JUSTICE'S RESPONSE TO THE GOVERNMENT CONSULTATION PAPER 'INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM'

Introduction

JUSTICE welcomes the government Consultation Paper *Interception of Communications in the United Kingdom*. The Consultation Paper proposes a revision of the Interception of Communications Act 1985, which is necessary to implement the *Halford* judgment of the European Court of Human Rights.

The 1998 JUSTICE report, *Under Surveillance*, strongly argued that the 1985 Act needs to be updated in the light of technological developments such as those highlighted in *Halford*, as well as to strengthen human rights safeguards. We welcome many of the changes that are now proposed, such as the extension of the coverage of the Act to include private networks, the introduction of a proper regime for disclosure of communications data and the proposal for a statutory Code of Practice to clarify the circumstances in which an application for an interception may be made.

However, there are a number of significant omissions. The Consultation Paper does not discuss the practice of 'participant monitoring' (where one party only consents to interception), nor does it propose any changes to the powers or procedures of the Interception of Communications Tribunal. In the light of recent cases before the European Court of Human Rights, JUSTICE would argue that changes are required on both matters. Also, while the Consultation Paper acknowledges that intrusive methods such as the use of listening devices raise similar human rights issues to the interception of communications, it does not consider whether both methods of surveillance should be regulated within a single legal framework (as is the case in several other countries). Although it would involve a more

radical programme of legislative amendment, such an approach could overcome the difficulty of legislative provisions falling behind technology and prevent the gaps in coverage that have arisen in IOCA and still exist in Part III of the Police Act 1997.

Finally, we remain concerned that important developments with regard to interceptions law and policy are being carried out separately from this consultation exercise. Our 1998 report criticises existing law on the interception of communications for having been developed in a piecemeal and ad hoc fashion; we are anxious that the revised Interception of Communications Act should follow a more integrated approach. We therefore consider that the interception of encrypted electronic communications, currently the subject of a draft Bill published by the Department of Trade and Industry, should be included within the framework of the present consultation exercise. Likewise, we are concerned that the present consultation exercise must take into account, and is likely to be affected by, negotiations on the EU Convention on Mutual Legal Assistance.

THE SCOPE OF THE LEGISLATION

Electronic communications and the definition of interception

1.1 JUSTICE welcomes the proposed extension of the scope of the Act to 'all telecommunications networks', regardless of the means of communication. This implements the *Halford* judgment and would provide an unambiguous legal basis for the interception of all telecommunications.

1.2 However, the draft Electronic Communications Bill which has been published by the Department for Transport and Industry appears to accept that certain electronic communications may continue to fall outside the scope of IOCA. Schedule 1 of this Bill prescribes different procedures for serving decryption notices depending whether the e-mail was obtained under a PACE, IOCA or Police Act warrant, or under the Data Protection Act. In our 1998 report, we criticised the fact that the interception of e-mail could fall under a number of separate legal regimes. It would be unacceptable if this situation were to continue even after the present consultation exercise: as the Consultation Paper states, IOCA ought to provide the legal framework for all interceptions. JUSTICE would welcome clarification on this issue.

1.3 The debate over what constitutes an 'interception' is a related issue. As discussed in our 1998 report, there has been some question as to whether the current interpretation of the term limits the scope of the Act: the Court of Appeal has held that 'the interception of a communication takes place when, and at the place where, the electrical impulse or signal which is passing along the line the telephone line is intercepted in fact.'[1] Such an interpretation would cast doubt over the legality of mobile phone interceptions, which by definition do not pass through an elaborate cable network, or the interception of e-mail which is sent in a number of separate information 'packets'.

1.4 To remove any ambiguities, it might be helpful to include a statutory definition, on the face of the Act, of what constitutes an 'interception'.[2]

[1] *Ahmed and others*, CA 29 March 1994, unreported, *per* Evans LJ

[2] *cf* the United States Code, 18 US 2510

Monitoring for business purposes

1.5 The consultation paper says that it is not proposed that the warranted interception regime should apply to the recording or monitoring of communications for lawful business purposes. It says that there are a number of legitimate reasons why employers or businesses may wish to monitor in this way. However, the paper also recognises the need to protect the rights of employees and those members of the public affected by using a monitored service.[3]

1.6 In this respect, the Government seems to presume that, so long as employees are told that interception of communications may occur, they can have no reasonable expectation of privacy and, therefore, no Article 8 issue arises. We believe that this is too wide an exclusion: awareness of monitoring cannot *ipso facto* be relied upon as removing the right to privacy. Telephone conversations taking place at work and mail sent to the workplace may fall within the concept of 'correspondence' in Article 8[4]; interception could then potentially breach Article 8 irrespective of any awareness on the part of workers that it was taking place. Further, since the development of relationships at and through work is an aspect of private life, some minimum guaranteed space for privacy may be required by Article 8. As the ECtHR stated in *Niemietz*:[5]

> "Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.
>
> There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world..."

1.7 It would be a surprising result if an employer could effectively remove *any* private interests of the workforce through a simple notice saying, for instance, that all communications may be monitored. It is therefore unlikely that merely informing workers that monitoring or recording is taking place can have the effect of removing any reasonable expectation of privacy. We would consider that principles of necessity and proportionality require further safeguards, such as guidance from employers as to the circumstances in which monitoring will occur, why it is necessary and the use that will be made of the information so generated (e.g. whether the information will ever be disclosed to third parties). In

---

[3] Paras. 3.9 and 4.6

[4] See *A v France* (1994) 17 EHRR 462 at 476-7: a phone conversation was protected because it constituted "correspondence". Therefore there was no need to consider whether recording infringed applicant's private life. See also the Commission in *Halford* case at paras 55-57, and the Court at para 43

addition, it is important that employees have some private space at work, where they know they will not be monitored.

