



# Investigatory Powers Act 2016

## 2016 CHAPTER 25

### PART 1

#### GENERAL PRIVACY PROTECTIONS

##### *Overview and general privacy duties*

#### **1 Overview of Act**

- (1) This Act sets out the extent to which certain investigatory powers may be used to interfere with privacy.
- (2) This Part imposes certain duties in relation to privacy and contains other protections for privacy.
- (3) These other protections include offences and penalties in relation to—
  - (a) the unlawful interception of communications, and
  - (b) the unlawful obtaining of communications data.
- (4) This Part also abolishes and restricts various general powers to obtain communications data and restricts the circumstances in which equipment interference, and certain requests about the interception of communications, can take place.
- (5) Further protections for privacy—
  - (a) can be found, in particular, in the regimes provided for by Parts 2 to 7 and in the oversight arrangements in Part 8, and
  - (b) also exist—
    - (i) by virtue of the Human Rights Act 1998,
    - (ii) in section 55 of the Data Protection Act 1998 (unlawful obtaining etc. of personal data),
    - (iii) in section 48 of the Wireless Telegraphy Act 2006 (offence of interception or disclosure of messages),
    - (iv) in sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences),

- (v) in the common law offence of misconduct in public office, and
- (vi) elsewhere in the law.

(6) The regimes provided for by Parts 2 to 7 are as follows—

- (a) Part 2 and Chapter 1 of Part 6 set out circumstances (including under a warrant) in which the interception of communications is lawful and make further provision about the interception of communications and the treatment of material obtained in connection with it,
- (b) Part 3 and Chapter 2 of Part 6 set out circumstances in which the obtaining of communications data is lawful in pursuance of an authorisation or under a warrant and make further provision about the obtaining and treatment of such data,
- (c) Part 4 makes provision for the retention of certain communications data in pursuance of a notice,
- (d) Part 5 and Chapter 3 of Part 6 deal with equipment interference warrants, and
- (e) Part 7 deals with bulk personal dataset warrants.

(7) As to the rest of the Act—

- (a) Part 8 deals with oversight arrangements for regimes in this Act and elsewhere, and
- (b) Part 9 contains miscellaneous and general provisions including amendments to sections 3 and 5 of the Intelligence Services Act 1994 and provisions about national security and combined warrants and authorisations.

## **2 General duties in relation to privacy**

(1) Subsection (2) applies where a public authority is deciding whether—

- (a) to issue, renew or cancel a warrant under Part 2, 5, 6 or 7,
- (b) to modify such a warrant,
- (c) to approve a decision to issue, renew or modify such a warrant,
- (d) to grant, approve or cancel an authorisation under Part 3,
- (e) to give a notice in pursuance of such an authorisation or under Part 4 or section 252, 253 or 257,
- (f) to vary or revoke such a notice,
- (g) to approve a decision to give or vary a notice under Part 4 or section 252, 253 or 257,
- (h) to approve the use of criteria under section 153, 194 or 222,
- (i) to give an authorisation under section 219(3)(b),
- (j) to approve a decision to give such an authorisation, or
- (k) to apply for or otherwise seek any issue, grant, giving, modification, variation or renewal of a kind falling within paragraph (a), (b), (d), (e), (f) or (i).

(2) The public authority must have regard to—

- (a) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means,
- (b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information,
- (c) the public interest in the integrity and security of telecommunication systems and postal services, and

- (d) any other aspects of the public interest in the protection of privacy.
- (3) The duties under subsection (2)—
  - (a) apply so far as they are relevant in the particular context, and
  - (b) are subject to the need to have regard to other considerations that are also relevant in that context.
- (4) The other considerations may, in particular, include—
  - (a) the interests of national security or of the economic well-being of the United Kingdom,
  - (b) the public interest in preventing or detecting serious crime,
  - (c) other considerations which are relevant to—
    - (i) whether the conduct authorised or required by the warrant, authorisation or notice is proportionate, or
    - (ii) whether it is necessary to act for a purpose provided for by this Act,
  - (d) the requirements of the Human Rights Act 1998, and
  - (e) other requirements of public law.
- (5) For the purposes of subsection (2)(b), examples of sensitive information include—
  - (a) items subject to legal privilege,
  - (b) any information identifying or confirming a source of journalistic information, and
  - (c) relevant confidential information within the meaning given by paragraph 2(4) of Schedule 7 (certain information held in confidence and consisting of personal records, journalistic material or communications between Members of Parliament and their constituents).
- (6) In this section “public authority” includes the relevant judicial authority (within the meaning of section 75) where the relevant judicial authority is deciding whether to approve under that section an authorisation under Part 3.

