



**JUSTICE**

**REGULATION OF INVESTIGATORY POWERS BILL**

**HUMAN RIGHTS AUDIT**

**May 2000**

# REGULATION OF INVESTIGATORY POWERS BILL

## HUMAN RIGHTS AUDIT

### INTRODUCTION

- 1.1. The purpose of the Regulation of Investigatory Powers Bill is to ensure that certain surveillance methods used during investigations by the police and other law enforcement agencies are compatible with the Human Rights Act 1998. The fundamental rights likely to be affected by covert policing are the right to respect for privacy under Art.8 and the right to a fair trial under Art. 6 of the European Convention on Human Rights. The text of these Articles are set out in Annex 1.
- 1.2. In its report, *Under Surveillance*, JUSTICE came to the overall conclusion that the present legislative and procedural framework governing the use of these proactive policing methods is out of date, inconsistent and unable to provide the safeguards required to comply with the Human Rights Act. We strongly urged the Government to take an integrated approach when looking at future regulation of surveillance methods in order to bring some consistency and cohesion to this complex area of regulation. Given the similarities between all forms of eavesdropping, such an approach would avoid confusion and uncertainty both for the policing agencies and suspects.
- 1.3. While JUSTICE welcomes the introduction of this Bill, we believe it represents a missed opportunity to rationalise a patch-work of legal measures. Despite its intentions to balance law enforcement needs with individual privacy rights, it succeeds largely in making an already complex legal environment even more so. **It will result in some nine or so separate but overlapping statutory regimes covering surveillance conduct by the police, intelligence services and other agencies (see Annex 2).** An investigation may well require authorisation under more than one regime.

### THE BILL'S COMPLIANCE

- 2.1. The Bill's five parts cover interception of communications, access to communications data, the decryption of encrypted material and covert surveillance operations, including the use of informers and undercover officers. It replaces the Interception of Communications Act 1985 with a new regime and amends other legislation including Part III of the Police Act 1997, the Security Service Act 1989 and the Intelligence Services Act 1994. **As we set out below, we believe that some of its provisions do not sufficiently comply with ECHR rights.**
- 2.2. One of the problems is that this is framework legislation with much of the detail to be provided for in secondary legislation, either in orders, regulations or codes of practice. It is therefore not possible to assess fully the human rights compliance of some of the activities, particularly where a wide discretion is given to ministers in the making of that legislation. **It contains**

**some twenty-two provisions for secondary legislation, most of which are subject only to negative resolution, and where the scope, intent and safeguards of the delegated powers are insufficiently set out in the statute.** In some cases, this may mean that the provisions fall foul of the ECHR requirement that any interference with rights is clearly ‘prescribed by law’. In other cases, the breadth of the delegated powers is such that significant breaches of human rights in the orders, regulations or codes cannot be ruled out.<sup>1</sup> There is no obligation to provide a certificate of compliance with the ECHR for delegated legislation as there is for primary. In this briefing, we refer to those delegated powers that raise important human rights concerns.

- 2.3. In preparing this audit report, we are grateful for the assistance of the following barristers: Clare Montgomery QC, Helen Mountfield, Keir Starmer, Michael Ford and Tom de la Mare.

## **PART 1 : INTERCEPTION OF COMMUNICATIONS**

### *Executive authorisation*

- 3.1 Under cl.7 authorisations for interception of telecommunications are to continue to be the responsibility of the Secretary of State. The Home Office in its consultation paper stated that it is ‘not persuaded’ of the need to depart from this regime, although it does not give reasons for this other than that it considers that the executive would still need to issue warrants applied for on national security grounds.
- 3.2 The question of who authorises intrusive surveillance operations is an important one. And it is a debate that has taken place several times before, most recently in relation to the use of bugging devices under Part III of the Police Act 1997. Putting it shortly, it is argued that a member of the executive lacks the necessary independence to authorise interception by a state agency and that it offends against the concept of the separation of powers; a senior judge would be a more appropriate arbiter of the balance between the rights of the individual and the interests of the state.
- 3.3 **While the European Court of Human Rights (EctHR) has not specifically required that such oversight by judicial, it has on several occasions stressed the importance of it being so.** In *Klass v Germany*, it stated that ‘*it is in principle desirable to entrust supervisory control to a judge*’. Likewise, in discussing the safeguards offered by French law on telecommunications interceptions, it placed considerable emphasis on the safeguard of prior judicial authorisation.<sup>2</sup>
- 3.4 **JUSTICE’s position is that the most intrusive surveillance operations, including interceptions, should all be subject to the same warrant procedures with authorisations by a High Court judge** (whether acting as a Commissioner as under Part III Police Act or otherwise). This is the practice

---

<sup>1</sup> A copy of a separate briefing prepared for the Delegated Powers Committee may be obtained from JUSTICE.