1.8 In that light we suggest that the following additional restrictions should be incorporated into statute. These aim to ensure that any interference is proportionate and will meet the requirements of Article 8:

- as well as specifying that interception may occur, the employer should be under an obligation to inform and explain to its workforce the *purpose* of the monitoring and the method(s) adopted; and it should be a requirement of the legislation that the purpose is specific (and not vague), lawful and relevant to work.[6] This should help to ensure that monitoring is done for a legitimate purpose and not merely to spy on workers. Such a principle is consistent with the law on data protection, with its requirement of specified lawful purposes,[7] and offers a clearer justification than the vague phrase 'in the course of lawful business'.[8]

- because the information obtained may relate to private matters, restrictions should be placed on what an employer or the holder of the information may do with it. In some cases the recordings will fall within the Data Protection Act 1998, and will thus be subject to protection in accordance with that Act.[9] But we suggest that this should be the case for all information obtained as a result of the interception of communications. The most straightforward amendment, we suggest, would be to deem that all information so generated falls within the Data Protection Act 1998, so that workers can discover what information is being collected, for what purposes, and to whom it may be disclosed. Alternatively, the employer should be obliged to comply with the Data Protection Act principles in relation to information obtained by intercepting employees' communications.[10]

- employers should be required to consult with employees and/or their representatives before interception systems and procedures are put in place, unless the interception is

---

[5] *Niemietz v Germany* [1991] Series A no 251-B

[6] As an example, the ILO Code of Practice on the Protection of Workers' Personal Data, adopted at the meeting of experts at Geneva on 1-7 October 1996, states that personal data should only be processed "for reasons directly relevant to the employment of the worker"

[7] See e.g. Section 4(4) and Schedule 1 Data Protection Act 1998

[8] The phrase in para 4.6 of the Consultation Paper

[9] That Act will apply if "specific information relating to a specific individual is readily accessible": Section 1(1), Data Protection Act 1998

[10] See the principles contained in Schedules 1 and 2 of the Data Protection Act 1998.

permitted to take place in conditions of secrecy (see below).[11] Employers are already subject to such an obligation with regard to the introduction of new technologies in the field of health and safety.[12] A similar obligation in relation to interception of communications will help, to some extent, to redress the imbalance of power between employees and employers. Such an obligation is a feature of the legal system of other European countries.[13]

- employees should be permitted some space where they know that they can communicate in conditions of privacy, consistent with Article 8 ECHR and the *Niemietz* case. If, for example, employees' phone calls are monitored, a telephone for private purposes should be provided on the premises. The same should apply to other forms of surveillance operating in the workplace, including aural monitoring and CCTV recording.

1.9 We suggest that the proposed Code of Practice should lay down guidelines for the monitoring of employees' communications.

1.10 As a more general point, we think that it is important that the amended IOCA dovetails into the procedures to be adopted under the Data Protection Act 1998. Given that at least some information obtained by intercepting communications will fall within that Act, it seems sensible for the two regimes to work together. The Data Protection Commissioner has announced that she intends to issue a code of practice on the use of personal data at work, based on a study report that she has commissioned.[14] This will seek to lay down some restrictions on the surveillance of employees.

1.11 The Consultation Paper states that 'specific authorisation' will be necessary for secret interception on non-public networks, although it gives no further details of how it is proposed that this should operate in such situations as the workplace. For example, is it proposed that such interceptions be allowed on grounds which are broader than those set out in Section 2 of IOCA (serious crime, national security and economic well-being of the UK) and, if so, what are the additional grounds? Likewise, if such interception is not to fall within the IOCA warranting regime, what will be the nature of the 'specific authorisation' and from whom is it to be sought? Where an employee is suspected of serious crime, is it

---

[11] As proposed by the Conference of European Data Protection Commissioners in "Telecommunications and Privacy in Labour Relationships": Data Protection Registrar, *Privacy at Work* (1997)

[12] See the Safety Representative and Safety Committees Regulations 1977, reg 4A(1)(e) and the Health and Safety (Consultation with Employees) Regulations 1996 reg 3(e)

[13] See e.g. the example of Austria, Belgium, France, Finland Germany, the Netherlands and Sweden, cited in the International Labour Office, *Conditions of Work Digest on Workers' Privacy, PT 11: Monitoring and Surveillance in the Workplace* (Geneva: 1993) at pp 53-55

[14] PPRU Study Report, *The uses and misuses of personal data in employer/employee relationships*, January 1999

to be the responsibility of law enforcement agencies to intercept or may the employer do so and will this be under the IOCA regime? Is it intended that the Interception of Communications Tribunal will have the power to investigate and the Commissioner the power of oversight over private sector, as well as state, interceptions?

