

These notes refer to the [Regulation of Investigatory Powers Bill](#) as introduced in the House of Commons on 9th February 2000 [Bill 64]

I. REGULATION OF INVESTIGATORY POWERS BILL

II. EXPLANATORY NOTES

INTRODUCTION

1. These explanatory notes relate to the Regulation of Investigatory Powers Bill as introduced in the House of Commons on 9 February 2000. They have been prepared by the Home Office in order to assist the reader of the Bill and to help inform debate on it. They do not form part of the Bill and have not been endorsed by Parliament.
2. The notes need to be read in conjunction with the Bill. They are not, and are not meant to be, a comprehensive description of the Bill. So where a clause or part of a clause does not seem to require any explanation or comment, none is given.

SUMMARY AND BACKGROUND

3. The main purpose of the Bill is to ensure that the relevant investigatory powers are used in accordance with human rights. These powers are:
 - the interception of communications;
 - intrusive surveillance (on residential premises/in private vehicles);
 - covert surveillance in the course of specific operations;
 - the use of covert human intelligence sources (agents, informants, undercover officers);
 - the acquisition of communications data (eg billing data);
 - access to encrypted data.
4. For each of these powers, the Bill will ensure that the law clearly covers:
 - the purposes for which they may be used;
 - which authorities can use the powers;
 - who should authorise each use of the power;
 - the use that can be made of the material gained;
 - independent judicial oversight;
 - a means of redress for the individual.

5. Not all of these matters need be dealt with in this Bill - in many cases existing legislation already covers the ground. The Bill will work in conjunction with existing legislation, in particular the Intelligence Services Act 1994, the Police Act 1997 and the Human Rights Act 1998.

III. OVERVIEW

6. The Bill is in five parts.

IV. *Interception of Communications and the Acquisition and Disclosure of Communications Data*

7. The existing arrangements for the interception of communications are established in the Interception of Communications Act 1985. Significant changes to that Act were proposed in the Consultation Paper "Interception of Communications in the United Kingdom" (CM 4368) published on 22 June 1999. A summary of the responses, along with copies of responses, is available at <http://www.homeoffice.gov.uk/oicd/constlist2.htm>.

8. This Bill repeals the 1985 Act and provides for a new regime for the interception of communications incorporating the changes proposed in the consultation paper. These changes go beyond what is strictly required for human rights purposes and provide also for the changed nature of the communications industry since 1985.

9. The provisions also implement Article 5 of Council Directive 97/66 of 15 December 1997, known as the "Telecommunications Data Protection Directive", which requires member states to safeguard the confidentiality of communications.

V. *Surveillance and Covert Human Intelligence Sources*

10. This Part provides a statutory basis for authorisation and use by the security and intelligence agencies, law enforcement and other public authorities of covert surveillance, agents, informants and undercover officers. It will regulate the use of these techniques and safeguard the public from unnecessary invasions of their privacy.

VI. *Investigation of Electronic Data Protected by Encryption etc*

11. This Part contains provisions to maintain the effectiveness of existing law enforcement powers in the face of increasing criminal use of encryption. Specifically, it will introduce a power to demand access to protected (encrypted) data.

12. The first consultation on this subject was undertaken by the previous administration in March 1997. A broader consultation "Building Confidence in Electronic Commerce: A Consultation Document was launched on 5 March 1999 (URN 99/642). Finally, provisions very similar to these were published as Part III of the draft Electronic Communications Bill issued for consultation on 23 July 1999 (CM 4419).

VII. *Scrutiny of Investigatory Powers and Codes of Practice*

13. This Part ensures that there will be independent judicial oversight of powers where necessary.

14. It also establishes a Tribunal as a means of redress for those who wish to complain about the use of the powers.

15. Finally, it provides for the Secretary of State to issue Codes of Practice covering the use of the powers covered by the Bill.

VIII. *Miscellaneous and Supplemental*

16. This Part makes minor amendments to Part III of the Police Act 1997 in the light of operational experience and extends those provisions to the Ministry of Defence Police, the British Transport Police and the Service Police.

17. Both the Police Act and the Intelligence Services Act 1994 are amended to ensure authority is given for interference with property or wireless telegraphy only where it is proportionate to do so.

IX. COMMENTARY ON CLAUSES

Clause 1: Unlawful and authorised interception

18. This Clause creates the offences of unlawful interception and a separate tort of unlawful interception, explains the locations and circumstances in which each is applicable, and the circumstances in which interception is lawful.

19. *Subsection (1)* sets out the circumstances in which interception of a communication being transmitted by a public postal service or public telecommunication system is a criminal offence. The offence is similar to that created by Section 1 of the Interception of Communications Act 1985, which this Bill repeals.

