by the Draft Code is sufficiently personal and sensitive to give rise to obligations on the part of the state under Article 8 of the European Convention on Human Rights (ECHR) in relation to the retention and storage of personal data as well as its processing and disclosure. The communications providers which retain the communications data are nearly always likely to be private businesses rather than public officials. If they are not “public authorities” for the purposes of the Human Rights Act 1998, they are not directly subject to the legal obligation imposed by section 6 of that Act to act compatibly with Convention rights. It is therefore unclear how the Draft Code would ensure that the state can discharge its obligations under ECHR Article 8 in relation to the retention and storage of the data.

b) It is not clear how the Draft Code’s standard periods of retention would meet the requirement of proportionality which forms part of the test of necessity in a democratic society when justifying an interference with rights under ECHR Article 8.

c) The availability of the communications data to agencies for purposes other than the protection of national security would call in question the legitimacy of the aim for which the data are to be retained, the necessity for that retention and its proportionality, all of which are elements of the justification for retention of personal data under ECHR Article 8.

d) It is not clear how thoroughly the consultation exercise required by section 103 of the Anti-terrorism, Crime and Security Act 2001 was carried out and how far the fruits of it have been taken into account in the Draft Code.

8. Our Chair wrote to the Home Secretary on 30 October 2003 asking a number of questions about these matters. The Home Secretary replied in a letter of 7 November 2003. We are grateful to the Home Secretary and his staff for replying so promptly. Both letters are appended to this Report. We have considered the Home Secretary’s response, and now report our considered views in the light of it.

Applicability of the Human Rights Act 1998 to service providers holding communications data

9. Paragraph 5 of the Draft Code says that it has been drawn up in accordance with various pieces of legislation, including the Human Rights Act 1998. The 1998 Act makes the
Convention rights, including the particularly relevant right under ECHR Article 8, part of the law in the United Kingdom. The Draft Code offers no guidance to service providers as to their responsibilities under the Act.

10. Generally, the obligations under the Human Rights Act 1998 are imposed only on “public authorities”. These are of two relevant kinds: “all-purpose” public authorities which exercise state authority, such as government departments and the police; and “functional” or “limited purpose” public authorities, which are public authorities to the extent that they exercise public functions but are otherwise private bodies. Communications providers are not likely to be all-purpose public authorities. If they were under a legal obligation to comply with Article 8, it would normally be because they are functional public authorities under section 6(3)(b) of the Human Rights Act 1998 (“any person certain of whose functions are functions of a public nature”) when holding data for an extended period for non-business purposes in order to comply with a requirement made under Part 11 of the Anti-terrorism, Crime and Security Act 2001.

11. We considered it to be important to clarify the obligations of communications providers in relation to ECHR Article 8 in order to ensure that the obligation of the state to secure the rights under the Convention to everyone within its jurisdiction, under ECHR Article 1, can be fulfilled. We therefore asked the Government whether it considered that service providers holding information for the purposes of the Anti-terrorism, Crime and Security Act 2001 were to be regarded as functional public authorities for the purposes of the Human Rights Act 1998. The Home Secretary told us that the Government takes the view that the retention of communications data by communications providers is “a private function that arises out of the commercial service that the communication services providers provide”. This has the disadvantage that the communications providers are not public authorities for that purpose and are not bound by the obligation to act compatibly with Convention rights under section 6 of the Human Rights Act 1998.

12. The right to respect for private life under ECHR Article 8 is of fundamental importance. Any invasion of the right must be strongly justified. Safeguards are essential. Making those who retain communications data subject to the Human Rights Act might be one such safeguard. Unless the primary legislation is amended to provide expressly that the providers are, or are not, public authorities for that purpose, only the courts can answer the question authoritatively. We note, however, that if the Government’s view is correct it increases the importance of ensuring that the provisions of the Code, under which the communications providers will work, are fully compatible with Convention rights, particularly ECHR Article 8. Indeed, this is recognized by the Government. The Government draws a distinction between “retention” of data (which in Part 11 of the Anti-terrorism, Crime and Security Act 2001 means the standard retention of all communications data relating to any person) and “data preservation”, by which the Home Secretary means retention of specified data relating to particular cases on a case by case basis at the express request of an agency. The Home Secretary says in his letter, in answer to question 2, … we fully accept that the approach to retention of communications data taken in the Code of Practice needs to comply with Article 8 of the European Convention on Human Rights. It must be necessary and proportionate for the Government to ask that the different types of data are retained for the periods set out in the Code. As a
starting point the Government needs to demonstrate why there needs to be blanket 
data retention at all, rather than data preservation.

In the second paragraph of his letter, the Home Secretary states that, in the Government’s 
view, retention of communications data is both necessary and proportionate in the light of 
advice received from the security and intelligence services and from the police.

**Across-the-board standard retention periods for communications 
data in various categories: necessity and proportionality**

13. Paragraphs 7 and 8 of the Draft Code state that the Secretary of State considers it to be 
necessary for the purpose of national security for service providers to retain 
communications data for the periods set out in Appendix A to the Draft Code. Paragraph 8 
explains that the Secretary of State would, if necessary, issue a certificate under section 
28(2) of the Data Protection Act 1998 to exempt such data from the fifth data protection 
principle (data not to be kept for longer than necessary for the purposes of processing).

14. This would not deal with the position under ECHR Article 8 and the Human Rights 
Act 1998. If a service provider is a functional public authority when retaining data for 
national security purposes, it would have to show both that the retention is necessary (in 
the sense of being a response to a pressing social need) and proportionate (interfering no 
more than is essential in the circumstances of the case with the right to respect for private 
life and correspondence). A retention which fails to meet those criteria will not be 
justifiable under ECHR Article 8.2.

15. We therefore asked the Government why it considers that it would be proportionate to 
retain communications data by reference to across-the-board standard periods of time, 
without reference to the identity of the user of the service or the circumstances in which 
the communications took place.

16. Whether or not the service provider is a functional public authority, the state seems to 
us to have an obligation under ECHR Article 1 and Article 8 to take positive steps to 
safeguard the service user’s right to respect for private life and correspondence. These 
include, as the Government accepts, ensuring that the blanket retention of 
communications data is necessary for a legitimate purpose, and that it is proportionate to 
the aim which it seeks to achieve. In the context of communications data, appropriate 
safeguards might also include legislation imposing on the service providers an obligation to 
ensure that an assessment of proportionality is made in relation to different pieces of data. 
However, neither the Regulation of Investigatory Powers Act 2000, the Anti-terrorism, 
Crime and Security Act 2001 nor the Draft Code indicates that there is a requirement of 
proportionality, let alone offers advice on how it should be applied.