1.12 These are extremely important issues that raise complex legal and policy considerations which are not discussed in the consultation paper. We believe that there cannot be proper consultation on this until there is greater clarification. For example, there are strong grounds for saying that an interception falling within the serious crime criteria is a law enforcement matter that should remain the sole responsibility of agencies such as the police. It would be wrong in principle to allow employers to engage in practices in the workplace that, if carried out by a law enforcement agency, would require special authorisation or possibly be prohibited altogether. However, the difficulty would then arise of where to draw the line between this and an employer's right to intercept, for example, for less serious criminal conduct.

1.13 A further point to be noted is the possible disparity that may be created under the Human Rights Act between different categories of employer. The Act will require that interceptions by public authorities in the workplace comply with the requirements of Article 8, including the lawful purpose exemptions under 8(2), which arguably does not include criminal conduct which is less than serious. It could be argued that non-public bodies and business will not be so restricted in the way that they may secretly intercept employees communications. This would create an anomaly in terms of individual privacy protection and safeguards particularly in employment situations.

1.14 In addition to criminal penalties for infringement of IOCA, no evidence obtained in breach of the Act should be admissible before any tribunal or court (see also Paragraph 4.11 below). This would in practice operate as an important deterrent to breaches.[15] We suggest, further, that an employer should not be able to subject an employee to detriment as a result of information obtained in breach of the IOCA.

Participant monitoring

1.15 The consultation paper also fails to consider the existing exemption for 'participant monitoring', despite the fact that this practice has implications for compliance with Article 8 of the ECHR. Under Section 1(2)(b) of IOCA, an exemption applies where one party to the communication consents to it being intercepted. This has the effect of

circumventing the procedures and safeguards of IOCA: in particular, no warrant is needed and the Commissioner and Tribunal do not have jurisdiction to review the legality of the interception. Commonly referred to as 'participant monitoring', the exemption is particularly relevant in cases where police or informers are used to extract evidence from suspects, and give their consent to the monitoring of communications.[16]

1.16 JUSTICE believes that it is strongly arguable that such an exemption directly contradicts the principle that it is the person whose privacy is infringed who should be afforded safeguards. The exemption therefore potentially breaches Article 8 of the ECHR. We consider that the same reasoning as the European Court of Human Rights applied in the case of *Lambert v France*[17] may be applied to the consent exemption under IOCA. In that case, the Court considered a judgment of the French Court of Cassation which had denied legal recourse to a person whose telephone calls had been intercepted on a friend's line. It held that, as a matter of principle, Article 8 protects people, not telephone lines:

> "[T]he Court of Cassation's reasoning could lead to decisions whereby a very large number of people are deprived of the protection of the law, namely all those who have conversations on a telephone line other than their own. That would in practice render the protective machinery largely devoid of substance." [18]

1.17 A recent Report and Consultation Paper[19] by the Irish Law Commission discusses the issues around participant monitoring exemptions in some detail. It recognises (as does the consultation paper: see Paragraphs 1.5-14 above) that there may be legitimate business reasons for the practice. For instance, many banks routinely record telephone calls and notify their customers of this practice. However, this must be distinguished from a one-sided consent interception which is made on behalf of the state. The Commission's report concludes that it is undesirable that the police should be allowed to circumvent statutory safeguards by using an informer or undercover officer to carry out an interception.[20]

---

[15] See the reasoning of the Swedish court in *State Prosecutor v Turid Johannessen*, cited in the ILO report, *Monitoring and Surveillance in the Workplace* , op.cit. p 64

[16] For such a case, see *R v Rasool and another* [1997] CrimLR 448

[17] [1999] EHRLR 123

[18] At Paragraph 38

[19] The subsequent report refers back to the Consultation Paper in this regard

[20] It should be noted that Article 8 and the issue of participant monitoring was not argued in the case of *Smith v UK* (1997) EHRLR 277

1.18 This reasoning follows the decision of the Canadian Supreme Court in the case of *R v Duarte*. This was a case where an informer had been wired up to record conversations between himself and the suspect. While the Canadian Criminal Code required a warrant for electronic surveillance generally, none was needed for such consent operations. Delivering the judgment of the Court, La Forest J held that it was a violation of the defendant's right to privacy:

> "I am unable to see any logic to this distinction between third party electronic surveillance and participant surveillance. The question whether unauthorised electronic surveillance of private communications violates a reasonable expectation of privacy cannot, in my view, turn on the location of the hidden microphone. Whether the microphone is hidden in the wall or concealed on the body of a participant to the conversation, the assessment whether the surreptitious recording trenches on a reasonable expectation of privacy must turn on whether the person whose words were recorded spoke in circumstances in which it was reasonable for that person to expect that his or her words would only be heard by the persons he or she was addressing."[21]

1.19 Following this decision, Section 184.2 of the Canadian Criminal Code now requires judicial authorisation for the interception of a private communication even where a party to it consents. The only exception is where there is a risk of bodily harm to the consenting person. Similarly, new legislation in the Netherlands does not exclude participant monitoring from the statutory regime.[22]

[21] *R v Duarte* [1990] 53 CCC (3d) 1

[22] The Special Investigative Powers Bill, passed in May 1999

INTERNATIONAL DEVELOPMENTS

2.1 Within the European Union, the issue of assistance between Member States in carrying out telecommunications interceptions has been under negotiation for some time in the context of the draft EU Convention on Mutual Legal Assistance.