"Public postal service" and "public telecommunication system" are defined in Clause 2(1).

20. *Subsection (2)* sets out the circumstances in which interception of a communication being transmitted by a private telecommunication system is an offence, and cross refers to subsection (6) where the circumstances in which such interception is not a criminal offence are explained.

"Private telecommunication system" is defined in Clause 2(1)

21. *Subsection (3)* creates the tort of unlawful interception on a private telecommunications network, the locations at which the tort applies and the persons who may bring an action under this subsection, namely the sender, recipient or intended recipient. For example, where an employee believes that their employer has unlawfully intercepted a telephone conversation with

a third party, either the employee or the third party may sue the employer. Clause 4(2) outlines circumstances in which interception by an employer may be lawful.

22. *Subsection (4)* applies to international agreements on mutual assistance in connection with the interception of communications which are designated under this subsection by an order made by the Secretary of State (negative resolution, see Clause 68). This will enable the United Kingdom to comply with the interception provisions in the draft Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. Although no similar agreements are currently under negotiation, this subsection will provide flexibility for the future.

23. In respect of agreements designated by this order, this subsection places the Secretary of State under a duty to ensure that no request for mutual assistance to intercept communications is made unless it has lawful authority in accordance with subsection (5). In practice, for the purposes of the draft Convention on Mutual Assistance in Criminal Matters, this will require the Secretary of State to issue an interception warrant under Clause 5(1)(b) prior to any request for mutual assistance.

X. *"International mutual assistance agreement" is defined in Clause 19*

24. *Subsection (5)* explains the circumstances in which interception of communications is lawful, and where the offences and the tort 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 Clauses 3 or 4 (for example where all parties to the communication consent to the interception); where an interception warrant is in existence; or where an existing statutory power is used in order to obtain stored communications. In the latter case, this covers circumstances such as where 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 apply 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)* cross refers to subsection (2) and explains the circumstances in which interception of communications activity may fall outside the scope of the criminal offence but within that of the civil tort. Essentially, it 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.

26. *Subsection (7)* specifies the maximum penalties to which a person who is found guilty of the criminal offence of unlawful interception may be sentenced; if he is found guilty in a Magistrates' Court he may be fined up to the statutory maximum (currently £5000); in the Crown Court he may be imprisoned for a period up to two years, or may be fined, or both. There is no upper limit to a fine on conviction in the Crown Court.

XI. *Clause 2: Meaning and location of "interception" etc*

27. This Clause sets out the definitions of telecommunications and postal services and systems relevant to the Bill, and assists in the interpretation of interception and other related matters.

"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 by other than 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.

28. *Subsection (2)* outlines the cases in which an interception of a communication takes place. This is relevant to the criminal offence and the tort in Clause 1; and to the issuing of a warrant by the Secretary of State which authorises or requires interception in Clause 5. The definition only applies to interception of communications on telecommunication systems.

XII. "Wireless telegraphy" and "apparatus" are defined in Clause 71.

29. Subsection (4) explains the phrase "in the United Kingdom" in Clause 1(1), (2) and (3). Either (a) or (b) must apply for the offence in 1(2) to occur.

30. *Subsection (5)* excludes from the definition of interception in subsection (2) any conduct which relates only to the communications 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 communications data.

31. *Subsection (7)* expands the phrase "while being transmitted", which is used in the tail 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 disclosed to someone other than the sender or intended recipient, or where a pager message waiting to be collected is so disclosed. Provision is made for such disclosures in Clause 1(5)(c).

32. *Subsection (9)* 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).

XIII. Clause 3: Lawful interception without an interception warrant

33. This Clause authorises certain kinds of interception without the need for a warrant under Clause 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 the Secretary of State in relation to the Wireless Telegraphy Act 1949.

34. *Subsection (1)* authorises interception where both the sender and the intended recipient of a communication have consented to its interception. This situation applies to the overt use of a telephone answering machine, for example.

35. *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 (Clause 27).

36. This situation might arise where a kidnapper is telephoning relatives of a hostage, and the police wish to record the call for the purpose of preventing or detecting serious crime.

37. *Subsection (3)* authorises interception where it takes place for service provision or operation purposes, 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.

38. *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 Clause 64, makes provision for interception of wireless telegraphy under the Secretary of State's authority.

"Designated person" is defined in Clause 64(11).

XIV. Clause 4: Power to provide for lawful interception

39. This Clause lists the cases where a power may be taken to provide for lawful interception without the need for a warrant under Clause 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; and in hospital premises where high security psychiatric services are provided.

40. *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. 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.

41. 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.

42. This subsection will allow the United Kingdom to comply with Article 17 of the draft Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. This Article, as currently drafted, 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.

