HOUSE OF LORDS

OPINIONS OF THE LORDS OF APPEAL FOR JUDGMENT IN THE CAUSE

Attorney General's Reference No 5 of 2002 (On Appeal from the Court of Appeal (Criminal Division))

[2004] UKHL 40

LORD BINGHAM OF CORNHILL

My Lords,

1. By this reference under section 36(1) of the Criminal Justice Act 1972 the Attorney General sought the opinion of the Court of Appeal on the correct construction of section 17(1) of the Regulation of Investigatory Powers Act 2000. Although the points of law which he referred were more elaborately expressed, the essential thrust of his questions was whether, and if so to what extent, a criminal court may investigate whether intercept material relied on by the Crown has been obtained by tapping a private as opposed to a public telecommunications system. The Court of Appeal (Clarke LJ, Morison J and Dame Heather Steel) considered the questions referred in considerable detail and accepted the argument advanced for the Attorney General: [2003] EWCA Crim 1632, [2003] 1 WLR 2902. The court however recognised the difficulty and complexity of the 2000 Act and exercised its power under section 36(3) of the 1972 Act to refer the Attorney General's questions to the House.

2. The acquittal which is necessary to trigger the Attorney General's power to refer under section 36(1) of the 1972 Act came about in this way. It was believed that Detective Sergeant W and two other police officers were supplying confidential and sensitive information to a known criminal, C, and that W had provided sensitive and confidential information to another man, L, and also to journalists. On 30 May 1996 the chief constable of the force to which W and the other officers belonged gave his consent in writing for the interception of communications to take place on a number of telephone extensions used by W and others. It is agreed between counsel that the telephone system used to make the interceptions was a system which linked several police

stations and which comprised several Private Automated Branch Exchanges linked together via BT Megastream lines, which were component parts of the public telecommunications system operated by BT under licence from the Secretary of State pursuant to section 9 of the Telecommunications Act 1984. The equipment used to carry out the interception was a system known as "Dial Up" which worked in the following way. A telephone call received on or made from the telephones in question activated the interception equipment. The interception equipment created a duplicate call which was relayed through a BT telephone line to another police station where equipment capable of recording the calls had been installed. The telephone calls were thus monitored and recorded.

3. The product of this interception confirmed the suspicion that W was supplying information of a confidential and sensitive nature to persons who had no entitlement to receive it. The interception continued until 21 June 1997 and the three officers and C were prosecuted in reliance on the material thus obtained. An indictment was preferred, charging all the defendants (in count 1) with conspiring to commit misconduct in a public office. Additional counts alleging misconduct in public office were laid against W alone.

4. The prosecution case at trial was that the interceptions had taken place within a private telecommunications system, and it served evidence on the defence before the trial to prove that fact. The defence case was that the interception had taken place on a public telecommunications system. At the trial in May 2002, before the prosecution evidence had been called, the defence submitted that section 17 of the 2000 Act prevented any investigation into the circumstances of the interception and, in particular, into whether the interception had taken place on the public side of the telecommunications system. Having heard argument, the judge ruled that section 17 prevented the defence from asserting that the interception had taken place on the public side of the system, although it did not prevent the prosecution from adducing evidence that it had taken place on the private side. The defence then submitted that the judge should exclude the prosecution evidence that the interception had taken place within a private telecommunications system under section 78 of the Police and Criminal Evidence Act 1984, since it would not be fair to admit that evidence and shut out the defence case that it had taken place on the public side of such a system. To this submission the judge acceded. This obliged the prosecution to offer no evidence, with the result that W and his co-defendants were acquitted on the judge's direction.

5. It is unnecessary to trace the history of official interception in the United Kingdom before 1985, which is uncontroversial and has been summarised on other occasions: see, for example, *R v Preston* [1994] 2 AC 130, 142, 147-148; *R v P* [2002] 1 AC 146, 155-157; *The Interception of Communications in the United Kingdom* (Cmnd 9438, 1985). It is enough to draw attention to four features of the practice as it then existed. First, telephones had for many years been tapped, and mail intercepted, pursuant to warrants issued by an appropriate secretary of state. Secondly, in cases culminating in criminal prosecution the tap or intercept was used for purposes of preventing and detecting crime, and not for the purpose of prosecuting culprits: the product of the tap or intercept was not relied on as evidence. Thirdly, there was no rule of law or practice which rendered inadmissible in criminal proceedings the product of any unofficial or private eavesdropping activity. While a trial judge might exclude such evidence in the exercise of his overriding discretion to ensure the fairness of a trial, he would not in the absence of special circumstances have been at all likely to do so. Fourthly, the process of interception, by whatever means, official or unofficial, of communications, whether public or private, was wholly unregulated by statute.