2.2 The Consultation Paper states that this Convention will provide a legal basis for international interceptions in two circumstances: seeking technical assistance to implement an interception warrant against a person on the territory of the intercepting Member State; and seeking the co-operation of another Member State to intercept a person on its territory. An example of the first would be where a person in the United Kingdom uses a satellite phone the signals from which are fed through a ground station in Italy.[23] If UK police wanted to intercepted such communications, they would need the assistance of the Italian authorities. An example of the second would be where an individual is under investigation by UK authorities, and they wish to intercept his mobile phone communications while he is abroad.

2.3 JUSTICE acknowledges the need for international assistance in such cases. However, we are concerned that negotiations on the interception provisions of this Convention have been in progress since early 1997. EU Member States have not been able to agree on a consensus, and the wording of the relevant provisions has been changed several times. Apparently, the current draft remains unacceptable to the Italian Government for constitutional reasons, while the UK still has a problem with its wording.[24] Therefore, it is unlikely that the provisions as set out in the Consultation Paper (at Paragraph 6.2) will remain the same.

2.4 JUSTICE has given evidence on the EU Convention to the European Scrutiny Committees of both Houses of Parliament. In our evidence, we questioned whether the provisions should be included in the Convention at all. Because of technological developments, the issue of telecommunications interceptions has now become so complex that JUSTICE believes it should be dealt with in an intergovernmental Convention of its own, with proper supervision and control mechanisms to safeguard individuals rights. Such a Convention should also deal with the kind of issues dealt

[23] As is the case with the existing Iridium system

[24] As stated in evidence by the Parliamentary Under-Secretary of State for the Home Office before the House of Commons European Scrutiny Committee, 19 May 1999

with in the 'ENFOPOL 98' paper, a draft Council resolution on the interception of satellite and internet-based communications.

2.5 As no clear conclusions have yet been reached on the EU Convention, it is very important that the continuing discussions should be transparent and should be fed into the consultation process and the parliamentary consideration of any proposed legislation. Any decisions reached at EU level would clearly affect both these processes.

External warrants

2.6 Under Section 3(2) of IOCA a warrant may be issued to intercept external communications sent or received outside the UK. These are issued simultaneously with a certificate specifying the description of material to be examined. Section 6(1)(b) prohibits reading, looking at or listening to any material which is not covered by the certificate.

2.7 Although the consultation paper does not invite discussion on these warrants, the manner in which they operate has been the subject of comment and criticism. This has particularly questioned the adequacy of the safeguards and highlighted the following:

- *the limited jurisdiction of the Interception Tribunal over external warrants*: the Tribunal may only consider an application from a person where the certificate specifies an address within the UK that is likely to be used by the applicant. However Section 3(3) says that an address in the UK may only be specified in cases involving terrorism. It is therefore arguable that there is no effective remedy in terms of Article 8 in relation to other communications falling within these warrants and certificates;
- *the practical effect of the examination limitation under Section 6(1)(b):* it is unclear, particularly in the context of new technology, to what extent it is necessary that all intercepted material should be examined in order to identify the material which is authorised under the certificate;
- *the lack of accountability*: the lack of any published figures on the number of warrants and the extent to which these overlap with Section 3(1) warrants are examples of the secrecy surrounding such warrants.

2.8 JUSTICE considers that these issues ought to be addressed in order to provide greater clarity and transparency in the procedures, and that external warrants should be subject to the same safeguards as ordinary warrants.

WARRANTRY PROCEDURES

3.1 JUSTICE acknowledges the need to change some of the procedures governing the authorisation of warrants and we particularly welcome the introduction of a Code of Practice to bring greater clarity and transparency to the process generally. As with the Code under Part III of the Police Act, we would wish to see detailed guidance on such matters as the nature of the information that should be recorded on the initial application and the recording of the interception outcome. The need for detailed data protection guidance to back up the current Section 6 IOCA safeguards is also an issue that we anticipate will be covered in the Code.

Authority to intercept

3.2 The question of who should authorise telephone interceptions is an important one. The European Court of Human Rights has on several occasions stressed the importance of judicial oversight. In *Klass v Germany*, it stated that 'it is in principle desirable to entrust supervisory control to a judge'.[25] Likewise, in discussing the safeguards offered by French law on telecommunications interceptions, it placed considerable emphasis on the safeguard of prior judicial authorisation.[26]

3.3 The 1985 Act requires interceptions to be authorised by the Secretary of State. The Consultation Paper says that, while other authorisation frameworks have been considered, the Government is 'not persuaded' of the need to depart from this procedure. However, the paper does not give any detail of the reasons for this decision, other than that the Executive would still need to issue warrants applied for on national security grounds, which might lead to parallel warranting arrangements.

3.4 JUSTICE's preferred position is set out in our 1998 report: authorisations for telecommunications interceptions should be given by a person holding high judicial office. This is the practice in a great number of other countries, including Canada, New Zealand, the United States, and European Union Member States. It would also have the additional advantage of bringing the law on the interception of telecommunications in line with the Police Act regime for intrusive surveillance. There are also practical considerations for favouring a judicial authorisation regime: the

[25] *Klass v the Federal Republic of Germany* (1978) 2 EHRR 214, at Paragraph 56

[26] *Huvig v France* (1990) 12 EHRR 528, at Paragraph 33: "The Court does not in any way minimise the value of several of the safeguards, in particular the need for a decision by an investigating judge, who is an independent judicial authority…"

sharp rise in the number of serious crime applications makes it increasingly impractical for the Home Secretary to scrutinise all applications in person. Judicial authorisation may also assist in some of the evidential problems referred to in paragraphs 4.1-11 below).