<sup>2</sup> *Huvig v France* (1990) at para.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...’

in a great number of countries, including Canada, New Zealand, the United States and other EU member states. It would also have the advantage of bringing the law on interceptions in line with similarly intrusive surveillance operations under the Police Act and Part II of this Bill.

- 3.5 As to the issue of warrants based on national security grounds, we question why the judiciary is not considered to be sufficiently competent to undertake the authorisation as they do in many other countries, such as Australia and Canada. **And even if it is shown to be necessary that such warrants remain with the Secretary of State, it would be possible to run parallel regimes with only those applications made by the security services remaining with the Secretary of State. This is what is proposed for 'intrusive surveillance' applications under Part II of this Bill (see cl.39).**<sup>3</sup>

#### *Participant monitoring*

- 3.6 Under section 1(2)(b) of IOCA 1985, there was an exemption where one party to the communications consented to it being intercepted. This is commonly known as the 'participant monitoring' exemption. It has the effect of circumventing the warrant procedures and safeguards of IOCA and is particularly relevant in cases where police or informers are used to extract evidence from suspects.
- 3.7 Although the exemption is not repeated in Part I of the Bill, it is to be found in Part II. The combination of clauses 25(4) and 45(4) have the effect of exempting interceptions of telecommunications done on the basis of the consent of one of the parties to the communication from being considered as 'intrusive surveillance' under Part II. Although unclear, it seems that the intention is to place such conduct under the lesser controls of 'directed surveillance under Part II (requiring only self-authorisation within the agency undertaking the conduct).
- 3.8 **JUSTICE would strongly argue that this is insufficient: the non-consenting person whose privacy is infringed is entitled to the same level of safeguards as any other person whose private telecommunications is being intercepted by a state agency.** And, in any event, we question that it should properly fall within the category of 'directed' rather than 'intrusive' surveillance' (see below).
- 3.9 We believe that any such different treatment for the non-consenting person potentially breaches Art.8 of ECHR. In the case of Lambert v France (1999), the EctHR considered a judgment of the French Court of Cassation which had denied legal remedy to a person whose telephone calls had been intercepted on a friend's line. It held that, as a matter of principle, Art. 8 protects people, not telephone lines:

'The 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.'

---

<sup>3</sup> And the distinction already exists in relation to surveillance operations involving trespass etc.: Part III of the Police Act 1997 applies to the police requiring judicial approval, whereas similar conduct by the security services requires Secretary of State authorisation under the Intelligence Services Act 1994.

- 3.10 This reasoning is in accordance with the decision of the Canadian Supreme Court in the case of *R v Duarte* (1990). This was a case of an informer who had been wired-up to record conversations between himself and the suspect. While the Canadian Criminal Code required a warrant for the use of electronic surveillance devices generally, none was needed for such consent operations. The Court held that this 'participant monitoring' exemption directly contradicted the principle that it is the person whose privacy is being infringed who should be afforded safeguards. The Canadian Criminal Code now requires judicial authorisation for the interception of a private communication even where one party consents to it. The Irish Law Commission has recently come to the same conclusion in a report on interception of communications.<sup>4</sup>