6. It was this last feature of the prevailing practice which led the European Court of Human Rights to hold, in the context of warranted police tapping of Mr Malone's telephone, that the interference with his right to privacy which the facts disclosed was not, as required by article 8 of the European Convention, "in accordance with the law": *Malone v United Kingdom* (1984) 7 EHRR 14. This adverse finding obliged the United Kingdom under articles 1 and 46 of the Convention to secure the protection of article 8 rights to all within its jurisdiction and to abide by the judgment. This it sought to do by enacting the Interception of Communications Act 1985. It is unnecessary for present purposes to cite the detailed provisions of that Act, but certain cardinal features of it should be noted. First, the United Kingdom did not respond to the adverse decision in *Malone* by enacting a comprehensive scheme to regulate the whole field of interception. The scheme embodied in the 1985 Act was directed to interception which was or should have been warranted, such as Mr Malone had successfully challenged. Thus section 1 of the Act made it an offence to intercept, intentionally, a communication in the course of its transmission by post or by means of a public telecommunication system (subject to an exception in section 1(3)), but the Act did not address interception otherwise than within the post or such a system. Secondly, the Act preserved the existing practice for issuing interception warrants by an appropriate secretary of state. The practice was very greatly formalised, and detailed provisions were made to govern the issue, form, contents, duration and effect of

warrants, to provide for access to a tribunal to resolve complaints and to provide for retrospective judicial invigilation of the new practice. But it was a reform of the old warrant regime in order to comply with the Strasbourg decision, not the establishment of a new regime. Thirdly, it remained the rule that, in the context of criminal activity, interception was to be an instrument of prevention and detection, not an instrument of prosecution. This was made clear by section 2(2)(b) of the Act which, in the criminal field, empowered a secretary of state to issue a warrant only if he judged it to be necessary "for the purpose of preventing or detecting serious crime", and by section 6(3) which required destruction of the interception product as soon as its retention was no longer necessary for that purpose. Fourthly, the Act was drafted in terms plainly intended to preclude any forensic enquiry into any aspect of the procedure of applying for or giving effect to warrants. This was made clear by section 9 of the Act, the terms of which must be quoted. As enacted, the section read:

> "9.-(1) In any proceedings before any court or tribunal no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest -
>
> (a) that an offence under section 1 above has been or is to be committed by any of the persons mentioned in subsection (2) below; or
>
> (b) that a warrant has been or is to be issued to any of those persons.
>
> (2) The persons referred to in subsection (1) above are -
>
> (a) any person holding office under the Crown;
>
> (b) the Post Office and any person engaged in the business of the Post Office; and
>
> (c) any public telecommunications operator and any person engaged in the running of a public telecommunication system.
>
> (3) Subsection (1) above does not apply -
>
> (a) in relation to proceedings for a relevant offence or proceedings before the Tribunal; or
>
> (b) where the evidence is adduced or the question in cross-examination is asked for the purpose of establishing the fairness or unfairness of a dismissal on grounds of an offence under section 1 above or of conduct from which such an offence might be inferred;

and paragraph (a) of that subsection does not apply where a person has been convicted of the offence under that section.

(4) In this section 'relevant offence' means -

(a) an offence under section 1 above or under section 45 of the Telegraph Act 1863, section 20 of the Telegraph Act 1868, section 58 of the Post Office Act 1953 or section 45 of the 1984 Act;

(b) an offence under section 1 or 2 of the Official Secrets Act 1911 relating to any sketch, plan, model, article, note, document or information which tends to suggest as mentioned in subsection (1) above;

(c) perjury committed in the course of proceedings for a relevant offence;

(d) attempting or conspiring to commit, or aiding, abetting counselling or procuring the commission of, an offence falling within any of the preceding paragraphs; and

(e) contempt of court committed in the course of, or in relation to, proceedings for a relevant offence."

The prohibition in subsection (1) applied both to interception which had been duly warranted and to interception which should have been duly warranted but had not, if in either case any person within subsection (2) had been involved. The obvious purpose of this prohibition was to preserve the secrecy of what had, to be effective, to be a covert operation.

7. These last two features of the regime established by the 1985 Act have been judicially recognised on a number of occasions: see, for example, *R v Preston* [1994] 2 AC 130, 143-144, 167-168, 170; *Morgans v Director of Public Prosecutions* [2001] 1 AC 315, 321, 337-339; *R v Sargent* [2001] UKHL 54, [2003] 1 AC 347, para 28; *R v P* [2002] 1 AC 146, 163-164. As Lord Hobhouse of Woodborough said in the last cited case, page 164,

" … the dominant principle guiding the interpretation of the provisions of the [1985] Act was the policy of preserving the secrecy of the surveillance operations to which the Act applied and, to that end, preventing as far as

possible any evidence relating to such operations ever reaching the public domain".

He added, pages 165-166:

> "In this country it is, in the judgment of the Government, the necessity to have a fully effective interception system which creates the necessity for secrecy and consequently the need to keep the evidence of it out of the public domain. But where secrecy is not required, the necessity is that all relevant and probative evidence be available to assist in the apprehension and conviction of criminals and to ensure that their trial is fair. The latter necessity exists in both cases but in the former case it is trumped by the greater necessity for secrecy, as the speeches in *R v Preston* [1994] 2 AC 130 explain".