3.5 JUSTICE does not consider that the single reason provided in the Consultation Paper against judicial authorisation—the need for a separate regime for police and the security and intelligence services—is compelling. Not only is this common practice in other countries, such as Australia; but also a parallel regime for intrusive surveillance by police and the security services already exists in the UK under Part III of the Police Act 1997 and the Intelligence Services Act 1994.

Criteria to be met

3.6 The consultation paper states that the IOCA criteria in section 2 are not to be amended. JUSTICE would argue, however, that here is a case for ensuring a consistent approach to the grounds for the use of all surveillance methods including those falling under Part III of the Police Act 1997. On the same reasoning, it is also important to ensure that the criteria fully reflect the proportionality tests relating to the nature of the operation and its likely impact on the target persons and those around them, as required by Article 8 of the European Convention on Human Rights.

Duration of warrants

3.7 In his latest Annual Report, the Commissioner describes the practice at the Foreign and Commonwealth Office whereby the Foreign Secretary issued a number of warrants for a duration of less than the statutory period of six months.[27] He criticised this practice, as the 1985 Act does not allow for such flexibility: if the Secretary of State wishes to issue a warrant for less than the statutory period, the only course of action open to him is to cancel the warrant in accordance with Section 4(4) of the 1985 Act.

3.8 The interception of telecommunications is an interference with an individual's right to respect for private life. Article 8(2) of the European Convention on Human Rights requires that such interferences should be kept to the minimum necessary to achieve the stated aim. Therefore, JUSTICE considers that it should be open to the

[27] Interception of Communications Act 1985, Report of the Commissioner for 1998, June 1999, Cm 4364, at pp. 9-10

authorising individual to issue a warrant for a duration of less than the statutory maximum in cases where this is considered appropriate.

Power to attach conditions

3.9 Interferences with privacy may also be minimised by attaching specific conditions to a warrant. For instance, restrictions might be attached to limit interference with solicitor-client privilege or other confidential relationships. With the extension of IOCA to e-mail, conditions could also specify whether or not the monitoring is 'real-time', or, with regard to communications data, the type of information to be provided. This is common practice in other Commonwealth countries. The annual figures published under the Canadian Criminal Code show that conditions are attached to the vast majority of authorisations for electronic surveillance: in 1995, the figure was 95%. This also helps explain the phenomenon of the low number of refusals of warrant applications: rather than refusing a warrant, Canadian judges prefer to grant them but with conditions attached.

Exemption for privileged material

3.10 The Consultation Paper proposes to lay down detailed rules on how to deal with legally or otherwise privileged information in a separate Code of Practice (in Paragraph 7.16). While JUSTICE welcomes the Government's intention to address this important issue, we consider that it should be included on the face of the legislation. This is the approach taken under Sections 98-100 of the Police Act 1997, which lay down strict rules for confidential material and matters subject to legal privilege.

Quashing of warrants

3.11 Under the Interception of Communications Act 1985, only the Tribunal has the power to quash a warrant, after an individual has lodged a complaint. The Commissioner does not have the power to quash warrants: if he finds a violation of the Act, he merely draws up a report to the Prime Minister.

3.12 In contrast, the Intrusive Surveillance Commissioner under Part III of the Police Act 1997 has the power to quash a warrant if he is satisfied that there were no reasonable grounds to order it, or where the surveillance criteria are no longer

applicable.[28] This power applies 'at any time', and is not limited to investigations after a complaint. JUSTICE recommends that the Interception of Communications Commissioner should have powers to quash a warrant similar to those conferred on the Intrusive Surveillance Commissioners.

[28] Police Act 1997, Section 103

USE OF INTERCEPT MATERIAL IN EVIDENCE

4.1 JUSTICE supports the proposal that lawfully intercepted material under IOCA should be *prima facie* admissible as evidence in criminal proceedings, subject to the usual judicial discretion under section 78 of the Police and Criminal Evidence Act 1984 (PACE). It is self-evident that the prohibition results in the loss of extremely useful evidence in the fight against organised crime and terrorism. In our view, public confidence in the official use of and procedures concerning interception would be enhanced by the transparent use of this evidence in legal proceedings; it would also render the process more accountable. It is, of course, also the position under Part III of the Police Act 1997 in relation to the use of surveillance devices; if the objections can be overcome for one form of surveillance, it is hard to see the continued justification for the Section 9 IOCA restrictions. In addition, the recent legislation establishing the Special Immigration Appeals Commission to hear cases involving national security matters specifically states that section 9(1) of IOCA is not to apply to its proceedings. It is also the practice to use such material in evidence in a number of countries including the United States, Canada and Australia.

4.2 We appreciate the concern that such a change could result in criminals making greater use of counter intelligence measures. However, we doubt whether the need to keep ahead of the game is not already a motivating force. Any reasonably alert criminal will no doubt assume that the capacity to intercept exists in relation to the various forms of communication or is likely to in the near future.

4.3 In Chapter 3 of our report, *Under Surveillance*, we examine in detail the fair trial issues arising out of covertly-obtained evidence. It seems to us that two main questions are raised in relation to Article 6. The first is the question of what material should be disclosed to the defendant. This necessarily raises particular questions over disclosure of unused material held by the prosecution and the use of public interest immunity (PII). The second question is the admissibility of evidence obtained by covert means, and in particular whether the prosecution should be able to rely in court on evidence which was obtained unfairly or unlawfully.

