ANTI-TERRORISM, CRIME AND SECURITY ACT 2001
RETENTION AND DISCLOSURE OF COMMUNICATIONS DATA
SUMMARY OF COUNSELS' ADVICE

1. The Information Commissioner (the "Commissioner") has sought and received advice from Leading and Junior Counsel[1] ("Counsel") addressing her concerns as to the lawfulness of proposed arrangements to be made under a voluntary Code of Practice governing the retention of data by communications service providers ("CSPs") to be issued under section 102 of the Anti-terrorism, Crime and Security Act 2001 ("ATCSA") and the subsequent disclosure of such data by CSPs to bodies authorised to seek access to communications data under section 22 of the Regulation of Investigatory Powers Act 2000 ("RIPA").

2. At the heart of the Commissioner's concerns is the apparent disparity between the purposes for which CSPs may be asked (or, ultimately, required) to retain data under ATCSA and the purposes for which they may then be asked to disclose such data under section 22 of RIPA. This disparity of purpose arises from the potential interaction between two separate legislative regimes.

3. The first (ATCSA) provides only for the retention of data which CSPs would otherwise retain for business purposes. Its object is not to enlarge the fields of data which a CSP may (or must) retain, but to permit (or require) CSPs to retain the data for longer than they would otherwise need to do for their own commercial purposes. The statutory purpose of the measure is to ensure that such data is available for the purposes of safeguarding national security or for the prevention or detection of crime or the prosecution of offences which relate directly or indirectly to national security.

4. The second regime (RIPA) permits a range of public authorities to obtain access to such communications data for a wide variety of public interest purposes (section 22(2) RIPA) which extend substantially beyond issues concerning national security. They include, for example, the collection of taxes or other levies due to any government department. The list of permissible purposes is, moreover, amenable to extension by statutory instrument.

5. The consequence of these two overlapping regimes is that data may be retained for longer than they otherwise would be, on the ground that their retention is necessary for the purposes of safeguarding national security, but that the data may then be accessed for a variety of collateral public purposes which have no connection (direct or indirect) with national security.

6. Part 11 of ATCSA establishes a new regime which is intended to govern the periods of time during which CSPs may retain communications data. CSPs are currently required to destroy or depersonalise communications data when their retention is no longer necessary for billing or marketing purposes, save to the

[1] Ben Emmerson QC and Helen Mountfield, both of Matrix Chambers

extent that their retention or disclosure is required by or under a statute, a rule of law or a court order, or their destruction or depersonalisation would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. The legislative bases for such restrictions on retention of communications data are to be found in the Data Protection Act 1998 and the Telecommunications (Data Protection and Privacy) Regulations 1999.

7. The object of Part 11 is to standardise the period of retention, and to extend that period, to enable communications data to be available for the purposes of safeguarding national security or for the prevention or detection of crime or the prosecution of offences which relate directly or indirectly to national security. It is apparent from the terms of the legislation itself, and from the amendments made during its passage through Parliament, that the intention of Parliament was to ensure the availability of communications data for the purpose of investigating terrorist offences, or offences relating to national security. During the passage of the bill the statutory purposes for which an extended retention period was to be provided were restricted to offences connected, directly or indirectly, with national security.

8. The result is a regime which was apparently intended by Parliament to secure the continued availability of a pool of communications data, which can then be the subject of a notice under section 22 RIPA where the data are necessary either for the purpose specified in section 22(2)(a) RIPA ("in the interests of national security") or for a purpose specified in section 22(2)(b) ("preventing or detecting crime or preventing disorder") *but, in the latter case, only where the offence in question related, directly or indirectly, to national security*. This extension of the CSP's retention period was considered necessary as part of the United Kingdom's response to the events of September 11 2001. It is clear that the purpose behind the legislation, and the terms of the legislation as enacted, are both rooted firmly and exclusively in the need to protect national security, and it was on this basis that Parliament gave its approval to the legislative scheme.

9. Under section 102(1) of ATCSA the Secretary of State is required to issue and may from time to time revise a Code of Practice relating to the retention by CSPs of communications data obtained by or held by them. The procedure for making the Code of Practice is governed by section 103 ATCSA. The Secretary of State is required to publish the Code in draft and to consider any representations about the draft. He is specifically required to consult with the Commissioner and with CSPs to whom the Code will apply. He is then to lay the draft Code before Parliament. The Code is to be brought into force by statutory instrument which is to be approved by Parliament under the affirmative resolution procedure.