43. *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 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.

44. *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.

45. *Subsection (5)* makes reference to directions under section 17 of the National Health Service Act 1977. Under section 4 of that Act the Secretary of State has a statutory duty to provide hospital services for persons who are liable to be detained under the Mental Health Act 1983 and in his opinion require treatment under conditions of high security on account of their dangerous, violent or criminal propensities. Under section 17 the Secretary of State may give directions to NHS bodies providing high security psychiatric services about their exercise of any functions. The directions must be compatible with Convention rights.

"high security psychiatric service" and "hospital premises" are defined in subsection (7).

XV. *Clause 5: Interception with a warrant*

46. This clause allows for interception to be carried out when an interception warrant has been issued by the Secretary of State and sets out the grounds on which a warrant may be issued. For "addressed", see clause 7(3).

47. *Subsection (1)(a)* authorises the interception of communications sent by means of a postal service or telecommunications system.

"Interception" is described in Clause 2.

48. *Subsection (1)(b)* allows the Secretary of State to issue an interception warrant for the purpose of making a request for assistance under an international mutual assistance agreement designated under Clause 1(4).

49. *Subsection (1)(c)* allows the Secretary of State to issue an interception warrant for the purpose of complying with a request for assistance under an international mutual assistance agreement designated under Clause 1(4).

50. *Subsection (1)(d)* allows for the disclosure of intercepted material and related communications data in a manner described by the warrant.

"Postal service" and "telecommunications system" are defined in clause 2(1).

"Related communications data", "intercepted material" and "international mutual assistance agreement" are defined in clause 19.

51. *Subsection (2)* requires that the Secretary of State may not issue an interception warrant unless he is satisfied that the warrant is necessary on grounds set out in subsection (3). *Subsection (2)(b)* introduces a proportionality test. Proportionality, under Convention case-law, is an essential part of any justification of conduct which interferes with an Article 8 right to privacy.

52. *Subsection (3)* sets out the grounds on which the Secretary of State may issue warrants. He may not do so unless he considers that the warrant is necessary on one of those grounds. It would not therefore be sufficient for him to consider that a warrant might be useful in supplementing other material, or that the information that it could produce could be interesting. The word 'necessary' reflects the wording of Article 8 of the Convention - "necessary in a democratic society".

53. *Subsection (3)(a)* "in the interests of national security" is the term used in Article 8 of the Convention. "National security" is not defined in the Bill, as it is not in any other legislation in which it is used.

54. *Subsection (3)(b)* "for the purpose of preventing or detecting serious crime". This reflects the provision in Article 8 "for the prevention of disorder and crime", but is qualified by the word "serious".

"Serious crime" is defined in clause 71(2) and (3).

55. *Subsection (3)(c)* "for the purpose of safeguarding the economic well-being of the United Kingdom" - this provision should be read in conjunction with Clause 5(5) which introduces an important limitation on its effect. Under Clause 5(5) the Secretary of State is prevented from considering a warrant necessary under Clause 5(3)(c) unless the information to be acquired under it is information relating to acts or intentions of persons outside the British Islands. A warrant could not therefore properly be issued in relation to purely domestic events. As with the other purposes for which interception is permitted, Clause 5(3)(c) closely reflects the wording of Article 8 of the Convention, though the term in Article 8 is understood to have a broader meaning and would include, for example, the protection of tax revenues. The limitation imposed in 5(5) is not found in the Convention.

56. *Subsection (3)(d)* ensures that the Secretary of State will not issue an interception warrant for the purpose of an international mutual assistance agreement designated under Clause 1(4) unless he is satisfied that the circumstances are equivalent to those in which he would issue a warrant for the prevention or detection of serious crime.

"International mutual assistance agreement" is defined in Clause 19: it must be designated for the purposes of clause 1(4).

57. *Subsection (4)* adds a further requirement upon the Secretary of State, in addition to those contained within subsections (2) and (3).

58. *Subsection (6)(a)* provides for the interception of such other communications (if any) as it is necessary to intercept in order to intercept the communications authorised by the warrant. This provides for situations where other communications are unavoidably intercepted in the course of intercepting the warranted communications.

59. *Subsection (6)(b)* allows for related communications data to be obtained during the course of interception. For example, this could cover the actions of a provider of communications services in effecting the requirements of a warrant where the intercepted material comprises both communications and related communications data.

60. *Subsection (6)(c)* allows for assistance in giving effect to the warrant to be provided to a person to whom the warrant is addressed; for example, by a person listed in Clause 11(4).