Disclosure issues

4.4 There is an argument for saying that the case of *Preston v UK*, cited in the Consultation Paper in support of the Government's stance on disclosure, was largely

decided on its facts. Many practitioners believe that, in different circumstances, the 'equality of arms' principle of Article 6 will result in a *prima facie* duty to disclose intercept material held by the prosecution. They point anecdotally to incidents when it has been obvious that the prosecution has asked questions at trial, based on knowledge obtained from such material.

4.5 If this view is correct, the debate is essentially around the nature of the disclosure regime for such material. We have reached the conclusion that there are no obvious grounds for saying that this material should be treated differently to other kinds of sensitive material. The only exception may be in relation to the material used in support of the warranting procedure which we consider below at Paragraph 4.7. In other words, we believe that the duty to disclose intercept material should be governed by the regime introduced by the Criminal Procedure and Investigations Act 1996: its existence must be recorded by the 'disclosure officer', and the prosecutor should decide whether it should be disclosed either at the primary or secondary disclosure stage and whether it is sensitive material which would not be in the public interest to disclose (see pages 62 - 67 of the 1998 report, Under Surveillance).

4.6 However, as set out in our report, we believe that there should be significant changes to this regime if it is to comply fully with Article 6[29]. For example, we recommend that the trial judge should have the discretionary power to appoint a special counsel (see below at Paragraph 5.3) in those cases where *ex parte* PII hearings are likely to be fundamental to the conduct of the case. We also believe that the court should always be informed of the existence of sensitive material irrespective of whether the prosecutor decides that it is non-disclosable.[30]

4.7 It can be fairly predicted that in some cases disclosure of the content and nature of the warranting process itself may also be in issue.[31] We believe that it will be difficult on Article 6 grounds to maintain the present section 9 exclusion of legal challenges to warrants when interception or other communications data is to be led in evidence. This is because defendants may quite properly seek to challenge the intercept evidence on grounds of the illegality of the initial authorisation and therefore require disclosure of material relating to the warrant application in order to do so.

4.8 This could well raise issues of even greater sensitivity than those involved in disclosing an interception transcript. Nevertheless, we consider that there should be

[29] The case of *Rowe and Davis v UK* currently before the European Court of Human Rights raises the same questions.
[30] Under Surveillance, p. 66

some independent procedure to determine whether, and what, disclosure may be authorised. There are two options for providing this. One is that such decisions should fall within the PII regime covering the disclosure of sensitive material generally. The other is to adopt an alternative procedure, involving the Interception Tribunal. As Tribunal members have a knowledge and expertise in overseeing the warranting process, it may be worth considering a procedure whereby the court refers the determination of any application for disclosure of warrant material to it. This would have the advantage of ensuring a consistent approach and could incorporate some of the Canadian 'judicial editing' procedures mentioned below. However, as with PII *ex parte* hearings, the Tribunal's procedures would need to be substantially amended so as to allow the defendant the necessary measure of procedural justice required under Article 6[32] (see paragraphs 5.1-7 below).

4.9 In Canada, an extensive jurisprudence has grown up on different procedural methods for seeking to challenge wiretapping evidence, including having the warrant declared void.[33] For example, the affidavits received by the authorising judge in support of the wiretap application are placed in a sealed packet, which can be opened in limited circumstances and be released to the defence.[34] These affidavits will normally contain sensitive details about informants, especially in drugs or conspiracy cases. It has therefore been held that their disclosure may be subject to judicial editing to remove information.[35] This editing may be challenged if it is more extensive than the public interest requires and impedes the defendant in making 'full answer and defence'.[36] The prosecution may also raise objections over the editing.

4.10 In undertaking this procedure, the courts have specifically adopted a low threshold test for disclosure to the defence: it is enough that the defendant asserts that his or her ability to make full answer and defence requires disclosure. It has been recognised that to impose any higher duty on the defendant—for instance, to establish a *prima facie* case that his defence could be assisted—would present a virtually insurmountable hurdle.[37]

---

[31] This will also be relevant to evidence falling within Part III of the Police Act 1997.

[32] Under Surveillance, pp. 25-26

[33] *Wilson v R* [1983] 2 SCR 594

[34] As provided for under the Criminal Code, Section 187(1)

[35] *R v Parmar* (1987) 34 CCC (3d) 260 (Ont. H.C.J.), aff'd (1990), 53 C.C.C. (3d) 489 (Ont. C.A.); R. v. Garofoli, [1990] 2 S.C.R. 1421.

[36] R. v. Durette, [1994] 1 S.C.R. 469, L'Heureux-Dubé, Gonthier and McLachlin JJ. dissenting.

[37] Dersch v. Canada (A.G.), [1990] 2 S.C.R. 1505 at 1517.

Admissibility of unlawfully obtained material

4.11 In our 1998 report, we argued that the move towards proactive investigatory methods which are difficult to monitor in traditional ways necessarily imposes on the courts a greater responsibility to set standards of propriety. For example, we recommend that PACE should be amended to state specifically that the courts may exclude evidence that has been obtained in breach of a fundamental right guaranteed by the Human Rights Act 1998 if its admission would prejudice the integrity of the criminal justice system.[38] This would be particularly relevant to interception evidence obtained in circumstances which fails to comply with the statutory requirements of IOCA and any relevant codes of practice.