10. In the event that the voluntary scheme fails, the legislation provides for a default position. Section 104 ATCSA confers on the Secretary of State power to issue a direction, by order made by statutory instrument, specifying the maximum period that a CSP may be required to retain communications data while the order is in force. The power to issue such an order is only to be exercised if, after reviewing the operation of any Code or agreement under section 102, the Secretary of State considers it to be necessary to do so. Such an order may only be made for the statutory purposes prescribed in section

102(3). Accordingly, the legislation envisages that the Secretary of State must first seek to achieve a workable system of voluntary data retention for national security purposes and only if that fails adequately to meet those objectives may he resort to compulsory powers. As with the Code, there are statutory consultation requirements but these do not include the Commissioner.

11. Section 102(2) provides that the Secretary of State may enter into such agreements as he considers appropriate with any CSP about the practice to be followed in relation to the retention of communications data. Both the proposed Code, and any agreement, are to be voluntary. Section 102(4) makes it clear that a failure by any person to comply with a Code or agreement under the section does not render him liable to any criminal or civil proceedings.

12. The purposes of such a Code or agreement are, however, restricted by section 102(3). This provides that a Code or agreement under the section "may contain any such provision as appears to the Secretary of State to be necessary (a) for the purpose of safeguarding national security; or (b) for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security".

13. It follows that the statutory purposes for which extended data retention under such a Code or agreement are permissible are each circumscribed by the need to protect national security. None of the broader public interest purposes contemplated by section 22(2) RIPA are within the proper ambit of such a code. It is, however, an inevitable consequence of the scheme envisaged by ATCSA that communications data which have been retained solely for the section 102(3) purpose of safeguarding national security will then be in the possession of the CSP for an extended period and available for production in accordance with a notice issued under section 22 RIPA for a purpose with no connection whatever to terrorism or national security.

14. Counsel regard it as significant that Parliament did not pass an amendment proposed during the passage of the bill to bring section 102(3) into line with the statutory purposes in section 22(2) RIPA. Counsel believe the proper inference to be drawn from this is that Parliament intended that data retained under section 102(3) ATCSA should be retained only for the section 102(3) purposes and not for the wider purposes envisaged by section 22(2) RIPA.

15. There is, in Counsel's view, no doubt that both the retention of communications data on behalf of a public authority, and the disclosure of such data to a public authority constitute an interference with the right to respect for private life and correspondence enshrined in Article 8(1) of the European Convention on Human Rights ("ECHR") (see, for example, *Leander v Sweden* (1987) 9 EHRR 433; *Hilton v UK* (1988) 57 DR 108; *MS v Sweden* (1997) 28 EHRR 313).

16. In order to be justified, under Article 8(2), any such interference must meet two requirements. First, it must be carried out "in accordance with the law". This requires that an interference must have some basis in national law (*Sunday Times v United Kingdom* (1979) 2 EHRR 245 at para. 47). In addition, the law concerned must be accessible and precise (i.e. it must be publicly available and

foreseeable in its consequences). Where the state has powers to carry out investigations involving an interference with the right to privacy, Article 8 requires a positive framework of legal rules circumscribing the exercise of any such power, and incorporating legally binding safeguards against abuse. The second requirement of Article 8(2) is that any interference must be proportionate to one of the legitimate aims set out in that paragraph. This involves, firstly, an assessment of the degree of intrusion involved, and of the strength of the public policy justification on which it depends. In addition, however, where the compilation and disclosure of personal data by or to the state are in issue, the concept of proportionality also involves an assessment of the adequacy of the safeguards in place to prevent abuse.

17. When the two statutory schemes are overlaid and considered in the context of a human rights analysis, and in particular the issue of proportionality, the problems raised by the disparity of purpose between section 22(2) RIPA and section 102(3) ATCSA come into sharp focus. Section 22 RIPA was enacted against the background of the existing restrictions on the period during which a CSP could retain communications data (and in particular the Telecommunications (Data Protection and Privacy) Regulations 1999). Whilst it is undoubtedly true that there were certain limited circumstances in which a disclosure notice could have the effect of requiring a CSP to retain data beyond the period necessary for its own commercial needs, there was no general provision for requiring such data to be retained and kept available for the wide list of public purposes set out in section 22(2) RIPA.

