
OPINION ON DRAFT COMMUNICATIONS DATA BILL

---

1. I am asked to advise the Open Rights Group ('ORG') concerning the provisions of the draft Communications Data Bill ('the Bill'). In particular, I am asked to advise on its compatibility with rights under the European Convention on Human Rights.

2. In outline, I conclude that the Bill is incompatible with the UK's obligations under Article 8 ECHR on the basis that:

    (i) it extends the power to obtain communications data under RIPA without improving on that statute's inadequate provision for authorisation and oversight; and

    (ii) it imposes a further requirement on CSPs and others to retain, make available and filter communications data for the purposes of lawful surveillance. In the absence of sufficient safeguards, this constitutes a further, disproportionate interference with the right to privacy.

Existing powers to obtain communications data

3. Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 ('RIPA) governs the power of public bodies to obtain communications data for the purpose of lawful surveillance.

4. 'Communications data' is defined by section 21 of RIPA. It includes traffic data, service user data and subscriber data as outlined above but excludes 'the contents of a communication' (section 21(4)(b)). 'Traffic data' includes any data that identifies:

    (a) all locations between which a particular communication is being carried out (e.g. origin and destination);

(b) the people involved (e.g. caller and receiver, sender and addresses, etc); or

(c) any equipment used to transmit, receive or route the communication (e.g. the type of phone being used).

5. Section 22 of RIPA governs authorisations for requests for communications data. It provides that each public body able to request data under RIPA has a designated person - typically a senior member of the organisation - who may request communication service providers to provide data where he or she believes it necessary:

a) in the interests of national security;

b) for the purpose of preventing or detecting crime or of preventing disorder;

c) in the interests of the economic well being of the United Kingdom;

d) in the interests of public safety;

e) for the purpose of protecting public health;

f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;

h) for any purpose … which is specified … by the Secretary of State;

i) to assist investigations into alleged miscarriages of justice; or

j) to identify and notify the next of kin of a deceased or incapable person.

6. In addition, the designated person may not request the provision of communications data unless he believes that it is proportionate to do so (section 22(2). The request to a service provider may be in the form of an authorisation (section 22(3)) or a notice (section 22(4)), the difference being the former is a request for information that the provider already holds, while a notice is a direction to the provider to acquire it on behalf of the requesting body. Notices and authorisations last one month unless renewed (sections 23(4) and (7)). Service providers must comply with notices requiring access to communications data under RIPA, unless it is 'not reasonably practicable' to do so (section 22(7)). If necessary, the Secretary of State can seek an injunction for the enforcement of the notice (section 22(8)).

7. Schedules 1 and 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) sets out an extremely broad range of public bodies that are able to request communications data under RIPA. However, not all public bodies have the same degree of access. First, there are various limitations on the purpose for which some public bodies can access data, e.g. the Scottish Ambulance Board may only make requests for the sake of preventing or mitigating injury or death during an emergency. Secondly, many public bodies are restricted in the type of communications data they can request, e.g. the Child Maintenance and Enforcement Commission is only able to request service user data and subscriber data but not traffic data.

8. Chapter 2 of Part 1 of RIPA came into force in January 2004. However, despite a promise made by the Interception of Communications Commissioner Sir Swinton Thomas in 2004 to provide details in his 2005 report (HC 549, November 2005), para 23), statistics on the annual number of requests for communications data were not made public until February 2007. Since January 2005, public bodies have made more than 2.7 million requests for communications data under RIPA. In the last reporting year alone, close to half a million such requests were made (HC 496, July 2012, para 7.3). The majority (52%) of these requests were for subscriber data, followed by traffic data (25%).

9. Section 37 of the Protection of Freedoms Act 2012 provides that local authorities will be only be able to request communications data under RIPA if they have obtained prior judicial authorisation. As the Bill's introduction notes, however:

Local authorities account for less than 0.5% of total annual RIPA requests for communications data. Following the implementation of the Protection of Freedoms Act, they will only be able to access this data if approved by a magistrate (p2).

10. It would be equally accurate to say, therefore, that 99.5% of all communications data requests under RIPA are not subject to prior judicial approval.

11. Oversight of requests for communications data is provided by the Interception of Communications Commissioner, a retired Court of Appeal judge working part-time (section 57(2)(b)). Since late 2005, public bodies able to make requests have been subject to an inspection regime carried out by an inspectorate under the direction of a Chief Inspector and the supervision of the Commissioner. However, it does not appear that any of the inspectorate are legally-qualified.

Compatibility of existing power under RIPA to obtain communications data

12. Article 8 ECHR provides that:

    1. Everyone has the right to respect for his private and family life, his home and his correspondence.

    2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

13. It is well-established that the right to respect for 'correspondence' under Article 8 includes not only the privacy of messages sent via post but also phone calls (*Klass v Germany* (1978) EHRR 214, para 41), pager messages (*Tasylor-Sabori v United Kingdom* (2003) 36 EHRR 17), emails and general Internet use (*Copland v United Kingdom* (no 62617/00, 3 April 2007).