### *Prohibitions against unlawful interception*

## **3 Offence of unlawful interception**

- (1) A person commits an offence if—
  - (a) the person intentionally intercepts a communication in the course of its transmission by means of—
    - (i) a public telecommunication system,
    - (ii) a private telecommunication system, or
    - (iii) a public postal service,
  - (b) the interception is carried out in the United Kingdom, and
  - (c) the person does not have lawful authority to carry out the interception.
- (2) But it is not an offence under subsection (1) for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person—
  - (a) is a person with a right to control the operation or use of the system, or
  - (b) has the express or implied consent of such a person to carry out the interception.

---

*Status: This is the original version (as it was originally enacted).*

---

- (3) Sections 4 and 5 contain provision about—
  - (a) the meaning of “interception”, and
  - (b) when interception is to be regarded as carried out in the United Kingdom.
- (4) Section 6 contains provision about when a person has lawful authority to carry out an interception.
- (5) For the meaning of the terms used in subsection (1)(a)(i) to (iii), see sections 261 and 262.
- (6) A person who is guilty of an offence under subsection (1) is liable—
  - (a) on summary conviction in England and Wales, to a fine;
  - (b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;
  - (c) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.
- (7) No proceedings for any offence which is an offence by virtue of this section may be instituted—
  - (a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;
  - (b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

#### **4 Definition of “interception” etc.**

##### *Interception in relation to telecommunication systems*

- (1) For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if—
  - (a) the person does a relevant act in relation to the system, and
  - (b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.

For the meaning of “content” in relation to a communication, see section 261(6).

- (2) In this section “relevant act”, in relation to a telecommunication system, means—
  - (a) modifying, or interfering with, the system or its operation;
  - (b) monitoring transmissions made by means of the system;
  - (c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.
- (3) For the purposes of this section references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with—
  - (a) any part of the system, or
  - (b) any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system.
- (4) In this section “relevant time”, in relation to a communication transmitted by means of a telecommunication system, means—

- (a) any time while the communication is being transmitted, and
  - (b) any time when the communication is stored in or by the system (whether before or after its transmission).
- (5) For the purposes of this section, the cases in which any content of a communication is to be taken to be made available to a person at a relevant time include any case in which any of the communication is diverted or recorded at a relevant time so as to make any content of the communication available to a person after that time.
- (6) In this section “wireless telegraphy” and “wireless telegraphy apparatus” have the same meaning as in the Wireless Telegraphy Act 2006 (see sections 116 and 117 of that Act).

*Interception in relation to postal services*

- (7) Section 125(3) of the Postal Services Act 2000 applies for the purposes of determining for the purposes of this Act whether a postal item is in the course of its transmission by means of a postal service as it applies for the purposes of determining for the purposes of that Act whether a postal packet is in course of transmission by post.

*Interception carried out in the United Kingdom*

- (8) For the purposes of this Act the interception of a communication is carried out in the United Kingdom if, and only if—
  - (a) the relevant act or, in the case of a postal item, the interception is carried out by conduct within the United Kingdom, and
  - (b) the communication is intercepted—
    - (i) in the course of its transmission by means of a public telecommunication system or a public postal service, or
    - (ii) in the course of its transmission by means of a private telecommunication system in a case where the sender or intended recipient of the communication is in the United Kingdom.

## **5 Conduct that is not interception**

- (1) References in this Act to the interception of a communication do not include references to the interception of any communication broadcast for general reception.
- (2) References in this Act to the interception of a communication in the course of its transmission by means of a postal service do not include references to—
  - (a) any conduct that takes place in relation only to so much of the communication as consists of any postal data comprised in, included as part of, attached to, or logically associated with a communication (whether by the sender or otherwise) for the purposes of any postal service by means of which it is being or may be transmitted, or
  - (b) any conduct, in connection with conduct falling within paragraph (a), that gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying such postal data.

For the meaning of “postal data”, see section 262.

## **6 Definition of “lawful authority”**

- (1) For the purposes of this Act, a person has lawful authority to carry out an interception if, and only if—
  - (a) the interception is carried out in accordance with—
    - (i) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2, or
    - (ii) a bulk interception warrant under Chapter 1 of Part 6,
  - (b) the interception is authorised by any of sections 44 to 52, or
  - (c) in the case of a communication stored in or by a telecommunication system, the interception—
    - (i) is carried out in accordance with a targeted equipment interference warrant under Part 5 or a bulk equipment interference warrant under Chapter 3 of Part 6,
    - (ii) is in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property, or
    - (iii) is carried out in accordance with a court order made for that purpose.
- (2) Conduct which has lawful authority for the purposes of this Act by virtue of subsection (1)(a) or (b) is to be treated as lawful for all other purposes.
- (3) Any other conduct which—
  - (a) is carried out in accordance with a warrant under Chapter 1 of Part 2 or a bulk interception warrant, or
  - (b) is authorised by any of sections 44 to 52,is to be treated as lawful for all purposes.

