

ACCESS TO COMMUNICATIONS DATA

Last summer there was considerable controversy when the Home Secretary brought forward Regulations to regulate access to communications data by non-police and customs enforcement bodies. Despite the Regulations being designed to put in place statutory controls on enforcement bodies such as the Radiocommunications Agency, they were portrayed as a "Snoopers' Charter" by the media and civil rights organisations. This resulted in the Home Secretary withdrawing the Regulations.

The Home Office has now published a public consultation document "Access to Communications Data - Respecting Privacy and Protecting the Public from Crime" - available at www.homeoffice.gov.uk/docs/consult.pdf. In this document the Home Office lists those enforcement bodies, including this Agency, which it is proposed should continue to have access to communications data. The document also proposes measures to be put in place to regulate access to communications data which go beyond those originally incorporated in the Regulation of Investigatory Powers Act 2000. Despite this the proposal that other enforcement agencies be given access to communications data is again attracting adverse criticism. The Home Office therefore considers it is essential that there is also seen to be support for any enforcement agency before they are included in Regulations authorising their access of communications data. The Agency's case for continued access to communications data is attached at Annex A.

In addition to being seriously concerned about losing the ability to access communications data in the course of its criminal investigations, the Agency also has concerns about some of the proposals in the consultation document for regulating access. For the purpose of the consultation communications data has been divided into three categories: traffic data; service use information; and, subscriber information (page 7). The introduction of the so called "double lock", ie introducing another tier of authority, for the purpose of accessing service use information we consider to be introducing an unnecessary level of bureaucracy (pages 26 and 29, para 49). We believe the process will introduce unnecessary delay and cost, especially as the processes for access will be governed by a Statutory Code of Practice. The intention to deny this Agency access to traffic data (page 29, paragraph 48) we consider will impinge on our enforcement ability, especially our work in locating pirate radio studios. Experience has shown that the seizure of a pirate radio studio and subsequent prosecution of those found in the studio has far greater impact than simply seizing the station's remote transmitter. While understanding the need to restrict access to such data, proper consideration does not appear to have been given to the ability to do this by restricting access to only those more serious offences investigated. For example, in the Agency's case this would be only offences related to pirate radio, false distress messages and deliberate radio interference. These offences carry a maximum penalty of two years' imprisonment and unlimited fine.

The Agency would welcome support for its case for having access to all three categories of communications data. This can be done by e-mail to: commsdata@homeoffice.gsi.gov.uk or in writing as detailed on page 8 of the consultation document. Responses are required by 3 June 2003.

REGULATION OF INVESTIGATORY POWERS ACT 2000

ACCESSING OF COMMUNICATIONS DATA BY RADIOCOMMUNICATIONS AGENCY

Background

The Radiocommunications Agency (RA) is responsible for implementing and enforcing the Wireless Telegraphy Act 1949 and associated legislation which is concerned with the management of the civil radio spectrum.

An RA study in 2001 on the economic impact of radio (The Economic Impact of Radio: a Study Produced by the Radiocommunications Agency, February 2001) has demonstrated that the economic value of the radio industry (excluding civil aviation, defence and other public sector use of radio) is some £20 billion per annum at 2000 prices. As the range of radio applications, and the number of users grows, the value of the spectrum to society continues to increase. Radio is the ideal means of meeting society's increasing demand for mobility. There are now 43 million mobile telephone users in the UK, compared to just 4 million in 1995. This underlines the importance of the radio spectrum and the need for its effective management.

It is part of the RA's mission to keep the spectrum clean so that those who have invested in and/or need to use radio may, as far as is practical, do so. In this context one of the Agency's main objectives is protecting authorised radio users, including safety of life services, against interference from illegal radio use. Many illegal radio users, especially pirate radio stations, use telecommunications services to facilitate their operations. The internet is also becoming a common means of selling radio equipment, the use of which would be illegal because of its potential to cause harmful interference to authorised radio use. Without speedy and effective enforcement action the ability of government, business and society to use the radio spectrum is threatened.

Questions and Answers

Q Why is it necessary for the RA to be listed in RIPA for the accessing of communications data?

A The RA has no statutory powers by which it can obtain such data. However, the Secretary of State for Trade and Industry has a statutory duty to enforce the provisions of the Wireless Telegraphy Act 1949 and associated legislation. Contravention of this legislation is a criminal offence. Responsibility for enforcement of this legislation rests with RA, an Executive Agency of DTI. Communications data often becomes evidence during the course of a criminal investigation, either in support or otherwise of the investigation into a suspect. It would also be anomalous for RA to be deprived of access to communications data under RIPA whilst authorised under the DTI umbrella in Schedule 1 of RIPA for the purposes of directed surveillance and use of Covert Human Intelligence Sources.

