

REGULATION OF INVESTIGATORY POWERS ACT 2000

EXPLANATORY NOTES

COMMENTARY ON SECTIONS

"International mutual assistance agreement" is defined in Section 20

24. *Subsection (5)* explains the circumstances in which interception of communications is lawful, and where the offences and the liability created in subsections (1), (2) and (3) do not therefore apply. These are where the interception is not authorised by an interception warrant yet falls into one of the exceptions described in Sections 3 or 4 (for example where all parties to the communication consent to the interception); where there is an interception warrant; or where an existing statutory power is used in order to obtain stored communications. The latter case covers circumstances where, for example, a person has been arrested in possession of a pager, and the police have reason to believe that the messages sent previously to that pager may be of assistance in the case. In this case they would be able to seek from a circuit judge an order under Schedule 1 to the Police and Criminal Evidence Act 1984 for the stored data to be produced.
25. *Subsection (6)* explains the circumstances in which interception falls outside the scope of the criminal offence introduced by subsection (2). This conduct attracts civil liability by virtue of subsection (3). Essentially, subsection (6) allows a person with a right to control a private telecommunication network to intercept on their own network without committing an offence. Examples of this type of activity are an individual using a second handset in a house to monitor a telephone call, and a large company in the financial sector routinely recording calls from the public in order to retain a record of transactions. Each of those cases may or may not give rise to civil liability, depending on the application of sections 3 and 4.
26. *Subsection (7)* specifies the maximum penalties for the offences created by this section. The statutory maximum referred to in paragraph (b) is currently £5000. There is no upper limit to a fine on conviction in the Crown Court.

Section 2: Meaning and location of "interception" etc

27. This Section sets out the definitions of telecommunications and postal services and systems relevant to the Act, and assists in the interpretation of interception and other related matters. For the interpretation of other terms used in Chapter I of Part I, see sections 20 and 81.

"Private telecommunication system" is defined as any telecommunication system which is not a public telecommunication system; but is attached to such a system. This means that an office network, linked to a public telecommunication system by a private exchange, is to be treated as a private system. Interception of such a system other than by the system controller or with his consent is a criminal offence. An entirely self-standing system, on the other hand, such as a secure office intranet, does not fall within the definition.

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

28. *Subsection (2)* explains what constitutes the interception of a communication in the course of its transmission by means of a telecommunication system. This is relevant to the criminal offence and the civil liability in Section 1; and to the issuing of a warrant by the Secretary of State which authorises or requires interception in Section 5. There is no equivalent definition for postal interception.