#### *Office and business monitoring*

- 3.11 The Bill allows persons with the right to control a private communications network to intercept without committing an offence, although they may be liable for a new civil tort if it is done without lawful authority (cl.1(6)). Lawful authority includes having 'reasonable grounds for believing' that both parties to the communication consent to the interception (cl.3(1)). This is intended to comply with the ECtHR's judgment in *Halford v UK* and appears to cover both private domestic networks and those found in offices and other establishments such as universities and private telephone exchanges as in hotels.
- 3.12 **JUSTICE considers that cl.1(6) is too wide an exemption in so far as it applies to offices and other work places, especially those that are public authorities and therefore bound by Art 8 ECHR.** An exemption based solely on consent of employees provides insufficient safeguards, particularly as most employees may not be in a position to assert their right to privacy because of the consequences this may have on their employment. At the same time, the potential liability to a civil tort under cl.1(3) is a less effective, *post facto*, remedy for individuals who will have serious difficulties in either knowing or proving that an unlawful interception has taken place.
- 3.13 **JUSTICE believes that interception in the work environment should be separately dealt with and be linked with the provisions on lawful business monitoring under cl. 4(2).** As currently drafted, there is no relationship on the face of the Bill between this exemption under cl.1(6) and the provisions on interceptions for business monitoring under cl.4(2). Under the latter, interceptions have to be for a legitimate business purpose and be made in the course of transmission on apparatus provided by the employer (i.e. a handset).
- 3.14 Although the Secretary of State's regulation making powers under cl.4(2) are wide, the danger (as has persistently been the problem with UK privacy regulation) is under-regulation. JUSTICE believes that there are certain principles that must be complied with in order that the practice of business monitoring is legitimate: for example, openness and transparency, protection for legal and other privileged material and protection for private confidences. It is therefore essential that a draft version of the first set of regulations under cl.4(2) should be published during the parliamentary proceedings of the Bill.

---

<sup>4</sup> *Privacy : Surveillance and Interception of Communications* (1998).

### *Intercept material as evidence*

- 3.15 In general terms, the current position of prohibiting the use of intercept material as evidence is to remain. However, there are two significant differences: first, under cl.14(4)(d) the material is not to be destroyed when the prosecution needs to hold it as part of its duty to 'secure the fairness of the prosecution'; second, under cl.17(5) disclosure of the material may be made by the prosecution to the trial judge who may direct the making of an admission of fact. There is no provision for the disclosure of this material to the defence (other than for specific intercept offences).
- 3.16 **JUSTICE would argue that this arrangement breaches the 'equality of arms' principle in Art.6 of the ECHR which guarantees a defendant a fair trial.** This is on several grounds. First, it permits the prosecution to have access to potentially relevant evidence, but not the defence. Even though the material may not be used by the prosecution as admissible evidence, it nevertheless may assist the prosecution as to how it conducts its case, including the asking of questions based on knowledge of the material. Second, it is a blanket provision whereby there are no circumstances when the *merits* of disclosing to the defence may be considered. This means that disclosure to the defence cannot be ordered even where the circumstances are 'exceptional' and the making of an admission by the prosecution is 'essential (i.e. when the material goes to the heart of the prosecution case). There are also no grounds for disclosure even when to do so would clearly not damage the public interest.
- 3.17 Third, the disclosure to the 'relevant judge' under cl.17(b) has implications for both procedural and substantive fairness. For example, the clause is silent about the circumstances in which a judge might make an order for disclosure to him or herself alone. Although cl.16 sets up a complete prohibition on making disclosures in legal proceedings, the prosecution will have to communicate in some way to the judge that it has this material and that it might be relevant to the proceedings. One question is how is this to be done?
- 3.18 For example, the communication might be made in an *ex parte* public interest immunity (p.i.i.) hearing. The question would then be whether there are sufficient procedural safeguards for the defence as required by the recent ECHR decisions in Rowe and Davis v UK, Jasper v UK and Fitt v UK. **We would argue that the procedure for disclosing intercept material to the judge and the judge being able to order an admission fall short of the p.i.i. procedures scrutinised and endorsed in these cases.** In particular:
- there is no provision for disclosure to the defence in any circumstances (see above)
  - the threshold for making admissions is not 'fairness' but both 'exceptional circumstances' and 'essential' admissions (i.e. some higher and unspecified criteria)
  - there is no opportunity for the defence to make representations as to what are 'exceptional circumstances' and what admissions might be 'essential'.
- 3.19 In addition, even where the 'exceptional circumstances' make the disclosure 'essential' in the interests of justice and the judge considers admissions should be made, cl.17(8) places severe restrictions on the kind of admissions

that can be made. It says that nothing may be admitted that breaches any of the prohibitions in cl.16(1) – that is, an admission cannot in any way tend to suggest that an interception has taken place. **Therefore even an admission which is considered ‘essential’ may not be made if by doing so it breaches cl.16(1). It is difficult to see how a fair trial could follow in such circumstances.**

- 3.20 **JUSTICE believes that lawfully intercepted material should be *prima facie* admissible as evidence in criminal proceedings, subject to the usual disclosure of evidence rules under the Criminal Procedure and Investigation Act 1996 and judicial discretion under s.78 of PACE.** This is the position for other material obtained by intrusive surveillance methods under Part III of the Police Act and Part II of this Bill. If the objections can be overcome for one form of surveillance, it is hard to understand the continued justification for interception material to be treated differently.
- 3.21 Copies of correspondence in relation to clauses 16 and 17 are also attached.