8. Following enactment of the 1985 Act, the courts were more than once called upon to consider whether evidence on which it was sought to rely was the product of interception of a public or private telecommunications system: see *R v Ahmed* (Court of Appeal, 29 March 1994, unreported); *R v Effik* [1995] 1 AC 309, 314. The focus of the enquiry in the latter of these cases is shown by the ruling of Lord Oliver of Aylmerton, with which all members of the committee agreed (page 317):

> "Once again, one sees the emphasis on the duty of the person running the public system and the transmission through that system.
>
> My Lords, in the light of these statutory provisions, I do not, for my part, entertain any doubt that the trial judge was right in concluding that the Geemarc cordless telephone used by Miss Sumer was a privately run system. The apparatus was clearly not 'comprised in' the public British Telecommunications system although it was connected to it by means of the socket at which, on the judges' finding, that system ended. A communication through a telecommunication system consists of a series of electronic impulses and what was actually intercepted by the use of the police officers' radio receiver consisted of

> the impulses transmitted between the base unit and the handset, both of which formed part of a telecommunication system 'run' by Miss Sumer (Act of 1983, section 4(2)) but formed no part of the public telecommunication system run by British Telecommunications."

In none of these cases does it appear to have been suggested that the enquiry whether the system was public or private was one which should not, or could not, be carried out.

9. The United Kingdom suffered a further reverse in the European Court of Human Rights in *Halford v United Kingdom* (1997) 24 EHRR 523. On this occasion the successful challenge related not to warranted interception of a public telecommunications system but to unwarranted interception by the police of a senior police officer's office telephone. But the outcome was very much the same. It was held that the interception, being wholly unregulated by statute, was not "in accordance with the law" and was thus an interference with the officer's article 8(1) right not saved by article 8(2). Thus the need for statutory intervention again arose, this time of unwarranted interception. It might, no doubt, have been decided to introduce a measure designed simply to provide the statutory regulation which had been found to be lacking in *Halford*. But the years since 1985 had been a time of rapid technological advance in the telecommunications field, and had moreover seen a proliferation of commercial service providers in the postal and telecommunications field which had formerly been the preserve of public monopoly providers. So the decision was made to introduce a measure, which became the 2000 Act, covering (in Chapter I) the whole field of interception, and also regulating other forms of surveillance. Chapter I was drafted to apply to postal as well as telecommunications services; to public as well as private systems; to interception requiring the issue of a warrant as well as interception not requiring such a warrant; to warrants requiring to be certified and warrants not requiring certification; to interception outside the United Kingdom as well as within it; to civil remedies as well as criminal liability. The draftsman faced a daunting task. If, however, as Lord Mustill suggested in *R v Preston* [1994] 2 AC 130, 148, the 1985 Act was a "short but difficult statute", the 2000 Act is both longer and even more perplexing. The trial judge and the Court of Appeal found it difficult to construe the provisions of the Act with confidence, and the House has experienced the same difficulty.

10. In seeking to overcome these problems, it is in my opinion helpful to begin by recognising the objects which, as I think plainly, Parliament was seeking to achieve in Chapter 1 of this Act. First of all, it was seeking to make good the deficiency identified in *Halford* by regulating the tapping of private telephones. It did not do so by prohibiting such interception altogether. The European Court in *Halford* had not held such a prohibition to be necessary: see paragraph 49 of its judgment. But it was necessary that such interception by a public authority should be regulated by law, and it was also necessary for the subject of such interception, if it was unjustified, to have a civil remedy. This was provided by section 1(3) of the Act, which read:

> "(3) Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority and is either -
>
> (a) an interception of that communication in the course of its transmission by means of that private system; or
>
> (b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system."

11. Secondly, and for present purposes less importantly, the 2000 Act attempted to provide for past and continuing technological advance in the telecommunications field. Whereas the 1985 Act had offered no definition of interception, the 2000 Act did so in section 2(2).

12. Thirdly, the 2000 Act made express provision for private as well as public service providers. This was evidenced by use of the expressions, defined in section 2(1), "postal service", "public postal service", "private telecommunication system", "public telecommunications service" and "public telecommunication system."

13. Fourthly, sections 5-11 and 15 of the 2000 Act preserved all the essential features of the regime established by the 1985 Act for the issue

of warrants by a secretary of state. Section 65 established a Tribunal with greatly enlarged jurisdiction as compared with that established under the 1985 Act, but the new Tribunal was still to have jurisdiction to entertain complaints about conduct for or in connection with the interception of communications in the course of their transmission by means of a postal service or telecommunication system. There was still to be a judicial invigilator of the interception process: section 57 of the 2000 Act.