## **7 Monetary penalties for certain unlawful interceptions**

- (1) The Investigatory Powers Commissioner may serve a monetary penalty notice on a person if conditions A and B are met.
- (2) A monetary penalty notice is a notice requiring the person on whom it is served to pay to the Investigatory Powers Commissioner (“the Commissioner”) a monetary penalty of an amount determined by the Commissioner and specified in the notice.
- (3) Condition A is that the Commissioner considers that—
  - (a) the person has intercepted, in the United Kingdom, any communication in the course of its transmission by means of a public telecommunication system,
  - (b) the person did not have lawful authority to carry out the interception, and
  - (c) the person was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception.
- (4) Condition B is that the Commissioner does not consider that the person has committed an offence under section 3(1).
- (5) The amount of a monetary penalty determined by the Commissioner under this section must not exceed £50,000.
- (6) Schedule 1 (which makes further provision about monetary penalty notices) has effect.

- (7) In this section “interception warrant” means—
- (a) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2, or
  - (b) a bulk interception warrant under Chapter 1 of Part 6.
- (8) For the meaning of “interception” and other key expressions used in this section, see sections 4 to 6.

## **8 Civil liability for certain unlawful interceptions**

- (1) An interception of a communication is actionable at the suit or instance of—
- (a) the sender of the communication, or
  - (b) the recipient, or intended recipient, of the communication,
- if conditions A to D are met.
- (2) Condition A is that the interception is carried out in the United Kingdom.
- (3) Condition B is that the communication is intercepted—
- (a) in the course of its transmission by means of a private telecommunication system, or
  - (b) in the course of its transmission, by means of a public telecommunication system, to or from apparatus that is part of a private telecommunication system.
- (4) Condition C is that the interception is carried out by, or with the express or implied consent of, a person who has the right to control the operation or use of the private telecommunication system.
- (5) Condition D is that the interception is carried out without lawful authority.
- (6) For the meaning of “interception” and other key expressions used in this section, see sections 4 to 6.

## **9 Restriction on requesting interception by overseas authorities**

- (1) This section applies to a request for any authorities of a country or territory outside the United Kingdom to carry out the interception of communications sent by, or intended for, an individual who the person making the request believes will be in the British Islands at the time of the interception.
- (2) A request to which this section applies may not be made by or on behalf of a person in the United Kingdom unless—
- (a) a targeted interception warrant has been issued under Chapter 1 of Part 2 authorising the person to whom it is addressed to secure the interception of communications sent by, or intended for, that individual, or
  - (b) a targeted examination warrant has been issued under that Chapter authorising the person to whom it is addressed to carry out the selection of the content of such communications for examination.

## **10 Restriction on requesting assistance under mutual assistance agreements etc.**

- (1) This section applies to—

---

*Status: This is the original version (as it was originally enacted).*

---

- (a) a request for assistance under an EU mutual assistance instrument, and
  - (b) a request for assistance in accordance with an international mutual assistance agreement.
- (2) A request to which this section applies may not be made by or on behalf of a person in the United Kingdom to the competent authorities of a country or territory outside the United Kingdom unless a mutual assistance warrant has been issued under Chapter 1 of Part 2 authorising the making of the request.
- (3) In this section—
- “EU mutual assistance instrument” means an EU instrument which—
    - (a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,
    - (b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and
    - (c) is designated as an EU mutual assistance instrument by regulations made by the Secretary of State;
  - “international mutual assistance agreement” means an international agreement which—
    - (a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,
    - (b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and
    - (c) is designated as an international mutual assistance agreement by regulations made by the Secretary of State.