## **ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA**

- 4.1 Under cl.20(4) communications data is defined as all that information relating to the use of a communication service other than the contents of the communication itself. It includes subscriber’s details, the names, addresses and numbers of those contacted, web sites visited and, in the case of mobile phones, the user’s geographical location. Such data is increasingly valuable to criminal investigations and its disclosure more intrusive to individuals; the underlying assumption that access to such data is less intrusive is no longer necessarily true.
- 4.2. Following the ECtHR decision in *Malone v UK* (1984) that such data fell within Art.8, the UK government inserted a new section 45 into the Telecommunications Act 1984. This has allowed disclosure on the broad grounds of prevention and detection of crime without any of the Art.8 safeguards. Including it within the statutory controls of this Bill is therefore to be welcomed.
- 4.2 However, there are the ‘catch all’ clauses allowing the Secretary of State to add to both the purposes and the public authorities that may obtain such data. At the moment, the latter includes a police force, NCIS, NCS, Customs and Excise and the intelligence services. **In light of the recent disclosure that the Home Office has a list of some 32 other agencies who will be added under a similar ‘catch all’ clause for ‘directed surveillance’ under Part II (see below), the Home Office should specifically be asked to give details of other public authorities that are, or are likely to be, given this power in the future.**
- 4.3 There is an additional issue whether self-authorisation within an agency is sufficiently independent to comply with Art. 8 requirements. The ECtHR has frequently criticised the practice of self-authorisation. In the recent case of *Kopp v Switzerland* (1998) it said: *‘Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office’s legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area...’*

- 4.4 As the nature of the communications data becomes more sensitive, the need for independent prior authorisation becomes stronger. This is particularly so when there is no challenge mechanism for those holding the data. **There are therefore strong arguments in support of communications data (or, at least, the most sensitive communications data) being safeguarded in the same way as access to special material under section 9 and Schedule I of PACE.**
- 4.5 The grounds on which a person's privacy may be lawfully interfered with under Art. 8 are closely proscribed in Art 8(2) (see Annex 1). It is therefore unclear why the Bill includes the collection of tax etc. as a legitimate ground for the disclosure of communications data (see cl.21(1)(f)). Either the collection of tax is legitimate as falling within one of the other grounds or it is not an aim that may be pursued under Art.8. And, in any event, it is far from clear why communications data is considered to be relevant to the collection and assessment of taxes. It is also curious that the Bill permits the Secretary of State the right by order to add to the list of permitted grounds in cl.21(2)(h): as the permitted grounds of Art.8(2) are already reflected in the clause, any additional grounds are likely to go beyond the scope of Art.8(2). **JUSTICE therefore believes that cl. 21(2)(f) and (h) should be deleted from the Bill on grounds that they may breach Art. 8 ECHR.**
- 4.6 There is nothing in this part of the Bill covering the safeguarding of the communications data disclosed. Although such data is likely to fall within the Data Protection Act 1998, there nevertheless should be uniform provisions on such matters as the destruction of the material within the Bill, as there is for interception material under cl.14.
- 4.7 Under cl.53(2)(b) the Interception of Communications Commissioner is required to review the working of these provisions covering communications data. However, it is not clear how this is to be achieved in the absence of a specific requirement for the 'designated person' to notify the Commissioner of each authorisation<sup>5</sup>. **As this is a key safeguard relied upon by the Home Office for arguing against the need for judicial authorisation in this area, it is essential that the *post facto* oversight by the Commissioner is made fully effective.**

*Privileged material*

- 4.8 There are no provisions for special procedures in relation to legally or otherwise privileged material. The ECtHR in Campbell v UK (1992) stated that a high level of protection is to be accorded to these sensitive categories of material and in the more recent case of Kopp v Switzerland (1999) it held that the law must make it clear how legal professional privilege is protected in practice. **Although, it may be intended to address this issue in a code of practice, we consider that the provisions should be included on the face of the Bill in relation to both Parts I and II.**

---

<sup>5</sup> Cl.54(1) only provides a duty to disclose documents and information as requested by the Commissioner.