14. There are three further points, all of them negative, but all of them in my opinion very important, which should guide the construction of the 2000 Act. First, there is nothing whatever which suggests an intention to depart from the principle that the issue of warrants by a secretary of state and all matters pertaining to such warrants should not be the subject of enquiry in the course of a criminal trial. Secondly, there was nothing in the 2000 Act, nor in the consultation paper which preceded it (*Interception of Communications in the United Kingdom*, Cm 4368, 1999), nor in the Hansard references to which the House was referred, which questioned or threw doubt on the decisions in *R v Ahmed* and *R v Effik* (see paragraph 8 above) in which the court had examined whether an interception had been made within a public or a private system. Since the 2000 Act was passed, there have been further Court of Appeal decisions in which the same enquiry has been conducted: *R v Allan* [2001] EWCA Crim 1027 (6 April 2001, unreported); *R v Goodman* [2002] EWCA Crim 903 (4 March 2002, unreported). Thirdly, there is nothing in the 2000 Act or in any other materials the House has been shown to suggest a parliamentary intention to render inadmissible as evidence in criminal proceedings any material which had previously been admissible, save to the extent explained in paragraph 20 below. As already shown, the United Kingdom practice has been to exclude the product of warranted interception from the public domain and thus to preclude its use as evidence. But this has been a policy choice, not a requirement compelled by the Convention, and other countries have made a different policy choice. Article 8(2) of the European Convention permits necessary and proportionate interference with the right guaranteed in article 8(1) if in accordance with the law and if in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. Save where necessary to preserve the security of warranted interception, there is no reason why it should have been sought to exclude the product of any lawful interception where relevant as evidence in any case whether civil or criminal.

15. Section 1(1) of the 2000 Act re-enacts, with immaterial differences of language, the offence created by section 1(1) of the 1985 Act of intentionally and without lawful authority intercepting in the United Kingdom any communication in the course of its transmission by means of a public postal service or a public telecommunication system. Lawful authority derives from a warrant duly issued by a secretary of state under section 5. Section 1 continues:

> "(2) It shall be an offence for a person -
>
> (a) intentionally and without lawful authority, and
>
> (b) otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection,
>
> to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system".

This subsection is of course new, as is the subsection on civil liability, quoted in paragraph 10 above, which follows. The references to lawful authority and exclusion from criminal liability are clarified in subsections (5) and (6):

> "(5) Conduct has lawful authority for the purposes of this section if, and only if -
>
> (a) it is authorised by or under section 3 or 4;
>
> (b) it takes place in accordance with a warrant under section 5 ('an interception warrant'); or
>
> (c) it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property;
>
> and conduct (whether or not prohibited by this section) which has lawful authority for the purposes of this section by virtue of paragraph (a) or (b) shall also be taken to be lawful for all other purposes.
>
> (6) The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that his conduct is excluded from criminal liability under subsection (2) if -

(a) he is a person with a right to control the operation or the use of the system; or

(b) he has the express or implied consent of such a person to make the interception."

16. The first source of lawful authority to tap a private telecommunication system is defined in section 3, which so far as material provides:

"(1) Conduct by any person consisting in the interception of a communication is authorised by this section if the communication is one which, or which that person has reasonable grounds for believing, is both -

(a) a communication sent by a person who has consented to the interception; and

(b) a communication the intended recipient of which has so consented.

(2) Conduct by any person consisting in the interception of a communication is authorised by this section if -

(a) the communication is one sent by, or intended for, a person who has consented to the interception; and

(b) surveillance by means of that interception has been authorised under Part II.

(3) Conduct consisting in the interception of a communication is authorised by this section if -

(a) it is conduct by or on behalf of a person who provides a postal service or a telecommunications service; and

(b) it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services.

The last of these subsections reproduces the effect (although not the language) of section 1(3)(a) of the 1985 Act, the subject matter of which was considered in depth by the House in *Morgans v Director of Pubic Prosecutions* [2001] 1 AC 315, without any suggestion that this was a subject matter into which it could not enquire.

17. The second source of lawful authority to tap a private, domestic, telecommunication system is defined in section 4(2) and (3), which provide:

> "(2) Subject to subsection (3), the Secretary of State may by regulations authorise any such conduct described in the regulations as appears to him to constitute a legitimate practice reasonably required for the purpose, in connection with the carrying on of any business, of monitoring or keeping a record of -
>
> (a) communications by means of which transactions are entered into in the course of that business; or
>
> (b) other communications relating to that business or taking place in the course of its being carried on.
>
> (3) Nothing in any regulations under subsection (2) shall authorise the interception of any communication except in the course of its transmission using apparatus or services provided by or to the person carrying on the business for use wholly or partly in connection with that business."

In subsection (7), "business" is defined to include any activities of a government department, or any public authority, or any person or office holder on whom functions are conferred by or under any enactment. The section makes special provision for the authorisation of conduct taking place in prisons, high security hospitals and certain Scottish hospitals. Plainly, the provisions of this section are apt to permit an employer to monitor such matters as insider-dealing, money-laundering or compliance with regulatory requirements.

18. Section 17 of the 2000 Act, to which this reference by the Attorney General is directed, must be quoted in full. It provides:

> "17 Exclusion of matters from legal proceedings
>
> (1) Subject to section 18, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner) -
>
> (a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted

communication or any related communications data; or

(b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur.