17. We therefore asked the Government whether, and if so why, it considers that a Code 
which does not mention the requirement of proportionality would discharge the United 
Kingdom’s obligations under ECHR Article 8.

18. The Home Secretary replied that it is not correct to assume that the communications 
providers will be making an assessment of proportionality on a case-by-case basis, so 
guidance as to how that should be done is unnecessary. Furthermore, the Government
10
does not consider data preservation on a case-by-case basis to be an adequate tool for fighting terrorism and safeguarding national security, because “data preservation will never aid investigation of a person who is not currently suspected of involvement with, say, a terrorist organization”. It is said to be necessary to keep all communications data because of the need to be able to check the communications record of a person who comes newly under suspicion after the communications in question have been made, in order to find out whether he or she has been in communication with other people who are known to represent a threat to national security or a threat of terrorism. In this way a “pattern of association” can be identified. The Home Secretary also says that Parliament recognized the need for data retention when it passed Part 11 of the Anti-terrorism, Crime and Security Act 2001.

19. We agree that Parliament accepted that there may be a need for data retention for those purposes, although we note that the relevant provisions were not debated by the Commons either at Committee or Report stage due to the effects of the programme order applied to the Bill. However, we have not been able to establish how pressing the need is, or how often the police and security and intelligence services find it necessary to make use of such data or are significantly hampered by its absence. Those matters seem to us to be relevant to the assessment, to be made by each House, of the necessity for the retention which would be sought by the Draft Code, and of the proportionality of the periods set for retention of each kind of communications data. **We draw these matters to the attention of each House.**

**Use of retained data for purposes unrelated to national security**

20. Although the Draft Code sets extended periods of retention for communications on the ground of national security, it says nothing about the use which could be made of data retained under it which could not otherwise have been lawfully retained for that period. Indeed, paragraph 25 of the Draft Code expressly disclaims any intention to do so. As the Draft Code stands, it appears that communications data retained for an extended period under the Anti-terrorism, Crime and Security Act 2001 could be obtained by or disclosed to public authorities for a variety of other purposes, including but not limited to the investigation of crimes unrelated to national security under the Regulation of Investigatory Powers Act 2000. As noted above, a Draft Order in Council, the Draft Regulation of Investigatory Powers (Communications Data) Order 2003, has been laid before each House. This Draft Order would greatly extend the range of bodies by whom communications data can be obtained and to whom they can be disclosed lawfully under the 2000 Act.

21. When we initially examined the Draft Code we were concerned that this might give rise to an unacceptable way by which a very wide range of investigators (including, if the Draft Order is approved, ambulance services) could avoid the restrictions placed by Parliament on the obtaining or disclosure of such data in cases unrelated to national security when the Regulation of Investigatory Powers Act 2000 was passed. If arrangements permit communications data retained under the Anti-terrorism, Crime and Security Act 2001 to be obtained, disclosed or processed for the purposes of other legislation, when the data could not lawfully have been retained under that legislation, there must be doubt about the
legitimacy of the aim for which they are being obtained, disclosed or processed, and the necessity for and proportionality of the obtaining, disclosure or processing of the data.7

22. We therefore asked the Government what legal or technological measures are being taken or are planned to ensure that the communications data retained for the purposes of Part 11 of the Anti-terrorism, Crime and Security Act 2001 will not be available for purposes other than the protection of national security, in order to ensure the proportionality and so the compatibility of the retention with rights under ECHR Article 8.

23. The Home Secretary replied that the Government does not intend to take any legal or technological measures to restrict the use of retained data to national security purposes. The Government’s view is that, if data are available, they should as a matter of policy be accessible at the request of other public authorities for other purposes. The Government gives the example of a murder investigation as a purpose for which data should be accessible. Furthermore, the Government does not accept that the Anti-terrorism, Crime and Security Act 2001, the Human Rights Act 1998 or the ECHR imposes any restriction on the use of retained data for purposes other than protecting national security. The Home Secretary points out that the Government’s view was made clear during debate on the Anti-terrorism, Crime and Security Bill in the House of Lords, and that an amendment which would have limited accessibility of the data under the Regulation of Investigatory Powers Act 2000 was withdrawn. In the light of that, he suggests, it is “very clear that when the 2001 Act was passed Parliament did not intend access to be restricted in that way.” A similar view was expressed by the Parliamentary Under-Secretary of State for the Home Department (Caroline Flint MP) during debate on the Draft Regulation of Investigatory Powers (Communications Data) Order in the House of Commons Third Standing Committee on Delegated Legislation.8

24. We recognize that there may be cases not involving national security in which it is both necessary and proportionate to have access to retained communications data if they are available and relevant. The investigation of a murder might be such a case. On the other hand, we do not consider that the relationship between the powers under the two Acts is as straightforward as the Government suggests. The 2000 Act authorised designated persons to issue authorisations permitting, or notices requiring, communications data to be obtained by investigators for purposes listed in section 22(2) if the designated person decided in each case, on a case-by-case basis, that he or she ‘believes it is necessary’ for one of the listed purposes and also ‘believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data’: section 22(1) and (5). The interests of national security are among the purposes for which an authorisation or notice may be given, but there are many others. The 2001 Act requires the Secretary of State to issue a Code of Practice, and allows him to enter into agreements, containing—

… any such provision as appears to the Secretary of State to be necessary—

(a) for the purpose of safeguarding national security; or

---

7 See Appendix 3
8 HC Deb, Third Standing Committee on Delegated Legislation, 4 Nov. 2003, cc 26-27
(b) for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security.9

It is not clear to us that Parliament, in enacting Chapter 11 of the 2001 Act, intended to affect the balance between rights, safeguards and the public interest in relation to access to communications data in cases which are unrelated to national security.

