

LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty response to the Home Office consultation: 'Access to Communications Data'

June 2003

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Introduction

1. This is Liberty's response to the Home Office consultation paper entitled "Access to Communications Data: Respecting Privacy and Protecting the Public from Crime, which seeks views on proposals for a draft Order under s. 25(2) of the Regulation of Investigatory Powers Act 2000 ("RIPA"). The resulting draft Order would be laid before Parliament in place of the draft withdrawn during 2002.

2. Liberty's interest in these matters is well known. We contributed extensively to the legislative process that led to enactment of RIPA. In particular we responded to the preceding consultation exercises on Interception of Communications (Cm 4368) and to the proposed interception provisions originally set out in the draft Electronic Communications Bill. We also proposed amendments to provisions of (among others) Part I of the Regulation of Investigatory Powers Bill, and provided material which helped inform Parliamentary debate on the legislation. More recently, we contributed our views to the consultation exercise on draft RIPA Codes of Practice published in August 2001 (mentioned in paragraph 12 of the present consultation paper).

3. We welcome the paper's numerous indications of the Government recognition of the importance of an approach based on the principles of necessity and proportionality. Liberty has long advocated the view that measures – and in particular clandestine measures – that intrude on privacy and other important rights of individuals should not be taken unless they meet a clearly established need, and go no further in extent than is necessary to satisfy that need in the circumstances.

4. In the context of this consultation, those principles operate at two levels. First, they govern the range of bodies that should be included in any Order, as well as the range of data to which each body should be entitled to seek access and the categories of post-holders within the body who should be entitled to exercise that entitlement. Second, they govern individual requests for access to data.

5. The latter point is important. Where a body successfully makes a case for inclusion in a draft Order, it will no doubt be subject to restrictions as regards the post-holders entitled to seek access and as regards the kinds of data that it may acquire. But there would still remain a risk of unnecessary and disproportionate interference with citizens' rights unless mechanisms are in place to ensure that data is accessed in individual cases only where, and to the extent that, a sufficient justification is established. The consultation paper recognises this in its discussion of safeguards. That is a key part of the balancing exercise to which the paper refers. The public interest in fighting crime or terrorism is not advanced in the slightest by the enactment of legislation permitting access to data beyond that strictly necessary to aid each particular investigation or operation.

6. Our comments on the paper's proposals are therefore directed at both levels. We deal with the general question of which sorts of organisation should be provided with powers of access to communications data (and subject to what overall restrictions), as well as the more specific challenge of maximise the safeguards that ensure that citizens' rights will be intruded upon only to the extent strictly necessary in each case.

Communications data and privacy

7. The consultation paper explains the distinction, drawn by RIPA itself, between the content of a communication on the one hand (access to which would fall within the interception provisions of Part I Chapter I) and data about the communication on the other. It is important to recognise that in practice the two categories shade into each other, as the example of a web server address and a specific page address demonstrates. It is possible through the use of communications data, in particular traffic data, to build up a detailed picture of an individual's activities, lifestyle and associations, from which detailed inferences can be drawn. The European Court has found violations of the Convention where State officials have made excessive use of powers to obtain access to documents in the nature of transaction records.¹

¹ *Funke v. France* (1993) Ser A no. 256-A. In the well-known *Malone* case ((1984) Ser. A no. 82) the Court found a violation of Article 8 in relation to telephone metering data as well as interception of content: see paragraphs 85-87

8. It would be wrong, therefore, to approach the regulation of access to communications data on the basis that such access raises less weighty privacy issues than access to content. In our view access to communications data requires safeguards no less effective than those needed in relation to interception proper.

Which bodies should the draft Order cover?

Overlap between existing and proposed powers of data access

9. It is inaccurate to suggest that each of the bodies within the withdrawn 2002 draft had pre-existing statutory powers of data access which those proposals would have conferred. There is a degree of overlap between the RIPA powers which the present proposals would confer on certain bodies and the powers of compulsory disclosure of information which those bodies already possess under specific legislation. To that extent, the bringing together of those bodies' powers of access to communications data under the rubric of RIPA, subject to proper conditions and safeguards, would be a step forward. Much of the subject-specific legislation conferring power to obtain disclosure is dated, and lacks the focus and safeguards necessary to enable a balance is maintained between individual rights and the wider public interest. Where there is an overlap between powers resulting from the draft Order and those resulting from other legislation, provision should be made to ensure whenever the body concerned seeks access to communications data, it does so under the RIPA regime. Otherwise the constraints and safeguards applicable to the RIPA scheme could simply be sidestepped.