XVI. Clause 6: Application for issue of interception warrants

61. Clause 6 describes the persons who may apply for warrants.

XVII. Clause 7: Issue of warrants

62. Clause 7 describes the persons who may sign interception warrants and the circumstances in which they may do so.

63. The combined effect of *subsections (1) and (2)* is that the warrant must be signed by the Secretary of State unless the case is either urgent or the purpose is to comply with a request for mutual assistance where the subject of the interception and the competent authority making the request are outside the United Kingdom.

64. In urgent cases a warrant may be signed by a senior official. The procedure in urgent cases has three elements:

- the senior official who signs the warrant must be expressly authorised by the Secretary of State to do so (under subsection (2));
- that express authorisation must be in relation to that particular warrant (subsection (2)(a)); and
- under *subsection (4)(a)* the official who signs the warrant must endorse on it a statement that he has been expressly authorised by the Secretary of State to sign that particular warrant.

65. Thus, even where the urgency procedure applies, the Secretary of State must have given personal consideration to the application in order to give instructions to a senior official for the signing of that particular warrant, which will be limited in duration to five working days.

"Senior official" is defined in Clause 71(1).

"International mutual assistance agreement" is defined in Clause 19.

66. *Subsection (2)(b)* allows an interception warrant to be issued under the hand of a senior official for the purpose of complying with a request for mutual assistance under an international mutual assistance agreement (designated under Clause 1(4)) in circumstances in which the subject of the interception and the competent authority making the request are outside the United Kingdom.

67. This will allow the United Kingdom to comply with the requirements of Article 16 of the draft Convention on Mutual Assistance in Criminal Matters. Article 16 includes the situation where the United Kingdom is requested to issue an interception warrant to the operator of a satellite ground station in the United Kingdom for the purpose of intercepting a satellite telephone being used on the territory of another Member State. Article 16 enables such warrants to be issued by the requested Member State (in this case, the United Kingdom) "without further formality" provided the competent authorities of the requesting Member State have already issued an interception order against the subject of interception. Since no decision is being made on the merits of the case, and the purpose of the warrant is solely to require the satellite operator to provide technical assistance to the other Member State, it is considered appropriate for these warrants to be issued by senior officials rather than the Secretary of State.

68. *Subsection (3)* specifies to whom the warrant must be addressed (see list in Clause 6(2)) and that in the case of a warrant under the hand of a senior official it contains one of the statements in subsection (4). The statement in subsection (4)(a) relates to urgent cases and is explained above.

69. *Subsection (4)(b)* applies only in cases where the warrant is issued in connection with a request made under an international mutual assistance agreement. It ensures, in conjunction with *subsection (5)*, that a statement of the purpose of the warrant is recorded, including the fact that it appears, at the time of the issue of the warrant, that the interception subject is outside the United Kingdom.

XVIII. Clause 8: Contents of warrant

70. This Clause describes the two different forms which a warrant may take.

71. *Subsections (1)(a) and (b)* require that either the person or the set of premises to be intercepted is named or described on the face of the warrant.

"Person" is defined in Clause 71(1).

"Interception" is described in Clause 2.

72. *Subsection (2)* requires that a warrant must include one or more schedules setting out how the communications from or intended for the person described in the warrant, or originating on or intended for transmission to the premises named in the warrant, are to be identified.

"Communication" is defined in clause 71(1).

73. *Subsection (3)* describes a second form which warrants may take. It applies if conditions in subsections (3)(a) and (b), and (4)(a) or (b) are met.

74. *Subsection (3)(a)* confines the conduct authorised or required by the warrant to conduct falling within subsection (4).

75. *Subsection (3)(b)* requires that at the time when the Secretary of State issues the warrant there must be in existence a certificate certifying the description of intercepted material the examination of which he considers necessary as is mentioned in clause 5(3)(a), (b) or (c) - namely the purposes for the issue of warrants. The effect of this subsection is to require the Secretary of State to authorise a certificate describing the intercepted material which falls properly within the purpose and may therefore be read, looked at or listened to by any person. No other intercepted material, though the communications are lawfully intercepted, may be so examined. The material authorised for examination is therefore fully subject to Ministerial control.

76. *Subsection (4)(a)* covers conduct that consists in the interception of communications in the course of their transmission by a telecommunications system. The effect of this is to limit warrants under this provision to telecommunications, and to exclude postal items. These telecommunications must also be external communications, i.e. sent or received outside the British Islands.

77. *Subsection (4)(b)* covers conduct authorised by an interception warrant by Clause 5(6). See Explanatory Notes for Clause 5(6)(a) to (c).

"External communications" is defined in Clause 19.

78. *Subsection (5)* requires a certificate to be issued under the hand of the Secretary of State. The control exercised through the certificate has therefore to be a personal Ministerial one. There is no provision for delegation of this power to officials, even in urgent cases.