25. It seems to us that the main safeguard against abuse of the power to access for non-national-security purposes communications data retained under the 2001 is the fact that any access will have to be authorised or required by a designated person in a public authority empowered to access such data by the 2000 Act. The designated person will be a public authority, bound by the Human Rights Act 1998 and the Convention rights, and also bound to refuse a notice or authorisation unless he or she believes that the requirements of necessity and proportionality are met on the facts of each particular case, under section 22(1) and (5) of the 2000 Act. On balance, we are prepared to accept the Government’s view that, as a matter of policy, it should be possible to have access to any communications data which are available and are relevant to a case if those conditions are satisfied on the facts of the particular case. We have come to the conclusion that the safeguards already mentioned, coupled with the availability of judicial review of a notice or authorisation under the 2000 Act and the need to comply with the Data Protection Principles under the Data Protection Act 1998 so far as they apply to such data, are capable in principle of providing appropriate protection for the right to respect for private life and correspondence under ECHR Article 8. We draw this matter to the attention of each House.

The consultation process

26. Before publishing a Draft Code, section 103(2) of the Anti-terrorism, Crime and Security Act requires the Secretary of State to consult with (a) the Information Commissioner and (b) the communications providers to whom the code will apply. The process of consultation could have begun as early as December 2001 or January 2002, but it was not clear to us how thorough the consultation has been, when it was commenced, or how long was allowed for it. We note that the consultation process is an essential part of the scheme of Part 11 of the Anti-terrorism, Crime and Security Act to ensure that the Code of Practice made under section 102 puts in place a properly limited scheme for retention of communications data which respects the requirements of the Human Rights Act 1998 and the ECHR as well as the Data Protection Act 1998 and related legislation. We are mindful of the fact that the Court of Appeal (Civil Division) has recently reaffirmed the importance of proper compliance with legal consultation requirements in the process of policy-making.10

27. We therefore asked the Government what views the Information Commissioner expressed when consulted on the Draft Code, what steps were taken to consult with the communications service providers, when and over what period these consultations took

---

9 Section 102(2), italics added
place, and what views the communications service providers expressed. In his reply, the Home Secretary referred to various fora in which representatives of the industry had an opportunity to express views about proposals for the Draft Code. There was a Technical Working Group, meeting monthly for several months until March 2003 to discuss technical matters relating to the Draft Code. A six-monthly Government Industry Forum gave an opportunity for the industry to speak to Government, as did an Operators Group and meetings with the Internet Service Providers Association. The Government also visited smaller providers to explain its objectives and to assess the impact of the proposals on them. Industry was then encouraged to participate in the public consultation which took place in the three months from 11 March 2003. During these processes, the Government sought to allay concerns of the providers about the legality of the proposals in the light of the ECHR.

28. We are satisfied that these steps were sufficient to comply with the Secretary of State’s duty under section 103(2) of the 2001 Act to consult the communications providers to whom the Draft Code will apply.

The timetable for parliamentary scrutiny

29. We asked the Home Secretary whether it was necessary to press ahead with the Draft Order and Draft Code of Practice now, and, if they could not be deferred for further consideration in Parliament, what the reasons for the urgency are, bearing in mind that the Government has laid a Draft Retention of Communications Data (Extension of Initial Period) Order 2003 which, if approved, would extend for two years from 13 December 2003 the power of the Secretary of State to give directions for the retention of communications data under section 104 of the 2001 Act. The Home Secretary responded that the draft Orders and Draft Code are high priorities in view of the terrorist threat, which makes it “critically important to put these measures in place as soon as possible, in order to provide investigators with the necessary tools to fight terrorism and safeguard national security”. The Home Secretary said that technical changes in the industry mean that providers need to keep communications data for less and less time for business purposes, so there is a danger that important data will cease to be available if the Draft Code is not quickly put in place. The Home Secretary also noted that the extension of powers under section 104 of the 2001 Act must be approved by both Houses before 13 December, and that the Draft Code and its associated Draft Order were laid before Parliament on 11 September 2003, in his view giving plenty of time for consideration by Parliament.

30. We note that the two Houses were sitting on 11 September, but rose for the conference recess on 19 September, to reassemble on 14 October. The total sitting period allowed for consideration of these proposals thus amounts to about five weeks. In our view, this is not sufficient in view of the importance of the measures, their potential to affect human rights, and the long period of gestation of the proposals since December 2001. We draw this matter to the attention of each House.
3 Conclusion

31. We are very concerned that the communications providers who will be retaining communications data under the provisions of Part 11 of the Anti-terrorism, Crime and Security Act, often for long periods, as a matter of course will not (if the Government’s view is correct) be functional public authorities for the purposes of the Human Rights Act 1998, and so will not be subject to any of obligations arising under ECHR Article 8. In our view, this makes it particularly important to ensure that the Draft Code, and the standard periods of retention which it contains, are necessary for a legitimate aim and are proportionate to the objective sought to be achieved. The Home Secretary has convinced us that making communications data accessible is likely to be a useful investigative tool, but we are not able to say that we are satisfied that the arrangements in the Draft Code would be proportionate to legitimate objectives (see paragraphs 11 to 12 and 18 to 19 above).

32. We also have some reservations about the Government’s approach to the possible accessibility of retained data to investigators inquiring into matters unrelated to national security. However, on balance we are satisfied that other safeguards, within the structure of the Regulation of Investigatory Powers Act 2000 and the procedures for judicial review, are likely to provide adequate safeguards for Convention rights (see paragraphs 24 to 26 above).

33. Finally, we regret that more time has not been allowed to permit Parliament to consider more fully these far-reaching proposals, and their relationship to the other Draft Orders currently before the two Houses in relation to powers under the Regulation of Investigatory Powers Act 2000 (see paragraphs 29 to 30 above).
Formal Minutes

Monday 10 November 2003

Members Present:

Jean Corston MP, in the Chair

Lord Bowness                        Mr David Chidgey MP
Baroness Perry of Southwark         Mr Kevin McNamara MP
Baroness Prashar                    Mr Richard Shepherd MP
Baroness Whitaker

The Committee deliberated.

Draft Report [Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001], proposed by the Chairman, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 33 read and agreed to.

Resolved, That the Report be the Sixteenth Report of the Committee to each House.

Summary agreed to.

Ordered, That certain papers be appended to the Report.

Ordered, That the Chairman do make the Report to the House of Commons and that Baroness Prashar do make the Report to the House of Lords.