(2) The following fall within this subsection -

"(a) conduct by a person falling within subsection (3) that was or would be an offence under section 1(1) or (2) of this Act or under section 1 of the Interception of Communications Act 1985;

(b) a breach by the Secretary of State of his duty under section 1(4) of this Act;

(c) the issue of an interception warrant or of a warrant under the Interception of Communications Act 1985;

(d) the making of an application by any person for an interception warrant, or for a warrant under that Act;

(e) the imposition of any requirement on any person to provide assistance with giving effect to an interception warrant.

(3) The persons referred to in subsection (2)(a) are -

(a) any person to whom a warrant under this Chapter may be addressed;

(b) any person holding office under the Crown;

(c) any member of the National Criminal Intelligence Service;

(d) any member of the National Crime Squad;

(e) any person employed by or for the purposes of a police force;

(f) any person providing a postal service or employed for the purposes of any business of providing such a service; and

(g) any person providing a public telecommunications service or employed for the purposes of any business of providing such a service.

(4) In this section 'intercepted communication' means any communication intercepted in the course of its transmission by means of a postal service or telecommunication system".

Section 18, to which section 17(1) is expressed to be subject, provides for the disapplication or partial disapplication of section 17(1) in certain situations which need not for present purposes be examined. Subsections (4) and (5) of section 18 should, however, be noted:

> "(4) Section 17(1)(a) shall not prohibit the disclosure of any of the contents of a communication if the interception of that communication was lawful by virtue of section 1(5)(c), 3 or 4.
>
> (5) Where any disclosure is proposed to be or has been made on the grounds that it is authorised by subsection (4), section 17(1) shall not prohibit the doing of anything in, or for the purposes of, so much of any legal proceedings as relates to the question whether that disclosure is or was so authorised."

19. These provisions plainly have the effect of excluding from the public domain in legal proceedings any product of any interception by a person falling within section 17(3) for which a warrant had been or should have been issued. If a warrant had not been obtained there would be an offence within subsection (2)(a). If it had, the matter would fall within subsection (2)(c), (d) or (e). In either event, the matter would fall within subsection (2) and therefore within the prohibition in section 17(1).

20. The inclusion in section 17(2) of an offence under section 1(2) of the Act poses an obvious problem of interpretation given the very sweeping language in which section 17(1) is expressed. The requirement in section 17(2)(a) that the conduct must be by a person falling within subsection (3), and the listing in that subsection of persons and bodies involved in the warrantry regime, strongly suggest that the focus of the prohibition is, as in the 1985 Act, on that regime. It is also relevant to recall that interception of a private telecommunication system is only criminal under section 1(2)(a) if without lawful authority and section 18(4) expressly provides that section 17(1)(a) shall not prohibit the disclosure of the contents of a communication if the interception of that communication was lawful by virtue of section 3 or section 4. In other words, disclosure is not prohibited if the interception was lawfully authorised under those sections. It would be absurd to conclude that there could be no enquiry to establish whether the interception was lawfully authorised or not, and whether or not the interceptor's conduct was excluded from criminal liability under section 1(6). In a civil claim under section 1(3) such an enquiry would be

inevitable. Given the obvious public interest in admitting probative evidence which satisfies the requirements of sections 1(6), 3 and 4, and the absence of any public interest in excluding it, I am satisfied that a court may properly enquire whether the interception was of a public or private system and, if the latter, whether the interception was lawful. If the court concludes that it was public, that is the end of the enquiry. If the court concludes that it was private but unlawful, that also will be the end of the enquiry. If it was private but lawful, the court may (subject to any other argument there may be) admit the evidence.

21. This construction is, in my opinion, strongly supported by the Explanatory Notes issued on the 2000 Act following its receipt of the Royal Assent in July 2000. That reference may properly be made to such material as an aid to construction of a Bill was established in *R (S) v Chief Constable of the South Yorkshire Police* [2004] UKHL 39, [2004] 1 WLR 2196, 2199-2200, para 4, following *R (Westminster City Council) v National Asylum Support Service* [2002] UKHL 38, [2002] 1 WLR 2956, 2957-2959, paras 2-6, and I have no reason to think that these Explanatory Notes on the Act differed from those on the Bill. The commentary on section 17 reads:

> "Section 17: Exclusion of matters from legal proceedings
>
> 136. Section 17, subject to certain exceptions, prohibits evidence, questioning or assertion in (or for the purposes of, or in connection with) legal proceedings likely to reveal the existence or absence of a warrant. A similar provision is contained in section 9 of the Interception of Communications Act 1985, which this Act repeals.
>
> 137. *Subsection (1)* imposes the basic prohibition. It does this directly, by stating that the contents of intercepted material and associated communications data may not be disclosed, and indirectly by prohibiting the disclosure of any suggestion that actions under subsection (2) have occurred.
>
> 138. *Subsection (2)* describes the actions which may not be disclosed, including actions by persons named in subsection (3) which would constitute offences under this Act or section 1 of the 1985 Act.
>
> 139. *Subsection (3)* lists the people referred to in subsection (2)(a). They are people who may be in possession of information about authorised interception. In paragraph (3)(b) persons holding office under the

> Crown includes constables and, by virtue of Section 81(b), Crown servants and members of the Armed Forces."