14. In *Malone v United Kingdom* (1985) 7 EHRR 14, moreover, the Grand Chamber of the European Court of Human Rights held that communications data constituted an 'integral part' of private communications, and was therefore subject to the same protection under Article 8 (para 84).

15. In particular, Article 8 requires that access to communications data must be governed by legislation in the same manner as other kinds of surveillance, including 'adequate and effective safeguards against abuse' (*Klass v Germany* (1978) 2 EHRR 213, para 50). In the case of interception of communications (i.e. access to the content of a communication), the Court has held that prior authorisation by a judge or other independent body (*Iordachi and others v Moldova* (App no. 25198/02, 10 February 2009), para 40). In relation to other, less intrusive types of surveillance (e.g. GPS tracking), the ECtHR has said that 'subsequent judicial review of a person's surveillance' would offer 'sufficient protection against arbitrariness' (*Uzun v Germany,* no.35623/05, 2 September 2010), para 72). It is also important to note that *Malone* was a case about communications data in the days of telephone metering. By contrast, the digital nature of modern communications means that the traditional distinction between so-called 'envelope data' and the actual content of an email or internet session is becoming increasingly blurred.

16. Under RIPA, however, there is no requirement for a request for communications data to be subject to prior authorisation by a judge or other independent body save in relation to local authority requests (which as the Home Office itself notes, accounts for less than 0.5% of total requests). Instead the power to authorise communications data requests is made by a senior member of the same public body that is seeking the data. In my view, such a person cannot be credibly described as sufficiently independent or objective to provide an effective safeguard against arbitrariness or abuse. Nor is there guarantee that the communications data will be used as evidence in criminal or civil proceedings, meaning that there is highly unlikely to be 'subsequent judicial review'.

17. In almost all cases, therefore, only prospect for independent review of the legality of a request for communications data is the possibility of inspection by the Interception of Communications Commissioner and his team of inspectors. It is apparent, however, that there was no inspection regime of communications data requests between January 2004 (when Chapter 2 of Part 1 of RIPA came into force) and late 2005 because of Home Office

delays in recruiting the necessary staff (HC 315, February 2007, para 10). Even with a team of inspectors in place, the sheer volume of requests - just under half a million each year - makes it impossible for the part-time Commissioner and his team to review anything other than a very small proportion of requests.

18. In the circumstances, I conclude that the existing regime for the authorisation and oversight of communication data requests under RIPA does not comply with the requirements of Article 8.

The draft Communications Data Bill

19. According to its explanatory notes, the draft Bill provides "a new framework to ensure the availability of communications data and its obtaining by law enforcement agencies and other approved public authorities".

20. In terms of the procedures for authorisation and oversight, however, there is little material difference between the scheme proposed under the draft Bill and that already in place under Ch 2 of Part 2 of RIPA, as amended by the Protection of Freedoms Act 2012. For the same reasons as outlined above, I consider that its provisions are equally incompatible with the safeguards required under Article 8.

21. I note that the draft Bill has received a statement of compatibility with Convention rights, supported by a memorandum. However, a statement of compatibility is no bar to a statute being subsequently found to be incompatible by the courts: see e.g. the Immigration and Asylum Act 1999 received a statement of compatibility under section 19 of the Human Rights Act yet the penalty scheme contained in Part 2 of the Act subsequently found to breach the requirements of the right to a fair hearing under Article 6 (*International Transport Roth GmbH v Secretary of State for the Home Department* [2002] EWCA Civ 158).

22. The primary justification for the Bill is described as follows:

> Communications data from [new] technologies is not as accessible as data from older communications systems like 'fixed line' telephones. Although some

> internet data is already stored by communication service providers, other data is neither generated nor obtained because providers have no business need for it. This means that the police are finding it increasingly hard to use some types of communications data to investigate crime. To address this growing gap, the proposals set out here will require some communications service providers to obtain and store some communications data which they may have no business reason to collect at present (p2).

I consider this to be misleading, however. The main innovations of the Bill are not the requirements to obtain and store certain kinds of communications data which some communications service providers ('CSPs') might not otherwise store, but fresh powers given to the Secretary of State to (1) require CSPs to store and make available communications data in a particular way that is convenient to those public bodies seeking to access communications data; and (2) impose Request Filters to require CSPs to obtain process and filter communications data for the sake of surveillance by public bodies.

23. First, clause 1 provides the Secretary of State with an order-making power to "ensure that communications data is available to be obtained" and "otherwise facilitate" its availability (clause 1(1)). These include the imposition of requirements (clause 1(2)(b)) "whether as to the form or manner in which the data is held or otherwise" which "ensure that communications data can be disclosed without undue delay to relevant public authorities".

24. The only safeguards provided on the face of the draft Bill in relation to this power are a requirement on the Secretary of State to consult various interested parties (clause 2); a 12 month time limit on the retention of the data (clause 4); a requirement to destroy the data at the end of the retention period (clause 6); a requirement that orders under clause 1 be in writing (clause 7(1)), the ability of a person served with a notice to refer it to the Technical Advisory Board (clause 7(2)), who may in turn make an advisory report to the Secretary of State (clause 7(3)).