[Adjourned till Monday 17 November at half past Four o’clock.]
1. Letter from the Chair to Rt Hon David Blunkett MP, Secretary of State for the Home Department

The Joint Committee on Human Rights is considering whether to report to each House on the human rights implications of the above Draft Code, laid before Parliament pursuant to section 103(4) of the Anti-terrorism, Crime and Security Act 2001. When the Committee reported on the Anti-terrorism, Crime and Security Bill in 2001, it endorsed the suggestion of the House of Lords Delegated Powers and Regulatory Reform Committee that the Joint Committee should scrutinize any draft Code laid before Parliament under what is now section 103(4) of the Act. The Committee was disappointed that the Home Office did not explicitly seek its views, preferably before the laying of the order bringing the Code into effect.

The Committee would therefore be grateful for your response to the following questions.

**Applicability of the Human Rights Act 1998 to service providers holding communications data**

The Draft Code, paragraph 5, says that it has been drawn up in accordance with legislation, including the Human Rights Act 1998. That appears to be the only reference to that Act. Of the Convention rights, ECHR Article 8 (right to respect for private life and correspondence, among other things) is particularly relevant. No guidance is given to service providers as to their responsibilities under the Act. Service providers are not likely to be public authorities for all purposes. If they are under a legal obligation to comply with Article 8, it will normally be because they are ‘functional’ public authorities under section 6(3)(b) of the Human Rights Act 1998 (‘any person certain of whose functions are functions of a public nature’) when holding data for an extended period for non-business purposes in order to comply with a requirement made under Part 11 of the Anti-terrorism, Crime and Security Act 2001.

1. Does the Government consider that service providers holding information for the purposes of the Anti-terrorism, Crime and Security Act 2001 are to be regarded as functional public authorities for the purposes of the Human Rights Act 1998?

**Across-the-board standard retention periods for communications data in various categories: necessity and proportionality**

Paragraphs 7 and 8 state that the Secretary of State considers it to be necessary for the purpose of national security for service providers to retain communications data for the periods set out in Appendix A to the Draft Code. Paragraph 8 explains that the Secretary of State would, if necessary, issue a certificate under section 28(2) of the Data Protection Act 1998 to exempt such data from the fifth data protection principle (data not to be kept for longer than necessary for the purposes of processing).

This would not deal with the position under ECHR Article 8 and the Human Rights Act 1998. If a service provider is a functional public authority when retaining data for national security purposes, it would have to show both that the retention is necessary (in the sense of being a response to a pressing social need) and proportionate (interfering no more than is essential in the circumstances of the case with the right to respect for private life and
correspondence). A retention which fails to meet those criteria will not be justifiable under ECHR Article 8.2.

2. If the Government takes the view that service providers will be functional public authorities for this purpose, why does it consider that it would be proportionate to retain communications data by reference to across-the-board standard periods of time, without reference to the identity of the user of the service or the circumstances in which the communications took place?

Whether or not the service provider is a functional public authority, the state might have an obligation under ECHR Article 1 and Article 8 to take positive steps to safeguard the service user’s right to respect for private life and correspondence. In this context, appropriate safeguards might, for example, take the form of legislation imposing on the service providers an obligation to ensure that an assessment of proportionality is made in relation to different pieces of data. However, neither the Anti-terrorism, Crime and Security Act 2001 nor the Draft Code indicates that there is a requirement of proportionality, let alone offers advice on how it should be applied.

3. Why does the Government consider that a Code which does not mention the requirement of proportionality would discharge the United Kingdom’s obligations under ECHR Article 8?

Use of retained data for purposes unrelated to national security

Although the Draft Code sets extended periods of retention for communications on the ground of national security, it says nothing about the use which could be made of data retained under it which could not otherwise have been lawfully retained for that period: see paragraph 25 of the Draft Code. As it stands, it appears that communications data retained for an extended period under the Anti-terrorism, Crime and Security Act 2001 could be obtained by or disclosed to public authorities for a variety of other purposes, including but not limited to the investigation of crimes unrelated to national security under the Regulation of Investigatory Powers Act 2000. The Committee notes that a Draft Order in Council, the Draft Regulation of Investigatory Powers (Communications Data) Order 2003, has been laid before each House. This Draft Order would greatly extend the range of bodies by whom communications data can be obtained and to whom they can be disclosed lawfully under the 2000 Act.

This could be seen as an unacceptable way of avoiding the restrictions placed by Parliament on the obtaining or disclosure of such data in cases unrelated to national security when the 2000 Act was passed. That Act represents a careful assessment of the appropriate balance between individuals’ rights and public interests for the purpose of ECHR Article 8.2. If arrangements permit communications data retained under the Anti-terrorism, Crime and Security Act 2001 to be obtained, disclosed or processed for the purposes of other legislation, when the data could not lawfully have been retained under that legislation, there must be doubt about the proportionality of that obtaining, disclosure or processing of the data.

4. What legal or technological measures are being taken or are planned to ensure that the communications data retained for the purposes of Part 11 of the Anti-terrorism, Crime and Security Act 2001 will not be available for purposes other than the protection of national security, in order to ensure the proportionality and so the compatibility of the retention with rights under ECHR Article 8?
The consultation process

Before publishing a Draft Code, section 103(2) requires the Secretary of State to consult with (a) the Information Commissioner and (b) the communications providers to whom the code will apply. The process of consultation could have begun as early as December 2001 or January 2002, but it is not clear to the Committee how thorough the consultation has been, when it was commenced, or how long was allowed for it.

5. What views did the Information Commissioner express when consulted on the Draft Code?

6. What steps were taken to consult with the communications service providers; when and over what period did these consultations take place; and what views did the communications service providers express?

The timetable for seeking approval

The Committee notes that the Government has laid before Parliament a draft Order, the Retention of Communications Data (Extension of Initial Period) Order 2003, which would extend for two years from 13 December 2003 the power of the Secretary of State to give directions for retention of communications data under section 104 of the Anti-terrorism, Crime and Security Act 2001. If this is approved, it would seem to remove much of the urgency from the process of obtaining approval of the Draft Code of Practice. The Committee has commented above on the impact on the Convention right under ECHR Article 8 of the inter-relationship between retention under the 2001 Act and retention under the Regulation of Investigatory Powers Act 2000, and of the proposed extension to the range of bodies entitled to obtain or receive disclosure of communications data under the latter Act in the Draft Regulation of Investigatory Powers (Communications Data) Order 2003, for which approval is due to be sought from Parliament in the near future.