## **PART II: SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES**

- 5.1 Part II provides the framework for authorising three forms of covert surveillance:
- ‘directed surveillance’
  - ‘intrusive surveillance’
  - the use and conduct of ‘covert human intelligence sources’ (informers, agents and undercover officers)
- 5.2 ‘Directed surveillance’ and the use of ‘covert human intelligence sources’ require the lesser control of self-authorisation from a designated person within the agency undertaking the action;<sup>6</sup> whereas, ‘intrusive surveillance’ requires approval from a High Court judge acting as a Commissioner before it can take effect.
- 5.3 On a general point, the Explanatory Memorandum makes it clear that Part II (in common with other parts of the Bill) do not impose a requirement on public authorities to seek or obtain an authorisation for surveillance. Unlike Part I where there is a criminal offence and a (limited) civil tort of unlawful interception, Part II creates no such penalties, other than the action may be unlawful under section 6 of the Human Rights Act 1998. **JUSTICE believes that this is an insufficient safeguard in an area of activity where the risk of abuse is high but the likelihood of it being uncovered is very low. The Bill should impose a duty to obtain an authorisation for surveillance under Part II, with appropriate criminal and civil penalties for failing to do so.**

### *Directed surveillance*

- 5.4 ‘Directed surveillance’ is defined as covert surveillance of individuals during a specific but *not intrusive* investigation (our emphasis). It is covert when it is carried out in such a way to ensure that those targeted are unaware that it is taking place (cl.25(8)). ‘Surveillance’ is defined as including any monitoring, observing and listening to persons, their movements, conversations or other activities or communications. It also includes any recording of such activity and surveillance by or with assistance of a device (cl.45(2)).
- 5.5 **This definition of ‘directed surveillance’ needs to be clarified.** We understand from a meeting with Home Office lawyers that the description of ‘directed surveillance’ as ‘not intrusive’ is not to be taken literally. It is in fact to cover intrusive activities (otherwise it would not be necessary to include it in the Bill) but it is conduct deemed to be ‘not intrusive’ in so far as it does not fall within the Bill’s definition of intrusive conduct in cl.25(3) (i.e. it does not take place in relation to residential property or a private vehicle). **JUSTICE believes that this kind of Alice In Wonderland ‘back to front’ analysis is in breach of Art 8 which requires that such laws on surveillance are clearly accessible.**

---

<sup>6</sup> The agencies are the police, NCIS, NCS, any of the intelligence services, the Ministry of Defence, any of the armed forces, Customs and Excise. These may be added to by order of the Secretary of State.

### *Directed surveillance v intrusive surveillance*

- 5.6 Although we accept that it is necessary to draw a distinction between less and more intrusive surveillance activities, the line presently drawn between 'directed' and 'intrusive' surveillance is somewhat artificial and creates a number of serious anomalies. As there are different safeguards and controls between the two forms of surveillance, the distinction is important both for compliance with Art 8 ECHR privacy rights and the protection of individuals. Below, we set out examples where the Bill provides that a particular form of conduct is to fall within the lesser controls of 'directed surveillance', when it should more properly fall within the 'intrusive surveillance' controls. **JUSTICE believes that the provisions in the Bill which inappropriately relegate certain conduct to the lesser controls of 'directed surveillance', when they should more properly fall within the controls of 'intrusive surveillance', need to be seriously questioned for compliance with Art.8 ECHR.**
- 5.7 For example, under cl.25(5) a surveillance device used from outside residential premises or a private vehicle that does not consistently provide the same quality and detail 'as might be expected' from a device actually present on the premises is not to be considered as 'intrusive surveillance'. Thus using a remote listening device located away from a house or a long lens photographic equipment will fall within either 'directed' or 'intrusive surveillance', depending on its recording qualities.
- 5.8 JUSTICE believes that if the intention is to observe, listen to or capture images of a person in residential premises (or anywhere where there is an expectation of privacy) through the use of a technical device, it must be assumed that the action is likely to be intrusive, irrespective of the quality of material actually obtained. As the Data Protection Commissioner has said, the fact that a picture from a long lens camera might not be quite as clear as from a camera placed in the room does not necessarily make the infringement of privacy any less.<sup>7</sup> And, from a practical standpoint, how is the quality of the information to be anticipated in advance, so as to know which procedures to follow? Following the wrong procedures risks the conduct being unlawful and the material inadmissible as evidence. **The exemption in clause 25(5) should be deleted from the Bill.**
- 5.9 Another example is the way in which the Bill deals with interceptions of a communication where one party to the communication consents to the intercept. As explained above, this practice of 'participant monitoring' is exempt from Part I controls. Although not expressly stated in the Bill, the Explanatory Memorandum says that it is to come within the lesser controls of 'directed surveillance' (see para.178).

