These notes refer to the Regulation of Investigatory Powers Act 2000 (c.23) which received Royal Assent on 28 July 2000

REGULATION OF INVESTIGATORY POWERS ACT 2000

EXPLANATORY NOTES

COMMENTARY ON SECTIONS

"Wireless telegraphy" and "apparatus" are defined in Section 81.

For "while being transmitted", see subsection (7).

29. The exclusion in *subsection (3)* for communications broadcast for general reception covers television and radio. It does not extend to pager or mobile phone signals; the interception of those communications is governed by the Act.

30. *Subsection (4)* explains how the territorial limitation works in Section 1(1), (2) and (3), each of which extends only to interception "at any place in the United Kingdom".

31. *Subsection (5)* excludes from the definition of interception in subsection (2) any conduct which relates only to the traffic data comprised in or attached to a communication (expanded in subsection (9)), or which relates only to so much of the content of the communication as is necessary in order to identify this traffic data.

32. *Subsection (7)* expands the phrase "while being transmitted", which is used in the tailpiece of subsection (2). The times when a communication is taken to be in the course of its transmission include any time when it is stored on the system for the intended recipient to collect or access. This means that an interception takes place, for example, where an electronic mail message stored on a web-based service provider is accessed so that its contents are made available to someone other than the sender or intended recipient, or where a pager message waiting to be collected is accessed in that way. However, if a stored communication is accessed in this way, that conduct may be lawful by virtue of Section 1(5)(c).

33. *Subsection (9)* sets out the meaning of "traffic data". It covers, for example, subscriber information under paragraph (a), and routing information under paragraph (b). Paragraph (c), which must be read with subsection (10) (which operates on subsection (5)), addresses what is commonly referred to as "dial through fraud". It covers, for example, data entered by a user seeking to arrange for a telephone call to be accepted and routed by a telecommunication system. Finally, paragraph (d) catches the data which is found at the beginning of each packet in a packet switched network which indicates which communications data attaches to which communication. The tailpiece to the definition puts beyond doubt that in relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic data may identify a server but not a website or page.

34. The tailpiece to the definition puts beyond doubt that in relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic may identify a server but not a website or page.

35. In s*ubsection (10),* paragraph (a) is explained above. Paragraph (b) ensures that the references to data being attached to a communication in subsection (5) include data which may not be transmitted simultaneously with the contents of that communication; for example, the data which identifies the number of the person making a telephone call (the calling line identifier).

Section 3: Lawful interception without an interception warrant

36. This Section authorises certain kinds of interception without the need for a warrant under Section 5, namely where one or more parties to a communication have consented to the interception, conduct is in relation to the provision or operation of services, or conduct takes place with the authority of a person designated for the purposes of the Wireless Telegraphy Act 1949.

37. *Subsection (1)* authorises interception where there are reasonable grounds for believing that both the sender and the intended recipient of a communication have consented to its interception.

38. *Subsection (2)* authorises interception where:

- either the sender or intended recipient of a communication has consented to its interception; and
- the interception has been authorised under Part II (see Section 48(4)).

39. This situation might arise where a kidnapper is telephoning relatives of a hostage, and the police wish to record the call in order to identify or trace the kidnapper. The operation will be authorised as surveillance, rather than by means of an interception warrant.

40. *Subsection (3)* authorises interception where it takes place for the purposes of providing or operating a postal or telecommunications service, or where any enactment relating to the use of a service is to be enforced. This might occur, for example, where the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown.

41. *Subsection (4)* authorises interception where it is authorised by a designated person and is undertaken for purposes connected with certain parts of the Wireless Telegraphy Act 1949. Section 5 of that Act, as amended by Section 73 of this Act, makes provision for interception of wireless telegraphy under the Secretary of State's authority.

For "designated person", see Section 5(12) of the 1949 Act, inserted by Section 73.

Section 4: Power to provide for lawful interception

42. This Section lists the cases where a power may be exercised to provide for lawful interception without the need for a warrant under Section 5: under an international mutual assistance agreement; under regulations made by the Secretary of State to permit certain kinds of interception in the course of lawful business practice; under prison rules; in hospital premises where high security psychiatric services are provided; and in state hospitals in Scotland.

43. *Subsection (1)* enables the Secretary of State to make regulations specifying the conditions under which communication service providers may be authorised to use telecommunications systems located in the United Kingdom to intercept the communications of subjects on the territory of another country in accordance with the law of that country. The effect of paragraphs (d) and (e) is that regulations must be in operation before interception is authorised under this subsection. This subsection applies only where the subject of the interception is in the country whose competent authorities issued the interception warrant. The inclusion of the phrase "or who the interceptor has reasonable grounds for believing is in a country or territory outside the

United Kingdom" reflects the fact that it will not always be possible to be certain about the precise location of the interception subject.

44. In practice, the "interceptor" is likely to be a communication service provider located in the UK which is either providing a public telecommunications service to another country or is in a business relationship with another communication service provider providing such a service.

45. This subsection will allow the United Kingdom to comply with Article 17 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. This Article is intended to allow operators of satellite communications systems to use a ground station in one Member State to facilitate interception using a "service provider" (in practice, a communications service provider which is in a business relationship with the satellite operator) located in another Member State. The "service provider" and the subject of interception are required to be in the same Member State.

46. *Subsection (2)* makes provision for the Secretary of State to make regulations describing the kinds of interception which it is lawful to carry out in the course of the carrying on of a business. Article 5 of Directive 97/66/EC (the Telecommunications Data Protection and Privacy Directive) exempts from its prohibition on interception.

""Any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication".

47. *Subsection (4)* makes reference to prison rules. Sections 47 and 39 of the respective Acts provide for the Secretary of State to make rules for the regulation and management of prisons and similar institutions, and for the classification, treatment, employment, discipline and control of people detained in them. The rules must, by virtue of section 6 of the Human Rights Act 1998, be compatible with the Convention rights.