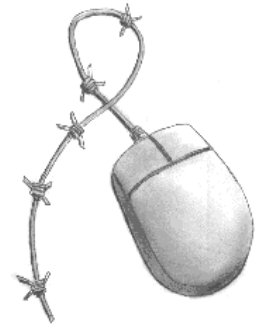


**GreenNet CSIR Toolkit Briefing**

# Interception and Surveillance

## The RIP Act and its implications for individuals and service providers



Written by Paul Mobbs for the  
GreenNet Civil Society Internet Rights Project. Revision 1, April 2003.  
<http://www.internetrights.org.uk/>

Those who control the legislature and the organisations of the state have long sought to discover the activities of persons or groups considered a threat to the maintenance of control or order. Although *intrusive surveillance* was initially developed to monitor the activities of supporters of foreign powers, during the Twentieth Century it was increasingly used against domestic targets; in particular groups such as journalists, trade unionists and public protest groups such as peace campaigners or environmentalists.

The Internet represents a new challenge to those organising state-sponsored surveillance. The UK government (well in advance of other states, who responded after the terrorist attacks of September 11<sup>th</sup> 2001) recently updated laws on surveillance, in order to take account of the new conditions that the use of computers and the Internet has created. The *Regulation of Investigatory Powers (RIP) Act 2000*<sup>1</sup> amends previous legislation (*The Interception of Communications Act 1985* and the *Police Act 1997*) that enabled the state to intercept communications.

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 that are authorised under the legislation; and
- ⊙ The criteria that enable the issuing of warrants for surveillance.

This briefing examines these areas of concern and also takes account of the implications of other relevant legislation, including the *Cybercrime Convention*.<sup>2</sup>

## Interception capabilities under the RIP Act

Monitoring the activities of individuals within society is very difficult. Information, be it letters, phone calls or Internet services, are routed via random paths across telecommunications networks. The only effective way of monitoring individuals' use of the Internet is to tap communications at their source. It is for this purpose that section 12 of the RIP Act empowers a Secretary of State (usually the Minister for the Home Office) to require telecommunications and Internet service providers to "maintain an interception capability" on their systems.

<sup>1</sup> *Regulation of Investigatory Powers Act 2000* - <http://www.legislation.hmsso.gov.uk/acts/acts2000/20000023.htm>

<sup>2</sup> *Cybercrime Convention* - <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=1>

*Interception capabilities* vary according to the nature of the service involved. For organisations who must operate under a licence, such as terrestrial, mobile and cable telephone and postal service providers, it is likely that the maintenance of an interception capability will be specified as part of their licence. If the providers refuse to comply, their license may be revoked at some future date.

Where a service provider does not need a license to operate (such as providers of Internet services) the process becomes more complex. Under the RIP Act *all* service providers must develop and maintain *interception capabilities* through the following procedures:

- Ⓞ Under section 12, paragraph 1, a *notice* is issued by a Minister of the Home Office requiring that a service provider set up *interception capabilities*. The notice specifies the steps required by the minister for the interception of communications (section 12, paragraph 2), and the forwarding of this information to the appropriate body (police, customs, security services, etc.). The technical conditions of the notice are produced by those requiring the interception, who may not of course have the required experience to define the terms of the interception notice. The Act (under section 13) permits the Home Office to establish a *Technical Advisory Body* to provide guidance to the Home Office and to organisations able to request interception.
- Ⓞ The notice is served (section 12, paragraph 3) to a person identified in the notice as being *responsible* for the aspects of the technical conditions specified in the notice. That person may contest (section 12, paragraph 5) whether the terms of the notice are technically feasible or correct in the modifications to systems required by the minister. In this case the notice is referred to the Technical Advisory Body for a ruling.
- Ⓞ Although the general assumption in the Act is that the notice will be complied with, it is open to the service provider to refuse to comply. In this case the minister may, after consultation with all parties involved, seek a court injunction to force the service provider to implement interception. Again, there are means whereby the service provider may contest the validity of interception notice (see *criteria for issuing notices* below). A provider may contest the notice, for example, on grounds of the implications for data protection or human rights. If the injunction is confirmed by the court then the service provider must comply or face proceedings for contempt of court (for which the penalties are very strict).
- Ⓞ The duration of the intercept is specified as part of the conditions provided with the notice. There is no reason why the intercept could not be permanent (see the paragraph on the *Cybercrime Convention* below), or that it could be renewed or extended by further notices issued by the minister.
- Ⓞ Part or all of any costs incurred by the service provider as part of the maintenance of interception may be refunded, at the discretion of the Minister (under section 14).

Under the system enabled by the *Interception of Communication Act 1985*, warrants for interception granted by the Home Secretary identified specific individuals, or organisations, and lasted for a specific period of time. The RIP Act is less precise, and more wide-ranging, in this respect.

The operation of Internet systems does not assign a specific communications channel for a specific individual. Most people who connect to the Internet are given a different *numeric network address*<sup>3</sup> each time they connect. Therefore,

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

<sup>3</sup> See GreenNet CSIR Toolkit Briefing no. 1, *Introduction to the Internet*.