### *Intrusive surveillance*

- 5.10 'Intrusive surveillance' is defined as covert surveillance in relation to anything taking place on residential premises or a private vehicle. It may be carried out either by a person or device inside residential premises or a private vehicle or by a device placed outside. This is intended to cover the gaps in Part III of the

---

<sup>7</sup> Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill, March 2000.

Police Act 1997 which only applies to devices whose installation involves trespass to property, criminal damage or interference with wireless telegraphy. It means that stand-off devices such as long-distance microphones and laser-beam equipment fall outside the controls of Part III.

- 5.11 **On a general point, JUSTICE believes it would be preferable to repeal Part III of the Police Act 1997 Act and provide for a single, comprehensive regime for all forms of intrusive surveillance within this Bill.** Instead, a complex regime has been created which allows a single authorisation to cover both an application under this Bill and under Part III of the Police Act, although the different provisions of each are still to apply (see cl.31(5)).<sup>8</sup>
- 5.12 **In addition, the definition of ‘intrusive surveillance’ is too narrowly defined.** It fails to acknowledge that the ECtHR has made it clear that Art 8 privacy rights can be engaged outside residential premises and private vehicles. For example, it is well-established in ECHR cases that an intrusion into a person’s privacy extends beyond the intimacy of the home. For example, in *Niemietz v Germany* the Court held that a person is entitled to a degree of privacy in professional and business relationships at the workplace. In doing so, it made it clear that *‘respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.’* In the same way, the US Supreme Court held as long ago as 1967 that privacy rights ‘protect people, not places’.
- 5.13 **The Data Protection Commissioner has recommended that the definition of ‘intrusive surveillance’ should be widened to include any premises or location where the individual has a legitimate expectation of privacy.** The Irish Law Reform Commission made a similar recommendation in a recent report on privacy and surveillance. This is also reflected in the laws of other countries: for example, the Canadian Criminal Code requires judicial authorisation of video surveillance when the person targeted might reasonably have an expectation of privacy. Examples of such places – a doctor’s surgery, an MP’s private office, a restaurant and a public place – would need to be fully illustrated in a code of practice.

#### *Authorisation for ‘directed surveillance’*

- 5.14 Again the Secretary of State has wide ‘catch-all’ clauses to add to the purposes and agencies that may undertake ‘directed surveillance’ (and the use of covert intelligence sources). **It was announced at Committee stage in the Commons that it is intended to include some 32 other agencies under the order-making power of cl.29(4)(h) as being public authorities who may carry out ‘directed surveillance’.**<sup>9</sup> These include the Immigration Service, the Benefits Agency, Inland Revenue, the Food Standards Agency, the Post Office, the Vehicle Inspectorate, MAFF, the Pesticides Safety Directorate and all local authorities.
- 5.15 JUSTICE has three main concerns with this:

---

<sup>8</sup> Note the authorisation procedure differs according to the agency making the application: the police and customs apply to a Commissioner in the same way as under Part III of the Police Act; the intelligence services, Ministry of Defence and Armed Forces apply to the Secretary of State

<sup>9</sup> Under cl.29(4) it is the police, NCIS, NCS, the intelligence services, the MOD, the Armed Forces and Customs and Excise who may do so.