7. Does the Government consider that it is necessary to press ahead with these Draft Orders and Draft Code of Practice at this time, and if so, why?

8. Are there any pressing considerations which would weigh against allowing the issues relating to these proposed items of legislation be dealt with according to a timetable which allowed more time for parliamentary scrutiny and further consultation?

If the Government still intends to seek approval of the Draft Regulation of Investigatory Powers (Communications Data) Order 2003 and related draft orders in the immediate future, I would be grateful for a reply to this letter not later than midday on Friday 7 November 2003 so that your reply can be considered by the Committee and a report provided to each House, if necessary, before 12 November.

If on the other hand the Government is willing to withdraw that Order for the time being, or to postpone parliamentary debate upon it, to allow time for further consideration of its implications alongside those of the Draft Code, a reply by Monday 17 November 2003 would be sufficient.

30 October 2003
2. Letter from Rt Hon David Blunkett MP, Secretary of State for the Home Department, to the Chair

Thank you for your letter of 30 October about the draft Code of Practice we have laid before Parliament under section 103(4) of the Anti-terrorism, Crime and Security Act 2001 (the 2001 Act). I am reluctant to delay consideration by both Houses and I hope that you will find the details in this letter helpful in expediting your scrutiny of our proposals.

I entirely accept that the blanket retention of communications data and its access by public authorities constitutes a potential interference with the right to respect for private life enshrined in Article 8 of the European Convention of Human Rights. The issue is whether it is necessary and proportionate for data to be retained for the periods set out in the Appendix to the Code. The Government’s view, in light of the advice it has received from the security, intelligence and law enforcement agencies, is that it is. But clearly this is an important step and that is why we have consulted extensively on the draft Code (I attach the consultation document published in March) before bringing it forward for Parliamentary consideration. I hope that the information I am providing for the Committee is a useful way of adding to that consideration. Let me deal with each of your questions in turn.

Q. 1 Does the Government consider that service providers holding information for the purposes of the Anti-terrorism, Crime and Security Act 2001 are to be regarded as functional public authorities for the purposes of the Human Rights Act 1998?

The Government does not consider that communication service providers who retain data in accordance with the voluntary Code of Practice should be regarded as functional public authorities for the purposes of the Human Rights Act 1998. The purpose of section 6(3)(b) is to deal with hybrid bodies that have both public and private functions. The Government’s view is that the communication service providers are not such a body and that the retention of communications data is not a public function, whether it is done for the communication service providers’ own business purposes or under the Code of Practice. Rather, it is a private function that arises out of the commercial service that the communication service providers provide.

Q. 2 If the Government takes the view that service providers will be functional public authorities for this purpose, why does it consider that it will be proportionate to retain communications data by reference to across the board standard periods of time, without reference to the identity of the user of the service or the circumstances in which the communications took place?

As I have indicated, the Government does not consider that communications service providers will be functional public authorities for this purpose. Nevertheless, we fully accept that the approach to retention of communications data taken in the Code of Practice needs to comply with Article 8 of the European Convention on Human Rights. It must be necessary and proportionate for the Government to ask that the different types of data are retained for the periods set out in the Code. As a starting point the Government needs to demonstrate why there needs to be blanket data retention at all, rather than data preservation. This is the issue the Committee identify in this question.

In this regard “data preservation” means the retention by communication service providers of specific data at the request of agencies on a case by case basis as such data is created. By way of contrast the Code covers “data retention” by which is meant routinely keeping an identified set of data for a specific period in the event of a subsequent need for access. The Government does not consider that data preservation is an adequate tool for fighting
terrorism and in safeguarding national security. This is because data preservation will never aid investigation of a person who is not currently suspected of involvement with, say, a terrorist organisation. For example, if a bomb warning is given prior to a terrorist attack by someone whose data is being preserved then investigators can use communications data to trace the originator of the call and later establish a profile of that individual and identify their contacts and whereabouts in the period prior to the bomb warning. However, if the call is made from a previously unknown source, there will have been no reason to preserve data associated with that particular subscriber. A sophisticated terrorist would be likely to have taken steps to minimize his traceability, consequently it may take some time to identify him. By this time the communication service provider may have erased the data relating to both the suspect’s communications and those of his co-conspirators. It is the ability to use historical communications data to build up a pattern of association that can be crucial to an investigation of a terrorist attack. It is for this reason agencies responsible for national security believe that data preservation can be used to supplement data retention but not to replace it. Furthermore, it was the need for data retention rather than data preservation that was recognised by Parliament when it passed the Part 11 of the 2001 Act.

Q. 3 Why does the Government consider that a code which does not mention the requirement of the proportionality would discharge the United Kingdom obligations under ECHR of Article 8?

I am not sure that the Committee is correct in appearing to assume that it will be communication service providers who will be deciding whether the retention periods set out in the Code are necessary and proportionate. The purpose of the Code is to set out the periods for which the Secretary of State himself considers it necessary and proportionate to retain different types of communications data for the purposes of safeguarding national security and for the purposes of the prevention and detection of crime or the prosecution of offenders which may relate directly or indirectly to national security. The purpose of the Code being approved by way of affirmative resolution is to allow Parliament, if it chooses, to endorse this view. But communication service providers do not need to reach a view on this. Rather, in deciding whether to retain data under the voluntary Code they are entitled to rely on the fact that the Secretary of State and Parliament will have concluded that the retention periods set out in the Code are necessary in order to safeguard national security.

In reaching his decision on the appropriate retention periods the Secretary of State has taken into account a number of factors. These include the potential infringement of the right to privacy under Article 8 of the European Convention on Human Rights that retention and access communications data might entail and the fact that communications data are an essential tool for the security, intelligence and law enforcement agencies in carrying out their work to safeguard UK national security. As is expressly set out in paragraph 11 of the Code, having considered all these matters the Secretary of State has concluded that the retention periods set out in the Code are both necessary and proportionate.

Q. 4 What legal or technological measures are being taken or are planned to ensure that the communications data retained for the purposes of Part 11 of the Anti-terrorism, Crime and Security Act 2001 will not be available for the purposes other than protection of national security in order to ensure the proportionality and so the compatibility of the retention with rights under ECHR Article 8?