25. Secondly, clauses 14 to 16 of the Bill provide a new power to the Secretary of State to establish Request Filters in relation to requests for data from internet-based

communications. These provisions contain various safeguards, including requirements of necessity and proportionality (clause 15(4), the destruction of any unfiltered data (clause 16(1)), restrictions on its disclosure (clause 16(2), an exclusion from local authorities obtaining traffic data (clause 17), and oversight by the Interception of Communications Commissioner (clauses 14(4), 16(5)(b)) and 22) and Investigatory Powers Tribunal (clause 23).

26. As noted above, the main innovations of the Bill are the powers to direct CSPs to store, make available and, where required, filter communications data for the sake of facilitating lawful surveillance. This is, in my view, an unprecedented power. There are of course a number of areas of the law where the state may reasonably require individuals and companies to store records in a particular manner for the sake of some public purpose (e.g. taxation). Similarly, there are many different kinds of regulatory schemes that may impose similar requirements on those subject to them to not only provide certain kinds of information but require them to provide it in a certain format, etc. What is wholly exceptional about the Bill's provisions is that they relate to material which is entirely private and indeed, as the European Court in *Malone* noted, an 'integral' aspect of private communications.

27. This is especially problematic where the consequence of the Secretary of State's order is almost certain to result in the large-scale retention of the communications data of millions of individuals by CSPs. As the Grand Chamber of the ECtHR noted in S and Marper v United Kingdom(2008) 48 EHRR 50 at para 103:

> The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford *appropriate safeguards* to prevent any such use of personal data as may be inconsistent with the guarantees of this Article .... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, *not least when such data are used for police purposes.* The domestic law should notably ensure that such data are relevant and *not excessive* in relation to the purposes for which they are stored .... The

> domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse [emphasis added].

I do not regard it as material for the purpose of Article 8 ECHR that the data in question relates to communications data rather than DNA data, nor whether the database is a centralised one or a distributed one. It is clear that communications data is protected on the same basis that private communications are. What matters is the ease of access that public bodies will have to the sensitive private data of millions of persons as a result. Indeed, the need for effective safeguards is even more crucial in the context of surveillance than in relation to DNA retention because of the necessary lack of transparency that covert surveillance involves: see *Klass*, et al.

28. I consider it highly unfortunate that the Home Office Memorandum accompanying the draft Bill fails to recognise the plainly intrusive nature of these further requirements. As the judgment of the ECtHR in *Malone* makes clear, communications data is protected under Article 8 in the same manner as communications themselves. Any interference must therefore not only be prescribed by law and pursue a legitimate aim but be "necessary in a democratic society" and proportionate to the aim pursued. A suitable analogy can be drawn with the use of a search warrant. A search of a person's home may be a justified measure notwithstanding the inevitable interference with their privacy. We would not say, however, that a generalised requirement on all people to keep their doors unlocked or store their belongings in a particular manner in order to facilitate searching by the police would be a proportionate measure.

29. The same is true of the draft Bill.. It is entirely reasonable to require CSPs to comply promptly to lawful requests for communications data. What is plainly disproportionate is the Bill's power to require CSPs to store, make available and filter their customers' private communications data in a particular manner for the sake of making covert surveillance easier. Such an approach fails to accord due weight to the private nature of the material in question. Even taking into account the Home Office's arguments concerning the changing nature of digital communications, such a dramatic extension of retention of communications data cannot properly be said to be "necessary in a democratic society".

30. Of particular concern is the possibility, not ruled out by the Bill, that the Secretary of State could order CSPs to provide unmediated access to communications data, for the involvement of CSPs who are themselves outside the apparatus of the state in facilitating surveillance is inevitably a practical check against arbitrariness and abuse. Although the Bill makes some attempt at providing safeguards (primarily in relation to time limits for retention, destruction of data, and oversight by the Interception of Communications Data), these are necessary measures but in no way sufficient to counterbalance the large-scale retention of communications data for surveillance purposes.

31. More generally, for the reasons addressed above, the draft Bill fails improve on the authorisation and oversight provisions of RIPA. As the Home Office itself concedes, 99.5% of communications data requests are not subject to prior judicial authorisation, nor is there any other requirement for prior authorisation by an independent body. Instead, requests for communications data other than those made by local authorities are approved by senior members of the same organisation seeking the information, and are therefore incapable of providing the necessary independence and objectivity required under Article 8 ECHR.

32. Nor does either RIPA or the draft Bill provide for effective *ex post facto* supervision: the Interception of Communications Commissioner is a part-time official, his inspectorate are not legally qualified and they inevitably inspect only a small proportion of approximately half a million authorisations for communications data made by public bodies each year.

33. On a more positive note, clause 24 makes provision for the repeal of various statutory powers for public bodies to obtain data outside of RIPA (see *Review of Counter-Terrorism and Security Powers* (Cm 8003, January 2011), p6). Given that these powers were not subject to any kind of authorisation or oversight for many a year, this is a long-overdue measure.

ERIC METCALFE

Monckton Chambers

26 July 2012