

# UK Internet Rights project: [www.internetrights.org.uk](http://www.internetrights.org.uk)

## Fact sheet: Interception and surveillance

### 1. What is interception and surveillance?

Internet communications data provides a very effective method of mapping people's activity. It is possible to produce a map of an individual's networks of electronic communications to identify those with whom they most often communicate, and disclose any particular patterns of activity by individuals or groups. This is surveillance.

Under current legislation on surveillance and interception, the Home Office may require Internet service providers (ISPs) to disclose system logs containing information on:

- the periods of time that certain accounts on the system were active, and the email addresses and network addresses assigned to those users during this period;
- the source and destination addresses of emails logged through the mail system, or through email lists;
- the network addresses of users using the services on the service provider's system, such as web servers, chat rooms and Usenet systems.

Electronic surveillance may be carried out via the Internet, via telephone networks or via the data profiling of individuals. As far as the Internet is concerned, collecting communications *data* is regarded as being less intrusive (and legally less problematic) than intercepting the *content* of the actual communication. A number of UK agencies have powers to obtain such traffic or communications data; these are mostly law enforcement, customs and immigration authorities.

### 2. How is interception covered by the law?

The *Regulation of Investigatory Powers (RIP) Act 2000* amends previous legislation (the Interception of Communications Act 1985 and the Police Act 1997) that enabled the state to intercept communications. The main types of communications it covers are:

- Postal information;
- Telephones;
- Data – such as fax, email or Internet data; and
- Communications data - the information which describes the origin, destination and content of communications.

Interception of these communications cannot take place without "lawful authority".

Section 12 of the RIP Act empowers a Secretary of State to issue notices to require telecommunications and Internet service providers to 'maintain an interception capability' on their systems.

An ISP may contest a notice issued to them to intercept certain communications, for example, on the grounds of implications for data protection or human rights. In this case the minister may seek a court injunction to force the service provider to implement interception.

A key problem for interception is that Internet systems do not assign a specific communications channel to a specific individual. The service provider must therefore either:

- ensure that the target of the interception is given a fixed network address to enable the interception; or
- enable its entire traffic to be monitored. All of its users, not just one targeted individual, would have their communications filtered and stored by the body requiring the interception.

After early objections to a 'black box' at all ISP's servers, the UK Government sought monitoring capabilities by the main data communications and Internet providers. Given the problems involved, and the amount of data produced by communications systems, there is still no agreement between service providers and the Government on how they should implement the requirements of the RIP Act.

Internet service providers have clear responsibilities under the law. They have:

- A contractual responsibility to those whose data they are being asked to pass on, particularly where there is a specific obligation in the contract relating to the protection of personal information from intrusion by any party; and
- An obligation under the *Data Protection Act 1998* to protect data, and ensure that any parties to whom data might be passed provide appropriate protection for that information.

As a party to interception the provider would be liable if the interception was subsequently proven to be unlawful. When presented with a notice for the maintenance of interception under the RIP Act, the service provider may need to obtain legal advice on whether the intrusion is warranted according to the tests under the Act, and whether compliance with these tests is sufficient to justify the breach of the rights of the individual(s) involved.

Activities may also be investigated on the grounds of *common purpose*. This is defined in the *Security Services Act 1996* and the *Police Act 1997*:

- *conduct which constitutes one or more offences shall be regarded as serious crime where it involves conduct by a large number of persons in pursuit of a common purpose.*

The European Cybercrime Convention allows states to monitor the use of the Internet by individuals or groups in order to track the use of the 'Net by criminals and computer hackers. In order to comply with the Convention, all service providers will probably have to log at least some data, under section 12 of the RIP Act. Additional interceptions may also possibly be required, where specific groups are being targeted under the RIP Act, or by other states under the terms of the Convention.

The Cybercrime Convention (Article 17) seeks to create a framework for the preservation of traffic data from specific communications. Collecting traffic data is simpler than collecting voice communications.

### **3. How do laws on interception and surveillance threaten civil liberties?**

There are serious concerns about the level of mass state surveillance that the RIP Act enables. There are three key aspects with significant implications for civil liberties:

- The requirement for maintaining interception at the request of the government;
- The types of surveillance authorised under the legislation; and
- The criteria for the issuing of warrants for surveillance.

Many social action campaigns are nowadays organised via the Internet. The legal principle of 'common purpose' could, for example, be used to collect communications data on people accessing certain Internet sites, or exchanging emails with certain groups. It could be used in relation to civil disobedience activities associated with social or environmental protests, for example.

In cases where interception is very broadly based, covering many people who may have no clear connection with each other, it could be open to challenge on the grounds of maintaining the obligations of service providers as outlined above.