10. Conversely, where a body has an existing theoretical right to gain access to communications data under its subject-specific disclosure powers, but has failed to convince Government that it ought to be included within a draft Order under RIPA, serious consideration should be given to taking the next available Parliamentary opportunity to

of the Court's judgment.

amend the subject-specific legislation to make clear that it does not confer, or no longer confers, power to obtain communications data. That is necessary because whereas Chapter 1 of Part 1 of RIPA provides for specific offences and a statutory tort in relation to unauthorised interception (section 1(1) to (3)), Chapter 2 makes no equivalent provision in relation to acquisition and disclosure of communications data.

A “shortlist” or a longer list of qualifying bodies?

11. We have some sympathy with the “shortlist” approach. However, we recognise that particular bodies beyond the obvious shortlist may be able to make a case for data access for limited purposes, and that it may not always be desirable or practicable for specialist investigations to be handed over to a shortlisted body such as the police or Customs. Indeed one argument in favour of keeping an investigation involving data access “in house” is that it minimises the risk of data leakage beyond the investigative purpose for which access was originally obtained: see further below.

12. We do, however, have a concern about bodies which would only rarely to seek access to communications data. Even if an accreditation or similar scheme were in place, it is unlikely that officers of such bodies would have an opportunity to acquire the necessary expertise in making suitably defined requests for access and in subsequently handling data in a way that minimises unnecessary intrusion into individual rights of privacy. Where a body would be likely to make only a very small number of requests annually – say 5 or fewer – it would be preferable for a more experienced body to deal with data access and handling on its behalf. That would not be tantamount to delegating an entire investigation, just the specific operations that involve access to and processing of communications data. Memoranda of understanding and the like between investigation or enforcement authorities are a common feature of the modern administrative framework, and such arrangements would provide an appropriate solution to this problem. A memorandum or agreement could contain specific terms aimed at minimising the risk of inappropriate obtaining or use of data.

Commercial organisations

13. Subject to the above points and the further point to be made here, we have no fundamental objection to the conferment of access powers, for the limited purposes and limited office-holders the paper suggests, to any of the various bodies proposed. The objection we make here concerns Royal Mail Group plc. That body now essentially operates as a commercial organisation in a market – albeit a regulated market – for postal services. We regard it as wrong in principle for commercial bodies, whether or not formerly part of the public sector, to be granted powers of access under RIPA or indeed any comparable statutory power. Such powers can be justified only on the basis of a public interest outweighing that of individuals affected by the exercise of the powers. A body in the commercial sector inevitably serves, and is perceived as serving, interests other than exclusively those of the public. It is moreover likely to be resistant to the degree of public accountability for its conduct that is necessary for supervision under RIPA to work effectively and to be seen to do so. We see no reason why (where appropriate) Postcomm, or in other cases the police, should not exercise the relevant access powers.

14. We would make the same principled objection to any future proposal to confer access powers on a commercial body. We also take the view that should any of the bodies on whom powers are conferred under the draft Order move into the private sector in the future, the powers should be removed.

Safeguards for the exercise of powers of access

The “double-lock”

15. We recommend that every instance of access to communications data pursuant to the draft Order should be subject to a “double lock” mechanism of independent scrutiny and authorisation. Our views on the proper nature of such a mechanism are well known and were expressed at the time of the consultation exercise that preceded the introduction of the Regulation of Investigatory Powers Bill. For the generality of cases we maintain our view that the appropriate procedure is prior *judicial* authorisation following an on-notice procedure

in which it would be open to the holder of the data to participate. There may be a case for relaxation of that requirement where (a) the data sought is merely subscriber information which would be readily available from published commercial sources, or (b) where the need for the information is particularly urgent (in which case there should be a requirement to obtain subsequent judicial validation of the action taken).

16. The case-law of the European Court of Human Rights emphasises that prior judicial authority is the preferable safeguard for the citizen's Article 8 rights in the investigative context.² The proposal for some administrative form of authorisation compares unfavourably with the framework for obtaining sensitive material in the course of ordinary criminal investigations. Under Schedule 1 to the Police and Criminal Evidence Act 1984, "special procedure material" (including journalistic material and other material held in confidence), the necessary authority must be given by a circuit judge, on notice to the third-party holder of the information. As far as the "serious crime" ground for data access is concerned, we see no reason why the safeguards for the suspect should not be at least as rigorous as those applicable to *routine* crime under PACE. Nor is there any compelling justification for less by way of safeguards where access is sought on other RIPA grounds.