### *Prohibition against unlawful obtaining of communications data*

## **11 Offence of unlawfully obtaining communications data**

- (1) A relevant person who, without lawful authority, knowingly or recklessly obtains communications data from a telecommunications operator or a postal operator is guilty of an offence.
- (2) In this section “relevant person” means a person who holds an office, rank or position with a relevant public authority (within the meaning of Part 3).
- (3) Subsection (1) does not apply to a relevant person who shows that the person acted in the reasonable belief that the person had lawful authority to obtain the communications data.
- (4) A person guilty of an offence under this section is liable—
  - (a) on summary conviction in England and Wales—
    - (i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or
    - (ii) to a fine,
 or to both;
  - (b) on summary conviction in Scotland—
    - (i) to imprisonment for a term not exceeding 12 months, or
    - (ii) to a fine not exceeding the statutory maximum,



- or to both;
- (c) on summary conviction in Northern Ireland—
  - (i) to imprisonment for a term not exceeding 6 months, or
  - (ii) to a fine not exceeding the statutory maximum,or to both;
- (d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

*Abolition or restriction of powers to obtain communications data*

**12 Abolition or restriction of certain powers to obtain communications data**

- (1) Schedule 2 (which repeals certain information powers so far as they enable public authorities to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator) has effect.
- (2) Any general information power which—
  - (a) would (apart from this subsection) enable a public authority to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator, and
  - (b) does not involve a court order or other judicial authorisation or warrant and is not a regulatory power or a relevant postal power,is to be read as not enabling the public authority to secure such a disclosure.
- (3) A regulatory power or relevant postal power which enables a public authority to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator may only be exercised by the public authority for that purpose if it is not possible for the authority to use a power under this Act to secure the disclosure of the data.
- (4) The Secretary of State may by regulations modify any enactment in consequence of subsection (2).
- (5) In this section “general information power” means—
  - (a) in relation to disclosure by a telecommunications operator, any power to obtain information or documents (however expressed) which—
    - (i) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and
    - (ii) does not deal (whether alone or with other matters) specifically with telecommunications operators or any class of telecommunications operators, and
  - (b) in relation to disclosure by a postal operator, any power to obtain information or documents (however expressed) which—
    - (i) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and
    - (ii) does not deal (whether alone or with other matters) specifically with postal operators or any class of postal operators.
- (6) In this section—
  - “power” includes part of a power,

“regulatory power” means any power to obtain information or documents (however expressed) which—

- (a) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and
- (b) is exercisable in connection with the regulation of—
  - (i) telecommunications operators, telecommunications services or telecommunication systems, or
  - (ii) postal operators or postal services,

“relevant postal power” means any power to obtain information or documents (however expressed) which—

- (a) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and
- (b) is exercisable in connection with the conveyance or expected conveyance of any postal item into or out of the United Kingdom,

and references to powers include duties (and references to enabling and exercising are to be read as including references to requiring and performing).

#### *Restrictions on interference with equipment*

### **13 Mandatory use of equipment interference warrants**

- (1) An intelligence service may not, for the purpose of obtaining communications, private information or equipment data, engage in conduct which could be authorised by an equipment interference warrant except under the authority of such a warrant if—
  - (a) the intelligence service considers that the conduct would (unless done under lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences), and
  - (b) there is a British Islands connection.
- (2) For the purpose of this section, there is a British Islands connection if—
  - (a) any of the conduct would take place in the British Islands (regardless of the location of the equipment which would, or may, be interfered with),
  - (b) the intelligence service believes that any of the equipment which would, or may, be interfered with would, or may, be in the British Islands at some time while the interference is taking place, or
  - (c) a purpose of the interference is to obtain—
    - (i) communications sent by, or to, a person who is, or whom the intelligence service believes to be, for the time being in the British Islands,
    - (ii) private information relating to an individual who is, or whom the intelligence service believes to be, for the time being in the British Islands, or
    - (iii) equipment data which forms part of, or is connected with, communications or private information falling within sub-paragraph (i) or (ii).
- (3) This section does not restrict the ability of the head of an intelligence service to apply for an equipment interference warrant in cases where—
  - (a) the intelligence service does not consider that the conduct for which it is seeking authorisation would (unless done under lawful authority) constitute

one or more offences under sections 1 to 3A of the Computer Misuse Act 1990, or

(b) there is no British Islands connection.

(4) In this section—

“communications”, “private information” and “equipment data” have the same meaning as in Part 5 (see section 135);

“equipment interference warrant” means—

(a) a targeted equipment interference warrant under Part 5;

(b) a bulk equipment interference warrant under Chapter 3 of Part 6.

## **14      Restriction on use of section 93 of the Police Act 1997**

(1) A person may not, for the purpose of obtaining communications, private information or equipment data, make an application under section 93 of the Police Act 1997 for authorisation to engage in conduct which could be authorised by a targeted equipment interference warrant under Part 5 if the applicant considers that the conduct would (unless done under lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences).

(2) In this section, “communications”, “private information” and “equipment data” have the same meaning as in Part 5 (see section 135).