The note on section 18(4) provides:

> "*Subsection (4)* allows the disclosure of the contents of a communication if the interception was lawful without the need for a warrant by virtue of Sections 1(5)(c), 3 or 4. This means that interception carried out in those circumstances may be evidential."

22. In the case of W the interception took place before the passing of the 2000 Act and the trial took place after it. This affected the questions referred by the Attorney General which, as amended during argument in the Court of Appeal, were these:

> "1. Does section 17(1) of the 2000 Act operate so as to prevent, in criminal proceedings, any evidence being adduced, question asked, assertion or disclosure made or other thing done so as to ascertain whether a telecommunications system is a public or a private telecommunications system?
>
> 2. Is the answer to question 1 above different if the evidence being adduced or question asked etc relates to events which took place before the 2000 Act came into force?
>
> 3. Where an interception of a communication has taken place on a private telecommunications system, is it permissible in criminal proceedings to ask questions or adduce evidence etc to establish that the interception has been carried out by or on behalf of the person with the right to control the operation or use of the system
>
> (a) where the interception took place before the 2000 Act came into force; and
>
> (b) where the interception took place after the 2000 Act came into force?

To the first two questions the Court of Appeal answered No, and I agree with those answers. To question 3(a) it answered Yes, and again I agree. To question 3(b) it answered "Yes, subject to the facts of a

particular case". While I am unsure that the qualification is really necessary, I would accept this answer also. On each of these points, I agree with the opinion of all my noble and learned friends.

LORD NICHOLLS OF BIRKENHEAD

My Lords,

23. I agree with the views expressed by all your Lordships. The problem arises out of section 17 of the Regulation of Investigatory Powers Act 2000. The basic object of this provision appears to be to preserve the secrecy of the warrant system. Section 17(1) seeks to achieve this object by excluding evidence on several points. It excludes evidence tending to suggest that an interception warrant has been issued. It also excludes evidence tending to suggest that the police or other persons listed in section 17(3) have committed an offence under section 1(1) or (2) by making an intercept without lawful authority.

24. This latter provision is widely drawn. Indeed, if section 17 were to stand alone it would apply too widely. It would apply to cases where the warrant system was not in any way involved in obtaining the intercept. Interception pursuant to a warrant issued under section 5 is only one of the circumstances where a person may have lawful authority to intercept a communication. Interception may also be authorised under sections 3 or 4 of the Act, or section 1(5)(c).

25. Take a case where the prosecution assert that both the sender and the intended recipient agreed to the interception, as envisaged by section 3(1). Court investigation of whether that was the position and, if it was, disclosure in court of the contents of the intercept would not damage the warrant system. It would not damage the warrant system even if a challenge by the defendant to the assertion that the interception was authorised under section 3(1) suggested that an offence had been committed under section 1(1) or (2).

26. So section 18(4) cuts down the width of section 17 in such cases. Section 17(1)(a) does not prohibit disclosure of the contents of a communication if interception was lawful by virtue of section 1(5)(c), 3

or 4. Section 18(5) takes the further, consequential step of permitting the doing of anything in legal proceedings relating to the question whether disclosure was authorised on one of those grounds. This enables the defendant to have a proper opportunity to test the prosecution evidence that the interception was duly authorised as alleged.

27. Thus far there is no difficulty. The difficulty which has arisen concerns *other* ingredients of the offence created by section 1(2). No offence is committed under section 1(2) if the interception is in course of transmission by a private telecommunication system and the interception was made by the person in charge of the system ('with a right to control the operation or the use of the system') or with his consent: section 1(2), (6). The question which arises is this: if the prosecution seeks to give evidence of the contents of an intercept as properly admissible on the basis that the interception was of a communication in the course of transmission by means of a *private* telecommunication system carried out with the consent of the person in charge of that system, can the defence advance a case that the place where the intercept occurred was part of a *public* telecommunication system even though this might involve the suggestion that an offence had been committed under section 1(1) by a person mentioned in section 17(3)?

28. Like all your Lordships I am in no doubt that the answer to this question is 'yes'. Investigating this issue, essential to the conduct of a fair trial, would not imperil the secrecy of the warrant system. Investigation of the 'lawful authority' grounds specified in section 1(5)(c), 3 or 4, essential to a fair trial when those issues are raised, would not imperil the secrecy of the warrant system, and Parliament has expressly cut down the width of section 17 to enable such an investigation to take place. The Act makes no comparable provision on the point now under consideration but it is impossible to suppose Parliament intended the position should be different. The rationale underlying the exclusionary provision in section 17 is as much absent in the case now under consideration as it is in the 'lawful authority' instances mentioned in sections 1(5)(c), 3 and 4. Section 17 must therefore be interpreted as inapplicable as much in the type of case now under consideration as it is in the cases specifically mentioned in section 18(4). Any other result would lack rational justification. It would serve no useful purpose, and would have the bizarre effect of rendering the offence-creating provision of section 1(2) nugatory in circumstances where disclosure would not jeopardise the operation of the warrant system. It would also make the civil liability provision in section 1(3)

unworkable. A statute should be interpreted so as to avoid such results if at all possible. I would therefore answer the questions raised by the Attorney General in the way proposed by my noble and learned friend Lord Bingham of Cornhill.