17. The on-notice PACE procedure was introduced as a necessary safeguard for important rights. Requests by the police for press disclosure of journalistic material raise issues under Article 10 of the Convention. The judge provides vital independent scrutiny of the request and is well-placed to strike the proper balance between the interests of the investigation on the one hand and the public interest in maintaining the freedom of the press on the other. In many cases privacy interests are also at issue, in the shape of the relationship between journalists and those who provide them with information.

18. By analogy with the PACE position, an application on notice would be appropriate where communications data, other than merely published and commercially available subscriber data, are sought from a communications service provider ("CSP"). There should be a simple procedure, similar to the practice on applications under Schedule 1 to PACE, for a request to be

² *Funke*, above.

served on the CSP and then considered at a private hearing before a High Court judge. In exceptional cases of genuine urgency, authorisation of very short duration could be obtained without notice and followed by an application on notice at the earliest opportunity. Existing statutory powers to make rules of court would provide ample authority for establishing the necessary procedural framework. The draft Order could incorporate the procedure by simple reference.

19. The consultation paper mentions possible costs concerns on the part of CSPs as a potential reason for adopting a course other than judicial authorisation. However, there would be no obligation on the CSP to participate in the process, and in any event it is difficult to see how other mechanisms would involve the CSP in lesser potential expense. Moreover, against this and other objections to a judicial process must be weighed the vital consideration of public confidence. Judicial involvement under PACE is designed to, and does, maintain public confidence in the operation of the system. The public response to the 2002 draft Order speaks eloquently of the need to build and maintain similar confidence in the implementation of RIPA Part I Chapter II.

20. As a fall-back, we would support a requirement of prior authorisation by the Commissioner, again following an on-notice procedure in the generality of cases. We agree that carries risks of blurring the authorisation and supervision roles. Indeed that may be a good reason for preferring judicial involvement. In the absence of a regime for judicial authorisation, the involvement of the Commissioner would be better than any other canvassed option.

Post-acquisition safeguards

21. While we welcome the proposed restrictive approach to defining the office-holders who may exercise a body's powers of access, the value of that safeguard would be seriously undermined in the absence of controls to prevent leakage of acquired data to a wider audience within and beyond the body concerned.

22. The importance of such controls cannot be overemphasised. Both the European

Convention and the Data Protection Act 1998 impose constraints on the post-acquisition treatment of material as well as on its initial acquisition. Unjustified disclosure and dissemination of material will violate a data subject's rights under Article 8 even if the original acquisition was justified, as the European Court recently affirmed in *Peck v. UK*³. Moreover, domestic law has long recognised the dangers inherent in public bodies assembling items of data about an individual, each obtained from discrete sources and for discrete purposes but together amounting to a more serious invasion of personal privacy. In *Marcel v. Metropolitan Police Commissioner*⁴, Sir Nicolas Browne-Wilkinson V.-C. observed: "There are today numerous agencies of state upon which Parliament has conferred the power compulsorily to obtain information and documents from the private citizen. ... if the information obtained were to be gathered together in one file, the freedom of the individual would be gravely at risk. The dossier of private information is the badge of the totalitarian state".

23. In practical terms, a body's internal procedures should ensure that the office-holders who exercise a body's powers of access are sufficiently insulated from other elements of the body to prevent onward disclosure of material in a form that raises privacy issues. Where parts of an investigation are conducted by personnel other than the authorised office-holders, the information passed on by the office-holders that is derived from accessed data should be confined to that strictly necessary for the specific tasks of the investigating personnel. Where the accessing body conducts an investigation on behalf of or in association with another body (a possibility contemplated above) similar restrictions should apply to transmission of information between the two bodies.

24. A body should not be included in a draft Order unless and until the Government is satisfied that the body's arrangements and procedures sufficiently meet these requirements. The draft Order should itself make express provision for post-acquisition safeguards, making

³ Judgment of 28 January 2003.

⁴ [1991] 1 All ER 845, Ch. D.

lawful access conditional on the subsequent observance of procedures representing best data protection practice.

Gordon Nardell
39 Essex Street Chambers