Q For what purpose does the RA require authority to carry out the accessing of communications data?

A The RA requires to access communications data during the course of its investigation of criminal offences contrary to the Wireless Telegraphy Act 1949. In practical terms this usually occurs when a pirate radio station is broadcasting contact telephone numbers or illegal radio equipment is being offered for sale with a contact telephone number or on a web site.

Q Why is it necessary for the RA to be able to access communications data when investigating Wireless Telegraphy Act offences?

A Illegal radio users often cause harmful interference to other legitimate radio services, including those with safety of life implications such as instrument landing systems at airports. Many businesses also rely on effective radiocommunications in the course of their operations. While the Agency is able to speedily remove individual sources of interference, where they form part of a deliberate pattern of illegal use it is necessary for the Agency to investigate those responsible in order that they may be brought before the courts. The prime example is pirate radio stations where those responsible go to great lengths to avoid detection. Communications data provides information about suspects and locations. This may be evidential in itself or it may be corroborative of other material or indicative, requiring further investigation. Furthermore, just as there is an ongoing convergence between telecommunication and radio systems to provide mobile communications for society those involved in Wireless Telegraphy Act offences are embracing the new technology to facilitate their activities. The RA must be able to access communications data to counter this development.

Q What would be the consequences of the RA not being listed in RIPA.

A The RA would lose an important and basic investigative tool at a time when Parliament is being asked to make those involved in: pirate radio; making hoax radio calls to the safety of life services; and, deliberately interfering with radio communications subject to arrest. It is a core tool from which successful investigations have been instigated and subsequently convictions obtained. Without this tool the RA may well be unable to launch an effective investigation into a repeated source of interference to the radio system of an emergency service or public telecommunications operator.

Q How has communications data previously assisted RA in criminal investigations?

A Communications data has proved to be an invaluable source of evidence in the conviction of individuals for the management of pirate radio stations. In one investigation the ability to obtain subscriber data for 25 telephone numbers resulted in evidence linking those involved in managing, operating and supplying a pirate radio station. Data from Internet Service Providers in tandem with telephone subscriber data has led to the conviction of those responsible for maintaining internet web sites promoting pirate radio.

Subscriber data has also been successfully used to support prosecutions of persons supplying radio equipment which conflicts with UK radio spectrum use and therefore likely to cause harmful interference to authorised radio systems if used.

Q When will communications data be sought?

A Communications data will only be sought where the RA has verified that a telephone number or telecommunications service is being used to facilitate criminal offences contrary to Wireless Telegraphy Act legislation. All RA enforcement officers are trained in the provisions of PACE 1984, CPI 1996 and RIPA 2000 and their respective Codes of Practice.

Q What type of communications data will be sought?

A In addition to **account and subscriber data** when investigating pirate radio stations it can be necessary to seek **location data** to assist in the location of the studio from which the pirate is operating. Where internet web sites are being used to promote pirate radio stations **account and routing data** in relation to those sites is required. Where an internet link is being used to link the pirate radio studio with a remote transmitter **routing data** is required. Where a web site is being used to offer for sale illegal radio equipment **account and routing data** is required.

Q Who in RA will be able to authorise the obtaining of communications data?

A A Range 9 officer (equivalent of Police Superintendent) in the RA Enforcement Policy Unit will be the designated officer except for communications data falling under section 21(4)(c) of RIPA where the designated officer will be a Range 8 (equivalent of Inspector) in the Unit.

Q How will RA seek communication data?

A The RA will seek communication data in accordance with the "Accessing Communications Data Draft Code of Practice." The RA Enforcement Policy Unit will serve as the Single Point of Contact with the telecommunications operators.

Q How often will RA seek to access communications data?

A At present the RA seeks subscriber details on average 30 times a month and account details twice a month. RA infrequently seeks other communications data.

Q Why do the police not investigate these offences?

A We are dealing here with a relatively small number of specialist offences where the principal offence can only be proved by trained specialist radio engineers. The Secretary of State prosecutes on her own behalf for these offences. Given their other priorities the police could not be expected to give priority to investigating such offences despite the serious impact they can have on other authorised radio users.

Q What are the penalties for these offences?

A The maximum penalty on indictment to the Crown Court for illegal radio transmissions is two years' imprisonment, an unlimited fine plus forfeiture of everything used in the offence.

Q **Does this apply to Scotland and Northern Ireland?**

A Wireless Telegraphy Act matters are reserved (that is, not devolved) and as RIPA Chapter II is applicable across the United Kingdom the RA will be able to use these powers in Scotland and Northern Ireland.