Although most parts of the RIP Act have been brought into force now, the monitoring of telecommunications networks is still a problem for the government. After early objections to a 'black box at all service provider's servers', the government moved 'upstream', to seek monitoring capabilities at the main data communications and Internet providers. But, given the problems involved, and the scale of data that is 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.

## The Cybercrime Convention

The UK led the negotiations on the Council of Europe's *Cybercrime Convention*<sup>4</sup>. The purpose of the Convention is to allow states to monitor the use of the Internet by individuals or groups. The aim is to track the use of the 'Net by criminals and computer hackers, but in actuality the use of electronic networks by anyone is open to scrutiny.

To enable this monitoring, the communications data (that is, information on the origin and destination of *data packets* transmitted across the 'Net) created as people use the Internet must be logged and stored, and then kept as part of a database that enables the extraction of information required by the law enforcement bodies of the states involved. It is likely that, in order to comply with the Convention, all service providers will have to log at least some data, under orders created under section 12 of the RIP Act. It may be that, as well as this day-to-day monitoring and logging, additional interceptions will be required where specific groups are being targeted under the interception powers of the RIP Act, or by other states under the terms of the Cybercrime Convention.

## Types of surveillance

The main types of telecommunications covered by the RIP Act are:

- Ⓣ *Postal information* - the carriage of documents;
- Ⓣ *Telephony* - the use of telephones to carry voice communications;
- Ⓣ *Data* - the use of telecommunications systems to carry fax, email or Internet data; and
- Ⓣ *Communications data* - the information created as part of the transactions of telephony and data that described the origin, destination and content of the communication.

Interception of these communications cannot take place without "lawful authority". The inclusion within the Act of *communications data* brings under the law services not specifically covered by previous legislation, such as email and other Internet communications.

The Act makes a distinction between public and private telecommunications systems:

- Ⓣ Owners of private telecommunications systems are considered to have a right to monitor their own systems. It is an offence to intercept a communication if you are not the owner, or are not authorised by the owner to do so.
- Ⓣ It is an offence to intercept communications from a public telecommunications system (section 1, paragraph 1) unless you are an authorised person with a warrant, or unless you are an engineer maintaining the telecommunications system (engineers must not divulge the content of any communications they may intercept as part of their work).

---

<sup>4</sup>*Cybercrime Convention* - <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=1>

## Monitoring traffic data

For intelligence purposes, the content of communications is sometimes not as important as the data created by communication. Communications data can be used to 'map' connections and associations between individuals, and between individuals and organisations. Combined with other information, such as travel information (assisted by the location information provided by mobile phones) or credit/debit card purchases, communications data can tie together an individuals activities.

The Cybercrime Convention (Article 17) seeks to create a framework for the preservation of traffic data from *specific communications*. Collecting traffic data is a cruder process than collecting voice communications. The treaty defines traffic data as:

- ⊙ a code indicating a network, equipment or individual number or account, or similar identifying designator, transmitted to or from any designated point in the chain of communication;
- ⊙ information on the time, date, size, and duration of a communication;
- ⊙ in any mode of transmission (including but not limited to mobile transmissions), any information indicating the physical location to or from which a communication is transmitted.

Section 2(9) of the RIP Act provides a cryptic but more precise definition that not only specifies the source and destination of communications, but also, in subparagraph (d), the nature or name of the file or information communicated:

*(9) In this section "traffic data", in relation to any communication, means-*

- (a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,*
- (b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,*
- (c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and*
- (d) any data identifying the data or other data as data comprised in or attached to a particular communication,*

*but that expression includes data identifying a computer file or computer program, access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.*

Traffic data is kept by telecommunications companies in order to create itemised bills. The traffic data of an individual will contain links to many others who, in all likelihood, have nothing to do with that individual's activities. Even so, these people may in turn be subject to some form of surveillance, most likely using their traffic data. In this way, using software already available to police forces and the government, it is possible to produce a map of an individual's networks of communications, to identify those with whom an individual most often communicates, and disclose any particular patterns of activity by an individual, or group of individuals.

Communications data provides a very effective method of mapping people's activity. It is likely that traffic data will be initially requested from service providers as part of the interception capabilities requirements of the RIP Act.

The Cybercrime Convention provides for the collation and sharing of such information between signatories of the Convention. This means that a priority will be to secure the collection and archiving of this information

as soon as possible. It is likely that the Home Office will require the disclosure of 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.

Much of this information is already logged automatically by server systems; some of it is archived, and some simply deleted. Such information is routinely used for checking system security, and for identifying whether there have been attempts to gain unauthorised access to the server. It is also a *low volume* activity in terms of the effort required to collect and forward it to an agency charged with collection.

The Home Office is likely to seek to collect information on traffic data first, therefore, before proceeding to force more complex disclosure of data streams (such as forwarding a particular user's entire data transactions to a government server).