LORD STEYN

My Lords,

29. The Regulation of Investigatory Powers Act 2000 is not easy to understand. On the other hand, there is a foothold or two to which one can cling in regard to the central question posed by the Attorney General, viz whether a court may investigate whether intercept material relied on by the Crown has been obtained by tapping a private as opposed to a public telecommunication system.

30. For my part, the critical matter is that explained in para 14 of the opinion of my noble and learned friend Lord Bingham of Cornhill. Before the statute of 2000 was enacted the clear understanding was that a court may examine whether an interception was made within a public or private system. Of course, Parliament could have legislated to place such an examination beyond the power of the court. If that had been intended, one would have expected the structure and scheme of the 2000 Act to have made that crystal clear. Neither the text of the 2000 Act, nor any of the external aids to its construction, give any indication that such a radical change of policy was intended.

31. It is true, as Lord Bingham has pointed out, that the inclusion in section 17(2) of an offence under section 1(2) of the Act creates a linguistic difficulty given the language in which section 17(1) is expressed. In my view, however, this point is decisively outweighed by a purposive interpretation of the statute. No explanation for resorting to purposive interpretation of a statute is necessary. One can confidently assume that Parliament intends its legislation to be interpreted not in the way of a black letter lawyer, but in a meaningful and purposive way giving effect to the basic objectives of the legislation. So approached the answer to the central question is obvious: a court may enquire into the question whether tapping took place on a private system.

32. I am in full agreement with the opinion of Lord Bingham. I would answer the Attorney General's questions as Lord Bingham proposes.

LORD HOPE OF CRAIGHEAD

My Lords,

33. The crux of the problem that your Lordships have been asked to resolve in this case is to be found by comparing section 1(6) with section 18(4) of the Regulation of Investigatory Powers Act 2000. Section 1(2) of the Act creates a new offence, which is the unlawful interception of a communication in the course of its transmission by means of a private telecommunication system. With this in mind, section 1(6) provides:

> "The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that his conduct is excluded from criminal liability under subsection (2) if –
>
> (a) he is a person with a right to control the operation or the use of the system; or
>
> (b) he has the express or implied consent of such a person to make the interception."

Section 18(4) provides:

> "Section 17(1)(a) shall not prohibit the disclosure of any of the contents of a communication if the interception of that communication was lawful by virtue of section 1(5)(c), 3 or 4."

34. Section 17(1)(b) of the Act provides that, subject to section 18, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with

any legal proceedings which tends to suggest that anything falling within subsection (2) of that section has or may have occurred or be going to occur. The conduct referred to in section 17(2) includes conduct that was or would be an offence under section 1(2). Section 18 provides a list of exceptions to the prohibitions that are set out in section 17(1). Absent from that list is a reference to section 1(6). As has been shown, section 1(6) is not mentioned in section 18(4). That is however where a reference to this subsection might have been expected. Nowhere else is it provided in terms by the Act that an interception of a communication without a warrant in the course of its transmission by a private telecommunication system by a person with the right to control that system or with the express or implied consent of such a person is lawful. The furthest the Act goes is to provide in section 1(6) that an interception in these circumstances is excluded from criminal liability.

35. Mr Roberts QC for the acquitted person submits that the Act is so carefully drawn that the list of exceptions in section 18 must be treated as comprehensive. He points out that nowhere in the Act is the situation that has arisen in this case provided for. The place where one would expect that provision to have been made, he says, is section 18(4). But there is no reference there to section 1(6) and, when it is read on its own, all section 1(6) does is provide a defence to a criminal prosecution. It does not provide that an interception in the circumstances which it describes is to be regarded for all purposes as lawful. It could not, of course, go that far. That would be to preserve the defect in the pre-existing system of statutory control that was identified in *Halford v United Kingdom* (1997) 24 EHRR 523. That defect has been remedied by section 1(3). That subsection provides that an interception in the circumstances which it describes which is made without lawful authority shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication. The conclusion must be that it would not have been consistent with the way in which the Act has been drafted to include section 1(6) in the list of exceptions that section 18(4) sets out.

36. The question then is whether what Steyn LJ helpfully described in *R v Effick* (1992) 95 Cr App R 427, 432 as "the forbidden territory" is drawn in this Act in such a fashion as to preclude any evidence being adduced or question asked in order to ascertain whether a telecommunication system which has been used to transmit a communication that has been intercepted is a public or a private telecommunication system. One has only to look at section 1(3)(a) to see that there can be only one answer to that question. As Mr Perry for the Attorney General was right to point out, the question whether the

interception of the communication with the consent of a person having the right to control the operation or use of a private telecommunication system was made in the course of its transmission by means of the private system must be capable of being explored in the civil proceedings which are provided for by that subsection. Otherwise the mere assertion that the system was a public and not a private system would defeat the right of action. The Act does not say in terms that this is a question that can be explored in evidence in these proceedings, and the absence of a reference in section 18 to section 1(3) in its list of exceptions to section 17 might be said, if Mr Roberts is right, to indicate that this is prohibited. But it is plain that the question must be capable of being explored in evidence if effect is to be given to section 1(3).