The disparity between the purpose for which data is retained under the Code and the purposes for which data can be accessed from communications service providers under the
Regulation of Investigatory Powers Act 2000 (the 2000 Act) was raised with the Home Office during consultation on the Code. It is addressed in the consultation paper. The Government do not consider that the fact that data is held by communications service providers under the Code of Practice for national security purposes should in itself prevent the police or other public authorities having access to that data for another purpose. It is considered that this would be wrong as a matter of policy and that legally no such automatic restriction exists.

Legally, the Government does not consider that the 2001 Act itself, the Human Rights Act or the European Convention on Human Rights places any blanket restriction on the purposes for which data held under the Code can be accessed. First, there is no explicit restriction in section 102 of the 2001 Act. Further, it was not the intention of Parliament at the time to impose such a restriction. Rather, when this question was raised in the House of Lords Lord Rooker made it explicitly clear that restricting the purposes in what became section 102 would not restrict access via the 2000 Act to data retained under the Code (see Hansard 4 December 2001 page 773-777). This was recognised by the Opposition in the Lords who laid an amendment to the 2000 Act designed to expressly prevent access for non national security purposes. However, that amendment was not pressed, so no restriction was placed in either the 2001 Act or the 2000 Act on the purposes for which data retained under the Code could be accessed. In light of this and, considering the wording of section 102, the Government does not consider that section 102 imposes any implicit restriction on the purposes for which data retained under the Code might be accessed.

The Committee appear to suggest that the human rights principle of proportionality would itself somehow prevent such access. However, the very essence of proportionality as a concept is that it does not impose blanket restrictions. Rather, in these circumstances, it involves considering in each case whether the privacy infringement access might entail is outweighed by the potential value of the data to the investigation in question. The Government finds it difficult to see that this balancing exercise is wholly dependent on the purpose for which the communication service provider holds the data in question, particularly where it is very clear that when the 2001 Act was passed Parliament did not intend access to be restricted in that way.

Furthermore, as a matter of policy the Government considers that it is right that whether data can be accessed by public authorities should not be restricted by the fact that it is held by a communications service provider under the Code rather than for its own business purposes. For example, in the course of a murder inquiry, say, a new suspect comes to light some 10 months after the murder itself. The police may need to obtain mobile phone location data to help identify the location of this suspect at the time of the murder. In the future this data might still be in existence only because it is retained by a communications service provider under the Code. Under the 2000 Act and the draft Regulation of Investigatory Powers (Communications Data) Order 2003 the police will be able to access location data for the purposes of preventing or detecting crime if it is necessary and proportionate to do so. However, say the murder does not relate to national security. Is it right that the police should not have access to the data simply because the communications service provider holds it under the Code rather than for its own business purposes? The Government thinks not, considering instead that whether access to such data should be allowed should depend on whether it is necessary and proportionate for the police to have access to that data in light of the circumstances of the particular case they are investigating. Accordingly, no legal or technological measures are being taken or are planed to ensure that the communications data retained for the purposes of Part 11 of the 2001 Act will not be available for the purposes other than protection of national security.
Q. 5 What views does the information commissioner express when consulted on the Draft Code?

The views on the Information Commissioner on the Draft Code are set out in section 11 of the Consultation Paper issued in March 2003. The Information Commissioner accepts that the processing of personal data involved in the retention of communications data by communication service providers in excess of the period required for their normal business purposes for the specific purposes identified in the 2001 Act will not in itself be unlawful processing under the Data Protection Act 1998 nor would it necessarily be unlawful on human rights ground.

Q. 6 What steps should be taken to consult with the communication service providers, when and over what period these consultations take place; and what views do the communications service providers express?

The Home Office undertook an extensive consultation with Industry which started in early 2002. The Home Office formed a Technical Working Group made up of representatives from Industry as well as the intelligence community to discuss the technical aspects of the draft Code of Practice. One day meetings were held every month for several months and culminated in a two day meeting in March 2003. The Home Office also organised a Government Industry Forum every six months which again gave the Industry a platform to speak to the Government. At the same time the Home Office met with the Operators Group and the Internet Service Providers Association, again giving Industry an opportunity to voice its opinions. In January 2003 the Home Office began visiting most of the larger communications service providers to discuss the draft Code of Practice with them individually. Having talked to the major players in the Industry, the Home Office then began visiting many of the smaller companies in order to explain its objectives and again discuss the draft Code of Practice. These meetings enabled the Government to assess the impact that the Code would have on both the large and smaller communication service providers. The Home Office public consultation began on the 11th March 2003 for three months and again Industry was encouraged to participate in this consultation.

The communications service providers expressed concerns over the legality of a voluntary Code of Practice and its compliance with European Convention on Human Rights. The Government gave repeated assurances on both these issues and the Information Commissioner also published a letter aimed at allaying these fears.

Q. 7 Does the Government consider that it is necessary to press ahead with these Draft Orders and Draft Code of Practice at this time, and if so, why?

These draft Orders and the draft Code of Practice are high on the list of government priorities and consequently the government is determined to press ahead with them at this time.

The 2001 Act was an emergency piece of legislation which was introduced as a consequence of the terrorist attacks on America on 11th September. That terrorist threat is still with us. It is therefore critically important to put these measures in place as soon as possible, in order to provide investigators with the necessary tools to fight terrorism and safeguard national security.

The current situation is that communications data is held by the many communication service providers for varying lengths of time depending on the individual company's business requirement. As technology has advanced the need to retain data for business purposes has diminished and this trend is set to continue. The government must act quickly in order to ensure that enough data is being retained. Failure to do so could lead to less
data being retained than there is at present which could significantly prejudice the fight against terrorism and the safeguarding of our national security.

Q. 8 Are there any pressing considerations which would weigh against allowing the issues relating to these proposed items of legislation being dealt with according to a timetable which allowed more time for parliamentary scrutiny and further consultation?

The Retention of Communications Data (Extension of Initial Period) Order 2003 must be debated in both Houses before the 13th December 2003 deadline set out in the 2001 Act. It is therefore critical that this Order be dealt with immediately otherwise the powers set out in section 104 of the 2001 Act, giving the Secretary of State the authority to issue directions, will lapse.

The Order relating to the Code of Practice was laid before Parliament on the 11th September and the Government believes that sufficient time has already been allowed for the document to be adequately scrutinised by Parliament.

As I have indicated, extensive consultation with the Industry has already taken place. We have consulted the Industry through the Operators Group, Internet Service Providers Association and with the Technical Working Group set up by the Home Office. In addition, the Home Office visited the majority of the major communication service providers to discuss the draft Code of Practice and made a huge effort to visit as many smaller companies as was possible. A three month public consultation has also been undertaken.