## The criteria for issuing interception warrants

The criteria specified in the section 5(3) of the RIP Act for issuing warrants are fairly straightforward:

- (3) *Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary-*
- (a) *in the interests of national security;*
  - (b) *for the purpose of preventing or detecting serious crime;*
  - (c) *for the purpose of safeguarding the economic well-being of the United Kingdom; or*
  - (d) *for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.*

... but in relation to communications data a slightly different set of criteria apply (under section 22(2)),

- (2) *It is necessary on grounds falling within this subsection to obtain communications data if it is 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; or*
  - (h) *for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.*

The reason for this difference is that the collection of communications data is regarded as being less intrusive than the interception of the content of the actual communication. It is also regarded as being

available for wider use by the state.

When these proposals went before Parliament for commencement in 2002, there was an outcry because of the range of bodies who would be able to obtain traffic data. After various protestations by the Home Office, they eventually agreed a slimmed down list of agencies who could access traffic data - mainly those related to law enforcement and customs/immigration.

## Common purpose

It could be argued that if records of communications data are databased with those of other individuals, collection may be just as invasive of a person's social or political activities as interception. This is particularly true where people are being investigated on the grounds of *common purpose*.

*Common purpose* is defined in clauses contained in the *Security Services Act 1996*<sup>5</sup> and the *Police Act 1997*<sup>6</sup>. These Acts state that...

*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.*

This covers ordinary criminal activity, but it would also cover the civil disobedience activities associated with social or environmental protests. As many of these campaigns are organised via the Internet, the collection of communications data for people accessing certain Internet sites, or exchanging emails with certain groups, could be used to clamp down on many of the kinds of social and environmental campaign that have we have seen in recent years.

## Liabilities of service providers

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
- ⊙ There is an obligation under the *Data Protection Act 1998*<sup>7</sup> to protect data, and ensure that any parties to whom data might be passed provide appropriate protection for that information.

When considering a request for interception or traffic data, interpreting these obligations will depend upon the scope of the interception sought. The RIP Act, however, provides no immunity for a service provider who wrongly discloses personal information as part of an interception.<sup>8</sup> As a party to interception the provider would be liable if the intercept 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.

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

<sup>5</sup>Section 2, *Security Services Act 1996* - <http://www.legislation.hmso.gov.uk/acts/acts1996/1996035.htm>

<sup>6</sup>Section 93, *Police Act 1997* - <http://www.legislation.hmso.gov.uk/acts/acts1997/1997050.htm>

<sup>7</sup>For more information see the GreenNet CSIR Briefing no.2 on *Data Protection*

<sup>8</sup>See section 79 of the RIP Act in relation to the liability of corporate organisations.

obligations of the service provider as outlined above. Where an individual is the subject of an interception warrant, it may be more difficult to challenge the basis of the interception, assuming that evidence to justify the intrusion into personal privacy will be specific to the circumstances.

## Further work

This briefing has been written in the context of the legal framework currently in force in the UK. If you live outside the UK you will need to make yourself aware of the procedures operating in your own country. Key points you will need to find out are:

- ⑩ Is your government a party to the Cybercrime Convention, if so, what laws have they put forward to implement the requirements of the treaty for monitoring and surveillance?
- ⑩ What current procedures or laws govern the interception of private communications, and how do they operate?
- ⑩ Are there any laws in your country that require Internet service providers to turn over the communications of a person to the police or security services?
- ⑩ Are there any appeals or review procedures for Internet service providers who wish to oppose interception, or for individuals who have been the subject of interception?

You should also contact any civil liberties organisations operating in your country. They may be able to provide you with much of the information you need on laws relating to surveillance and interception of communications.

## The GreenNet Internet Rights Project

GreenNet<sup>9</sup> is the UK member of the Association for Progressive Communications<sup>10</sup> (APC), and is leading the European section of the APC's Civil Society Internet Rights Project<sup>11</sup>. The primary goal of this project is to provide the resources and tools necessary to defend and expand space and opportunities for social campaigning work on the Internet against the emerging threats to civil society's use of the 'Net. This involves developing ways and means of defending threatened material and campaigning, as well as lobbying to ensure a favourable legal situation for free expression on issues of public interest.

Until recently, the social norms of Internet communities, together with a very open architecture based on supporting these norms, regulated the Internet, and was responsible for its openness. The main forces of regulation now, however, are the business sector and government legislation. Corporations and governments are pressing for fundamental changes in legislation and in the architecture of the Internet. Unless challenged, these moves could radically change the nature of the 'Net, making it a place of oppressive controls instead of freedom and openness. It is in this context that APC's Internet Rights project is being developed.

This briefing is one in a series<sup>12</sup> that document different aspects of work and communication across the Internet. Although written from the perspective of the UK, much of its content is applicable to other parts of Europe. There is continuing work on these issues, as part of the European project. If you wish to know

---

<sup>9</sup>GreenNet - <http://www.gn.apc.org/>

<sup>10</sup>APC - <http://www.apc.org/>

<sup>11</sup>CSIR Project - <http://rights.apc.org/>

<sup>12</sup><http://www.internetrights.org.uk/>

more about these briefings, or the European section of the APC Civil Society Internet Rights Project, you should contact GreenNet. You should also check the APC's web site to see if there is already a national APC member in your country who may be able to provide local help, or with whom you may be able to work to develop Internet rights resources for your own country.