37. One answer to the problem which this case raises, therefore, might be to say that a rectifying construction should be given to the Act of the kind described by Lord Herschell LC in *Institute of Patent Agents v Lockwood* [1894] AC 347, 360, when he said:

> "You have to try and reconcile [the provisions] as best you may. If you cannot, you have to determine which is the leading provision and which the subordinate provision, and which must give way to the other."

But I do not think that it is necessary to go that far. The statute does not in terms prohibit the line of questioning that was sought to be developed in this case. On the contrary, section 1(3) opens the door to it in civil proceedings. And, if the door is open in civil proceedings, why should it not be open in criminal proceedings too in a case where the question whether the communication was by means of a public or a private telecommunication system is a relevant question?

38. In *Morgans v Director of Public Prosecutions* [2001] 1 AC 315 Lord Mackay of Clashfern explored the problem of reconciling the prohibition in section 9 of the Interception of Communications Act 1985 with the exception to the offence created by section 1(1) of that Act which was set out in section 1(3). He said, at pp 319-320, that a construction of section 9 should be sought which gave effect to the limits of the scheme of the Act described by Lord Mustill in *R v Preston* [1994] 2 AC 130, namely that the scheme described did not apply except to situations in which a warrant was required and where, without it, the interception would be without statutory authority:

> "The challenge is to find a construction of section 9 which would provide a workable boundary. The difficulty is that any discussion in evidence of the question whether a particular exception to section 1 applied would be in essence a discussion of whether or not the interception resulted from an offence under that section. I have reached the view that this is best dealt with by saying that in construing section 9, it should not apply where the proceedings are for the enforcement of any enactment relating to the use of postal or public telecommunications services or where the proceedings relate to a communication being transmitted by wireless telegraphy and the communication is intercepted by the authority of the Secretary of State."

39. The particular problem which Lord Mackay was discussing in *Morgans* has been dealt with expressly by section 18(4) of the 2000 Act, which provides that section 17(1)(a) – which has replaced section 9(1) of the 1985 Act – shall not prohibit the disclosure of any of the contents of a communication if the interception of that communication was lawful by virtue of sections 1(5)(c), 3 or 4. Section 3(3) authorises the interception when it takes place for a purpose associated with the provision or operation of a telecommunications service. It puts that material expressly into the permitted territory. But the way in which Lord Mackay solved the problem is, I believe, open to your Lordships in this case also. That was the view of the Court of Appeal, and I too would adopt it: see [2003] 1 WLR 2902, 2928, paras 93-95.

40. The forbidden territory is now much more closely and carefully defined by the 2000 Act than it was by the 1985 Act. Nevertheless I think that a workable boundary between what is forbidden and what is not can be said to exist where the only questions to be explored in evidence are whether a telecommunication system is a public or a private telecommunication system and, if so, whether the interception was made by or with the consent of the person with the right to control the operation or use of that system: see section 1(6). These, plainly, are questions that can be explored as a defence to a prosecution under section 1(2) of the Act, and as has already been said the question whether the telecommunication system was a private system must be capable of being explored if effect is to be given in civil proceedings to the remedy which is provided by section 1(3). So it cannot be said to be contrary to the policy of the Act to hold that these questions are outside the forbidden territory. The policy of the Act, as the conduct referred to in section 17(2) and the list of the persons referred to in section 17(3)

indicate, is to regulate and protect the surveillance process. It will not be impeded by permitting evidence to be adduced or questions asked and answered simply in order to ascertain whether a particular telecommunication system is a public or a private system in any proceedings in which an answer to that question is relevant.

41. For these reasons, and those in the speech of my noble and learned friend Lord Bingham of Cornhill with which I am in full agreement, I too would answer the questions referred by the Attorney General as Lord Bingham proposes.

LORD WALKER OF GESTINGTHORPE

My Lords,

42. I have had the privilege of reading in draft the opinion of my noble and learned friend Lord Bingham of Cornhill. I agree with it and for the reasons which Lord Bingham gives I would answer the Attorney General's questions as he proposes.

43. I add one brief footnote to the problem of why section 17(2)(a) of the Regulation of Investigatory Powers Act 2000 ("the Act") refers to an offence under section 1(2) (as well to an offence under section 1(1)) of the Act. By section 5(1)(a) of the Act the Secretary of State may issue a warrant for interception of communications transmitted by means of a private telecommunication system (see the definitions in section 2(1)). The House was told that such action would be very unusual, if not unprecedented, but it is at least a theoretical possibility.

44. The reference in section 17(2)(a) to section 1(2) may therefore have been included in order to avoid any possible gap in the protection which Parliament intended to extend to any form of warranted interception. The need for the conduct in question to be that of a person falling within section 17(3) does, as Lord Bingham points out, keep the focus of the prohibition on the warrant regime.