[38] *Under Surveillance*, Recommendation 14 at page 76

OVERSIGHT AND REDRESS

The Interception of Communications Tribunal

5.1 JUSTICE's report sets out those areas of the Tribunal's procedures that are less than satisfactory in providing an effective remedy.

- It has no jurisdiction over interceptions that are not authorised by a warrant. This means that even if the Tribunal comes across an unauthorised interception as part of its investigation into a complaint, it has no power to disclose this fact to the applicant and no duty to refer the matter to the police. The Tribunal also has no power to investigate the misuse of data obtained under a lawful warrant.
- In ruling upon a complaint, the Tribunal may only apply judicial review principles. It cannot consider, for example, either the accuracy or the merits of the evidence put forward in justifying the obtaining of a warrant.
- The applicant has no right to an oral hearing.
- There is only limited disclosure of evidence.
- The Tribunal does not give reasoned decisions. If no violation is found, for example, applicants are merely informed that no breach of IOCA has taken place.
- The Tribunal's decision can be neither appealed nor judicially reviewed in the courts.

5.2 Although the consultation paper mentions the European Commission cases of *Esbester v UK*, *Hewitt and Harman v UK* and *Campbell Christie v UK* as approving the role of the Tribunal, it does not discuss the implications of the more recent European Court decisions in *Chahal v UK* and *Tinnelly v UK*, particularly when national security issues are raised. The Court has made it clear that applying judicial review principles is an inadequate remedy insofar as it denies a Tribunal the ability to assess the factual basis of a decision. It takes the view that it should be possible to employ procedures which both accommodate legitimate security concerns and also accord individuals a substantial measure of procedural justice.

5.3 We believe that these decisions are directly relevant to the adequacy of the Interception Tribunal's procedures and its compliance with Articles 6 and 13. We therefore recommend that the procedures adopted in the Special Immigration Appeals Commission Act 1997 to implement the ECtHR's decision in *Chahal* should

be considered as a suitable model for the Interception of Communications Tribunal (and other similar tribunals) when security sensitive matters are at issue. This includes provision for the appointment of a special advocate and rules requiring that the applicant be given a summary of the submissions and evidence. A reasoned decision should be given to the extent that this is possible without disclosing information contrary to the public interest.

Notification

5.4 We think it is regrettable that the consultation paper makes no mention of notification procedures. We believe that a comprehensive review of interception of communications should include a debate about notification, its role and effectiveness. Many other countries have adopted some form of notification on the grounds that any complaints procedure will inevitably offer only limited possibilities of an effective remedy if, in the main, people are unaware that they have been the subject of an interception. It is also recognised that notification introduces an important element of accountability.

5.5 Under the Wiretap Act in the United States the judge granting the warrant has the discretion to notify the named individuals within 90 days of its expiry so long as police investigations will not be prejudiced. This may be delayed where it is established that such notice would be contrary to the interests of justice. The notification includes information on the period of the interception and portions of the material recorded, as the judge determines. Judges in Canada have a similar discretion although there is no requirement to include the contents or details of the authorisation. The Solicitor General's Annual Report on the Use of Electronic Surveillance in Canada shows that 407 people were notified during the period of 1996-7. Many European countries including Denmark,[39] Germany[40] and the Netherlands[41] also have some form of notification. The requirement is also included in the Council of Europe's Recommendation on the use of police data.

5.6 The European Court of Human Rights has looked at the issue of notification in the case of *Klass v Germany*, where the applicants alleged that German law did not give them an effective remedy for unlawful telecommunications interceptions. While it did not find a violation, the Court placed considerable emphasis on the fact that German

[39] Paragraph 788, Code of Criminal Procedure

[40] Section 5(5) Restriction of Privacy of Mail, Posts and Telecommunications Act 1989

law required notification of the individuals concerned as soon as this was possible without prejudicing police activities.

5.7 JUSTICE acknowledges that this is an issue raising difficult policy and practical considerations. As we say in our report, it warrants further research into the practice in other countries and the different forms that notification may take. JUSTICE believes that at the very least notification is required where there has been a breach of the statutory requirements covering interceptions, subject only to delay on grounds of prejudicing police operations. This means that it should be a duty on the authorising official (currently the Secretary of State) and the independent supervisor (the Commissioner) to notify, for example, where a warrant has been improperly or erroneously issued or complied with. Such occurrences are referred to in the Interception Commissioner's report.

Transparency and the reporting requirement

5.8 Under IOCA, the Interception of Communications Commissioner reports annually to the Prime Minister on the operation of the Act. This report is published and laid before Parliament after sensitive and confidential material is removed: in practice, this is information relating to the security and intelligence services and GCHQ.

5.9 In our 1998 report, we criticised this process on several grounds.[42] Our main criticism was the comprehensiveness of the information: only the numbers for the Home Office and Scottish Office are made public. Moreover, even the figures published are an inadequate guide to the number of people affected by an interception: one warrant can cover an entire organisation. Canadian figures show that one average, thirty *identifiable* people were affected per warrant. Another criticism concerns information on the cost and effectiveness of interceptions. In countries such as Australia, New Zealand and the United States, the law requires publication of information on the number of applications refused, the average duration of warrants and their extension, the categories of serious crime involved, and statistics on the effectiveness of operations in terms of arrests, convictions and the cost of operations. We would particularly refer to the United States annual federal 'Wiretap Report' which contains

[41] Article 126bb of the Special investigative Powers Bill, appended to the Under Surveillance report. The Bill was passed in May 1999

[42] At pp. 22-23

information on all these issues together with a 236 page Annex containing a break-down per warrant.[43]

5.10 JUSTICE considers that the transparency of the interception process could be greatly enhanced by publishing more detailed annual reports, including information on the number of people affected, duration of warrants and their extensions, costs and effectiveness in terms of arrests, prosecutions and convictions.