7 November 2003

3. Letter from the Chair to David Tredinnick MP, Chairman, Joint Committee on Statutory Instruments

I am aware that the Joint Committee on Statutory Instruments considered the above Draft Orders and reported on them in its Twenty-Eighth Report. At its most recent meeting, various matters relating to them were drawn to the attention of the Joint Committee on Human Rights. Your Committee might find it helpful to know of the concerns of the JCHR in relation to the human rights implications of the Draft Orders, which link to our concerns about an order proposed to be made under the Anti-terrorism, Crime and Security Act.

1. Draft Regulation of Investigatory Powers (Communications Data) Order 2003

This would extend the class of bodies currently allowed to obtain communications data or to receive disclosures of communications data under the Regulation of Investigatory Powers Act 2000, section 25(1). Retention and disclosure of communications data represent an interference with private life, and require to be justified under the Human Rights Act 1998 and ECHR Article 8.2 if they are not to amount to a violation of the right to respect for private life under ECHR Article 8.1. If the interference is not justified, the retention or disclosure is unlawful except so far as it is required by the terms of primary legislation which cannot be read or given effect in a manner compatible with the right: Human Rights Act 1998, sections 3 and 6. To be justifiable under Article 8.2, a disclosures must be in accordance with the law, and necessary in a democratic society for one of the purposes specified in Article 8.2. ‘Necessary in a democratic society’ means that the interference must be a response to a pressing social need, and must be proportionate, i.e. must not interfere with the right more than is necessary in order to achieve the legitimate objective and must be shown to strike a fair balance between the right in question and the public interest.
At present, the class of bodies authorized under section 25 of the 2000 Act is tightly confined. This restriction can be seen as an important aspect of the balance struck by Parliament between the right to respect for private life and the public interest in the prevention and detection of crime.

By vastly increasing the range of bodies allowed to obtain access to communications data, and thereby extending the variety of purposes for which the communications data could be used, the Draft Order would risk undermining the proportionality of the statutory scheme. Such an Order might as a result be *ultra vires*, because subordinate legislation which is not compatible with a Convention right is liable to be struck down on that ground unless the incompatibility is required by primary legislation. The Order might also purport to authorize requests from public authorities for disclosure which, because of section 6(1) of the 1998 Act, would be unlawful by virtue of incompatibility with a Convention right as being unjustifiable under ECHR Article 8.2. If a communications service provider is regarded as a ‘functional’ public authority under section 6(3)(b) of the 1998 Act, it too would act unlawfully if it made a disclosure which could not be justified under ECHR Article 8.2.

The JCHR was concerned that there might be insufficient justification for allowing, for example, ambulance services to seek communications data, and that a provision permitting it might be disproportionate to any legitimate aim and so unlawful under the Human Rights Act 1998.

The JCHR was also concerned that the greatly increased class of bodies allowed access to communications data under the Draft Order might also have access to data which could not lawfully be retained under the 2000 Act but would be available on account of being retained for an extended period for the purposes of Part 11 of the Anti-terrorism, Crime and Security Act 2001 under the Draft Voluntary Code of Practice which has been laid before Parliament. The Committee considered that this ‘leakage’ of information, retention of which is justified only to protect national security, into other inquiries might compromise the proportionality of the interference with ECHR Article 8 through both Part 11 of the 2001 Act and section 25 of the 2000 Act. The JCHR has written to the Home Secretary to ask about this aspect of the relationship between the Draft Voluntary Code of Practice under the 2001 Act and the Draft Regulation of Investigatory Powers (Communications Data) Order 2003. I enclose a copy of this letter.


This would extend the class of bodies entitled under Part II of the Regulation of Investigatory Powers Act 2000 to authorize directed surveillance, and in the case of some of the bodies also to authorize the use of covert human intelligence sources, under sections 28 and 29 of, and Schedule 1 to, the Act.

The authorization and use of these powers represents an interference with the right to respect for private life under ECHR Article 8 and the Human Rights Act 1998. As this brings into play considerations of pressing social need and proportionality (as noted above) under ECHR Article 8.2, the JCHR was concerned that the Government should be able to establish the lawfulness of the extension by showing why the extension of the powers to these additional bodies is necessary and proportionate.


This would designate the Northern Ireland Office, and specifically the Northern Ireland Prison Service, as a body authorized to undertake intrusive surveillance under Part II of the
Regulation of Investigatory Powers Act 2000. Intrusive surveillance can intrude on the most intimate aspects of people's private and family lives. It always engages the right to respect for private life, and often engages the right to respect for family life, under ECHR Article 8 and the Human Rights Act 1998. Because of the sensitivity and intimacy of the fields into which the surveillance intrudes, it requires very strong justification.

The JCHR was concerned that the Government should be able to show that it is really necessary for the Northern Ireland Prison Service to have this power, and that its use would be likely to be proportionate to a pressing social need and advance one of the legitimate aims under ECHR Article 8.2, since a failure to establish that those requirements are met could lead to either the Draft Order, or actions taken pursuant to it, or both, being ultra vires and unlawful.

As the JCSI has reported these instruments without comment, we do not intend to report on them separately. However, I thought it would be helpful to make your Committee aware of these concerns, since it appears the instruments are to be prayed against in the Lords on 12 November. I expect to publish this letter as an appendix to a report from the JCHR before then if possible.

3 November 2003

4. Letter from David Tredinnick MP, Chairman of the Joint Committee on Statutory Instruments, to the Chair

Thank you for your letter of 3 November concerning the above draft Orders. The Joint Committee considered the matter at its meeting this afternoon.

As you note, my Committee completed consideration of these draft Orders at its meeting on 21st October, and determined that the special attention of both Houses did not need to be drawn to any of them on any of the criteria against which it is instructed to assess instruments. It may be helpful if I set out the reasons why the Committee arrived at this decision, given the concerns which your Committee has raised about the draft Orders.

Generally speaking, in cases such as these, concerns about an instrument turn on an assessment of whether the provision made is necessary and proportionate to the legitimate aim of the instrument. Any such assessment is likely to involve an investigation of the merits of the instrument or the policy which lies behind it.

