

Dear Sirs

The Foundation for Information Policy Research would like to submit the following comments.

Communications Data

1. The content of letters, emails and telephone calls can be extremely private. Access to this content by law enforcement agencies is only allowed under very strict controls - at present, a warrant signed by a senior minister.
2. "Communications data" such as a list of websites visited, addresses of e-mail correspondents, and the location of mobile phones, are also very sensitive personal data that can paint a very detailed picture of an individual's life. They provide profound insights into a person's contacts, movements and thinking.
3. FIPR agrees with Elizabeth France, the former Information Commissioner, that privacy can be seriously compromised by access to traffic data as well as to intercepted content. Mrs France commented in a Parliamentary briefing that "[b]oth sets of data provide insight into the private lives of individuals and should therefore be subject to equivalent controls and safeguards" [1].
4. Those safeguards should be commensurate with the invasiveness of the surveillance. However, the self-authorisation procedure in section 22 of the Regulation of Investigatory Powers Act 2000 (RIPA) means that law enforcement agencies do not require judicial approval to obtain broad access to communications data. We feel that this draws the line in the wrong place.

Subscriber Data

5. The vast majority of current requests that will fall under the RIPA s22 self-authorisation regime are for "subscriber information" (such as the name and address of the owner of a particular telephone number or email address). Although hard data is scarce, FIPR estimates that well over a million such requests are made each year.
6. It is clearly unworkable to have the courts deal with such a large number of requests, which only infringe privacy to a limited degree. We therefore suggest that law enforcement agencies should be able to obtain subscriber information on presentation of a written request by a suitably senior officer. However, access to communications data in general should require a judicial warrant.
7. However, the current definition of what is "subscriber information" is extremely confusing. RIPA s21(4)(c) defines it in terms of information that does not fall under (a) and (b), which have turned out to be hard to transpose from their legalistic drafting into real world examples.
8. FIPR recommends that this section of RIPA be rewritten to provide a succinct definition of "subscriber information". The existing (a) and (b) distinctions between

different types of "communications" and "traffic" data serve no useful purpose and should be amalgamated.

9. Subjects of both subscriber and communications data requests should be notified within six months of this access unless a judicial order is made that this notification would prejudice an ongoing investigation. The notification could be sent at little extra cost with subscribers' monthly bills. This will deter abuse, as insiders who corruptly obtain access to data on behalf (for example) of private investigators will very likely be caught if their behaviour is at all persistent. It will also bolster public confidence.

Data Retention

10. Given that communications data can be as sensitive as the contents of communications, proposals to require the retention of large quantities of such data by Communication Service Providers (CSPs) should be viewed in the same light as mandatory retention of communications content.

11. We agree with the European Data Protection Commissioners that "such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights" [2].

12. This was confirmed by a legal opinion obtained by the Information Commissioner, which expressed 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" [3].

13. FIPR believes that the creation of warehouses of communications data will lead to significant abuses of individuals' rights. It is predictable that excuses will be found to trawl through them looking for patterns of behaviour or patterns of association. Such warehouses are exactly the tools needed to create a totalitarian state, and it is foolish in the extreme to create them.

14. The powers encapsulated in Part 11 of the Anti-Terrorism Crime and Security Act 2001 should be allowed to lapse. They have turned out to be unimplementable, and the sense of urgency under which they were enacted can now be seen to be a misunderstanding of how much data the CSPs already have available.

15. In practice, the data retained by CSPs for business purposes (such as itemised phone bills) is enough for Law Enforcement Agencies to do their jobs. Under exceptional circumstances (such as the aftermath of 11 September 2001) it can already be lawfully kept for a slightly longer period of time.

International Cooperation

16. FIPR notes that the Government signed the Council of Europe's Cybercrime treaty in 2001. This means that retained data will need to be provided to foreign law enforcement officials, sometimes only a few minutes after it is collected.

17. FIPR believes that this raises considerable practical difficulties in ensuring that public policy objectives are maintained. The present "Mutual Legal Assistance" regime relies upon an extended timescale to ensure that we do not assist foreign governments whose policy objectives we disagree with - for example, because the offence in question is not an offence here, or because the evidence gathered might be used to secure a conviction leading to capital punishment.

18. The implementation by the UK government should have a firm requirement on dual criminality, and access to retained data by foreign governments should never be automatic. A senior UK law enforcement officer should approve each request.

Summary

19. We recommend a three-tier system. Subscriber data, such as the name and address corresponding to a telephone number, should be available to law enforcement on written request (as at present); communications data, such as the phone numbers a suspect has called or been called from, should be available on a judicial warrant; and the content of communications (such as telephone taps) should only be available with a warrant signed by the relevant Secretary of State (as at present).

20. This will keep the control regime for electronic surveillance broadly in line with the rules already governing physical surveillance, such as routine police enquiries, search warrants, and warrants for the interception of mail.

Ian Brown
Foundation for Information Policy Research
E-mail: ian@fipr.org

[1] <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def30802566360045bf4d/3fddbd098455c3fe802568d90049ac04?OpenDocument>

[2] <http://www.fipr.org/press/020916Commissioners.html>

[3] <http://www.privacyinternational.org/countries/uk/surveillance/ic-terror-o>