[43] Available at http://www.uscourts.gov/wiretap98/contents.html

Provision of communications data

6.1 The European Court of Human Rights in *Malone v the United Kingdom* made clear that even the limited nature of communications data available at that time—essentially a print-out of a list of numbers called—was covered by Article 8:

> 'The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8).'

6.2 Since then, metering technology has undergone rapid change, rendering it both more valuable and more intrusive. Within Europe, a set of 'International User Requirements' has been agreed requiring communication providers to provide on request to law enforcement and security services the following minimum information[44]:

- signalling of access ready status;
- called party number for outgoing connections even if there is no successful connection established;
- calling party number for incoming connections even if there is no successful connection established;
- all signals emitted by the target, including post-connection dialled signals emitted to activate features such as conference calling and call transfer;
- beginning, end and duration of the connection;
- actual destination and intermediate directory numbers if call has been diverted;
- for mobile phones, the most accurate geographical location known;
- data to law enforcement agencies on the specific services used by the interception subject and the technical parameters for those types of communication.

6.3 A draft EU agreement adapting these requirements to satellite and internet communications indicates that information on users' credit card details, cryptography keys, information about subscribers in other countries operating within the agency's

[44] As annexed to Council Resolution of 17 January 1995 on the lawful interception of telecommunications, OJ C 329, 04 November 1996, p. 1

jurisdiction, and voice-mail information may also need to be passed on whenever this is necessary for law enforcement purposes.[45]

6.4 It is a requirement that this information be made available as the call is being made, in 'real time'. Modern software analysis tools may be used to interpret the information to establish links between different persons, and patterns of behaviour. For instance, a software product called 'Watson', made by Harlequin software, has been used extensively by UK police to investigate internet pornography rings.[46] This involved analysing websites visited, the location from which potentially pornographic material had been downloaded, and e-mail contacts. In such cases, it may not be necessary for the police to intercept the contents of messages: investigators can tell as much or more from analysing communications patterns as from the message content. The development of unbreakable cryptography which poses real problems for content interceptions is likely to accelerate the development of these analysis tools and place even greater reliance on the release of communication data.[47]

6.5 In the case of mobile phones the availability of real time information on a person's geographical location transforms metering into an active surveillance tool.

6.6 In the 1998 report, we criticised the lack of any proper controls over the provision of such information in Section 45 of the Telecommunications Act 1985 and the Data Protection Act 1984. We therefore welcome the Government's proposal to bring it within the statutory framework on interceptions. It is arguable whether the practice as it is developing is necessarily always less intrusive than a contents interception (see Paragraph 10.3 of the consultation paper), and it can undoubtedly amount to a significant interference with privacy in individual cases. This needs to be reflected in the regulations both in terms of the appropriate person to give authorisation and the grounds that need to be satisfied.

6.7 The Consultation Paper, however, does not provide sufficient detail of the proposal to facilitate proper consultation. For example, there is no discussion of who should take the role of 'authorising official', a key element in the safeguarding process. Presumably, in most cases where a full interception warrant is sought, this will also include a request for disclosure of communications data and be put before the relevant Secretary of State. The question is therefore whether applications to provide

[45] Draft Council Resolution on new technologies, ENFOPOL 98 REV 2, Doc. no. 10951/2/98

[46] According to Harlequin, its products have been used by Durham and Warwickshire police: http://www.harlequin.com/products/hints/watson/

communications data alone should also be authorised at the same level, by the Secretary of State.

6.8 At Paragraphs 3.2-5 we have set out JUSTICE's general position on authorisations. In relation to more intrusive surveillance operations, we are in favour of independent authorisation from a member of the judiciary. This is the situation in countries such as America and Canada for both telephone interceptions and the disclosure of communications data. As we say at para. Xxx, there is also a practical consideration as to the volume of applications. Moreover, the recent decision in *Morgans v DPP*[48] on the difficult technical line to be drawn between what amounts to metering and interception is an additional reason for ensuring that authorisation for both should be given by the same person.

6.9 The consultation paper proposes wider grounds for the provision of such information that those that apply under IOCA warrants: serious crime, national security and the UK's economic well-being. However, it provides no evidence or justification as to why those wider grounds are necessary. For example, what is the justification for extending them to any crime, however minor? Similarly, why is it necessary to include 'the assessment or collection of any tax or duty'? Although the latter is included in the disclosure exemption for data protection legislation, this could not of itself justify a blanket extension to require information to be provided. Without further details of the proposed extent of the practice, what crimes it is proposed to cover, and its anticipated effectiveness, it is impossible to assess whether the proposed grounds satisfy the proportionality principle required by Article 8.

---

[47] This is emphasised in the European Commission's Communication 'Towards A European Framework for Digital Signatures And Encryption' COM(97) 503

[48] *Morgans v Director of Public Prosecutors* [1999] 2 CrAppR 99 (QBD)