18. In enacting section 102(3) of ATCSA, Parliament has now decided that a general extension of that period *is* justified, *but only in a narrow range of circumstances, where national security considerations are at stake.* The balance struck in the legislation represents Parliament's own assessment of the limits of proportionality in this context. Assuming that Parliament were to endorse the period proposed in the draft Code, then it would have concluded that *where national security was in issue*, the retention of communications data for that period, in order to make it available for national security purposes under section 22 RIPA, was proportionate to the legitimate aim pursued.

19. But Parliament plainly did not conclude that a general extension was proportionate to the less pressing public interests in section 22(2). Quite the reverse; Parliament's decision not to follow the terms of section 22(2) RIPA, and instead to restrict the statutory purposes under section 102(3) ATCSA to cases involving national security is, in Counsel's view, powerful evidence that it did not consider those less pressing public interests to be sufficiently weighty to justify a general requirement for the extended retention of communications data.

20. If that is right then the issuing of a notice by a RIPA designated person under section 22 RIPA for a purpose entirely unrelated to national security, where the CSP concerned has retained the data in question beyond the period necessary for its own business purposes, such that the data have been retained solely for the purposes of national security in accordance with section 102 ATCSA, is arguably disproportionate and therefore incompatible with Article 8.

21. There is thus a significant risk that a RIPA designated person would, in the circumstances outlined in paragraph 20 above, be acting unlawfully under section 6(1) of the Human Rights Act 1998 (the "HRA"). However, it does not necessarily follow that a CSP that acted in obedience to such a notice would be acting unlawfully. The Commissioner sought advice as to whether CSPs are to be regarded as public authorities for the purposes of the HRA in circumstances where the CSP retains communications data beyond the period during which such retention is necessary for its own private commercial purposes in reliance on a voluntary Code of Practice issued under section 102 ATCSA for the purposes of national security. It is arguable that in those circumstances CSPs are exercising functions of a public nature that may bring them within the definition of "public authority" in the HRA and therefore within the ambit of the duty at section 6 of the HRA. The position in law is not clear. All that Counsel can say with certainty at this point is that a CSP would not be safe to assume that extended retention under Part 11 ATCSA (whether under a voluntary or mandatory scheme) is a purely private function outside the scope of section 6 of the HRA.

22. Counsel consider that where a RIPA designated person seeks or obtains access to communications data retained solely under section 102 ATCSA (and beyond the period necessary for business purposes) for a section 22(2) RIPA purpose unrelated to national security, there is a significant risk that the rights of the data subject under Article 8 would be infringed. This arises because, in Counsel's view, Parliament has fixed the limits of proportionality in this context by confining extended retention to national security purposes.

23. Counsel took account of the fact that Parliament has endorsed the adoption of a voluntary scheme based upon a Code of Practice and voluntary agreements. However, Parliament's intention must be judged in light of the restricted statutory purposes set out in section 102(3) ATCSA. As such the Commissioner is entitled to take into account, in commenting on the Code of Practice, the likelihood that the proposed regime will lead directly to disclosures under section 22 RIPA which are inconsistent with Parliament's intention in passing ATCSA, and thus arguably unlawful under Article 8 ECHR and section 6 HRA.

24. The Commissioner has been advised that it is not data retention under ATCSA which is arguably unlawful but rather the potential collateral use which may be made of such data under section 22 RIPA. The result would be the same whether the arrangements for extended retention are made voluntarily under section 102 ATCSA or under compulsory powers contained in section 104. Either way, the governing purpose of the retention is circumscribed by Parliament's decision, through section 102(3), to limit extended retention to that which is necessary for national security purposes.

25. The Commissioner has been advised that this problem cannot be adequately redressed by amendments to the Code. The arrangements governing disclosure are not within the proper ambit of the Code, which is concerned only with retention. A Code issued under section 102 ATCSA could not, in Counsel's view, restrict the scope of the statutory powers under section 22 RIPA or the

statutory obligation on a CSP to comply with a section 22 notice. Indeed, if it purported to do so the Code would be arguably *ultra vires*.