My Committee is not well-placed to make this assessment because, consistently with its standing order, its consideration of an instrument is limited to aspects other than its merits or underlying policy. For this reason, my Committee will not usually require the Government to demonstrate that an instrument is necessary and proportionate in human rights terms. However, it would, for example, request a memorandum from the Department concerned if the instrument were of a kind for which the Government has agreed to provide the equivalent of a section 19 statement and no such statement has been provided.

In the case of each of these three Orders, the explanatory memorandum contained a statement of the Minister's view that it was compatible with the Convention rights. The main effect of each of the orders is to enable additional public bodies to operate (subject, in the case of two of the Orders, to restrictions) procedures already set out in the Regulation of Investigatory Powers Act 2000 itself. Those procedures include requirements as to proportionality and necessity. Accordingly, while recognising that there may well be issues for your Committee, my Committee did not consider it necessary to investigate
further whether the act of making any of the orders (if approved) would be incompatible with a Convention right and so unlawful under section 6 of the Human Rights Act 1998.

In the past, where the question of the compatibility of an instrument with the Convention has turned on the fine judgments referred to above, my Committee has been willing to draw matters to the attention of your Committee for further investigation. We are entirely happy for this collaboration to continue.

I am content for this letter, and your letter of 3 November, to be printed as appendices to the relevant report of your Committee.

11 November 2003
### Reports from the Joint Committee on Human Rights since 2001

The following reports have been produced

#### Session 2002–03

<table>
<thead>
<tr>
<th>Report</th>
<th>Title</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>Scrutiny of Bills: Progress Report</td>
<td>HL Paper 24/HC 191</td>
</tr>
<tr>
<td>Second</td>
<td>Criminal Justice Bill</td>
<td>HL Paper 40/HC 374</td>
</tr>
<tr>
<td>Third</td>
<td>Scrutiny of Bills: Further Progress Report</td>
<td>HL Paper 41/HC 375</td>
</tr>
<tr>
<td>Fourth</td>
<td>Scrutiny of Bills: Further Progress Report</td>
<td>HL Paper 50/HC 397</td>
</tr>
<tr>
<td>Fifth</td>
<td>Continuance in force of sections 21 to 23 of the Anti-terrorism, Crime and Security Act 2001</td>
<td>HL Paper 59/HC 462</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HC 489-I</td>
</tr>
<tr>
<td>Seventh</td>
<td>Scrutiny of Bills: Further Progress Report</td>
<td>HL Paper 74/HC 547</td>
</tr>
<tr>
<td>Eighth</td>
<td>Scrutiny of Bills: Further Progress Report</td>
<td>HL Paper 90/HC 634</td>
</tr>
<tr>
<td>Ninth</td>
<td>The Case for a Children’s Commissioner for England</td>
<td>HL Paper 96/HC 666</td>
</tr>
<tr>
<td>Eleventh</td>
<td>Criminal Justice Bill: Further Report</td>
<td>HL Paper 118/HC 724</td>
</tr>
<tr>
<td>Twelfth</td>
<td>Scrutiny of Bills: Further Progress Report</td>
<td>HL Paper 119/HC 765</td>
</tr>
<tr>
<td>Thirteenth</td>
<td>Anti-social Behaviour Bill</td>
<td>HL Paper 120/HC 766</td>
</tr>
<tr>
<td>Fourteenth</td>
<td>Work of the Northern Ireland Human Rights Commission</td>
<td>HL Paper 132/HC 142</td>
</tr>
<tr>
<td>Fifteenth</td>
<td>Scrutiny of Bills and Draft Bills: Further Progress Report</td>
<td>HL Paper 149/HC 1005</td>
</tr>
</tbody>
</table>

#### Session 2001–02

<table>
<thead>
<tr>
<th>Report</th>
<th>Title</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>Homelessness Bill</td>
<td>HL Paper 30/HC 314</td>
</tr>
<tr>
<td>Second</td>
<td>Anti-terrorism, Crime and Security Bill</td>
<td>HL Paper 37/HC 372</td>
</tr>
<tr>
<td>Third</td>
<td>Proceeds of Crime Bill</td>
<td>HL Paper 43/HC 405</td>
</tr>
<tr>
<td>Fourth</td>
<td>Sex Discrimination (Election Candidates) Bill</td>
<td>HL Paper 44/HC 406</td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Paper Code</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>Sixth Report</td>
<td>The Mental Health Act 1983 (Remedial) Order 2001</td>
<td>HL Paper 57/HC 472</td>
</tr>
<tr>
<td>Seventh Report</td>
<td>Making of Remedial Orders</td>
<td>HL Paper 58/HC 473</td>
</tr>
<tr>
<td>Eighth Report</td>
<td>Tobacco Advertising and Promotion Bill</td>
<td>HL Paper 59/HC 474</td>
</tr>
<tr>
<td>Ninth Report</td>
<td>Scrutiny of Bills: Progress Report</td>
<td>HL Paper 60/HC475</td>
</tr>
<tr>
<td>Tenth Report</td>
<td>Animal Health Bill</td>
<td>HL Paper 67/HC 542</td>
</tr>
<tr>
<td>Twelfth Report</td>
<td>Employment Bill</td>
<td>HL Paper 85/HC 645</td>
</tr>
<tr>
<td>Thirteenth Report</td>
<td>Police Reform Bill</td>
<td>HL Paper 86/HC 646</td>
</tr>
<tr>
<td>Fourteenth Report</td>
<td>Scrutiny of Bills: Private Members' Bills and Private Bills</td>
<td>HL Paper 93/HC 674</td>
</tr>
<tr>
<td>Seventeenth Report</td>
<td>Nationality, Immigration and Asylum Bill</td>
<td>HL Paper 132/HC 961</td>
</tr>
<tr>
<td>Nineteenth Report</td>
<td>Draft Communications Bill</td>
<td>HL Paper 149/HC 1102</td>
</tr>
<tr>
<td>Twentieth Report</td>
<td>Draft Extradition Bill</td>
<td>HL Paper 158/HC 1140</td>
</tr>
<tr>
<td>Twenty-fourth Report</td>
<td>Adoption and children Bill: As amended by the House of Lords on Report</td>
<td>HL Paper 177/HC 979</td>
</tr>
<tr>
<td>Twenty-fifth Report</td>
<td>Draft Mental Health Bill</td>
<td>HL Paper 181/HC 1294</td>
</tr>
</tbody>
</table>