- first, it is insufficient to include these agencies merely on the basis that they have ‘indicated their wish to continue their use of these techniques’.<sup>10</sup> Especially as it is acknowledged that the Home Office was unaware of the current use of covert surveillance by many of these agencies, **it is essential that a proper inquiry is carried out to ensure that the use of such techniques by each agency ‘is necessary and proportionate’ and therefore justifies the inclusion.** In several cases, the ECtHR has said that the use of surveillance should be limited to ‘serious and defined offences’, it should not be exploratory or general and be limited to those cases where conventional means of inquiry are ineffective or have been unsuccessful.<sup>11</sup>
- second, the addition of such agencies should not be done by way of delegated legislation; **they should be included on the face of the Bill in a Schedule.** This goes to the quality and accessibility of the law, as required by Art 8 ECHR.
- third, how the Covert Investigations Commissioner is to monitor such surveillance activities, particularly in the absence of any requirement on the agencies to report their activities to the Commissioner (see also below at para.6.3).

#### *Authorisation for intrusive surveillance*

5.16 In relation to the authorisation procedures involving the Surveillance Commissioner, JUSTICE has the following comments:

- In an age of new technology, we question whether it is necessary to treat urgent applications differently (cl.33(3)(b)) thereby allowing the conduct to go ahead without prior approval of the Commissioner. As this is also provided for in Part III of the Police Act, the Home Office should be asked to provide details of how often it has been relied upon since that Act came into force. The experience in other countries such as Australia is that authorising judges are able to respond quickly and there is no evidence to suggest that a requirement for prior approval in all cases has an adverse effect on police operations.
- **The Commissioner should have the power to attach specific conditions to a warrant.** These may be restrictions or limitations on who, how, when, where or what kind of surveillance may be undertaken. This is common practice in other countries. The annual figures published under the Canadian Criminal Code show that conditions are attached in the majority of authorisations for electronic surveillance: in 1998 the figure was 98%.
- **Strict rules covering legal or otherwise privileged material should be included on the face of the legislation and not left to a code of practice.** This is the approach taken under sections 98 -100 of Part III of the Police Act and should therefore be followed in this Bill. The ECtHR in Kopp v Switzerland (1999) said that the law must make it clear how professional legal privilege was to be protected in practice.

<sup>10</sup> Home Office Minister, Charles Clarke MP, Report stage, Hansard 8 May 2000 col.609.

<sup>11</sup> Klass v Germany 1980.

- The Commissioner should be *required*, for example, to quash an authorisation if s/he is satisfied at any time that there are no reasonable grounds on which it should continue. Under cl. 35 the Commissioner has a discretion whether to do so in relation to this and other matters. **The word 'may' in sub-clauses (2), (3), (4) and (5) should be replaced by 'shall'.**
- Before any renewal of an authorisation, the Commissioner should be satisfied that a review has been carried out on the surveillance already undertaken and take account of its results. This is a requirement for the renewal of a covert human intelligence source authorisation under cl.41(6) and should apply to all forms of surveillance under Part II.

*Authorisation by Secretary of State*

5.17 In relation to the authorisation procedures involving the Secretary of State, JUSTICE has the following comments:

- As the Security Service (MI5) has the power to carry out investigative policing activities under its new remit of being tasked to investigate serious crime, there are strong arguments that these powers should be exercised under the same procedures as apply to the police. Otherwise there are obvious dangers in two agencies having different powers and operating to different procedures when tackling the same threat of serious crime.
- The Secretary of State has an unfettered power to extend the 'public authorities' who may carry out 'intrusive surveillance' under cl.39(1)(d). **For the same reasons mentioned above, the Home Secretary should be asked to justify this provision and identify the authorities that may be included in the future.**
- Again, there are no strict rules covering legal and other privileged material (see above).
- A warrant for 'intrusive surveillance' granted to the intelligence services has a duration of six months (cl.42(4)) as compared to three months for police and other law enforcement authorisations (cl.41(3)(c)). **The Home Secretary should be asked to justify this difference.**

*Covert human intelligence sources*

5.18 JUSTICE particularly welcomes the provisions placing the use and conduct of informers and undercover officers under statutory control. This need for operational control over such persons has recently been endorsed by the ECtHR in the Teixeira de Castro v Portugal case in relation to a 'buy and bust' undercover drugs operation.

- 5.19 However, we also appreciate the difficulties in providing a statutory framework that has to cover a wide range of activities. At one end, an informer may be a person who merely gives information to the police; at the other extreme, he or she may be actively engaged in the commission of an offence. And in terms of undercover policing, there are fine gradations between involvement, incitement and entrapment. However, the role played by the informer or undercover officer will determine the degree of intrusion and therefore the level of safeguards required.
- 5.20 **JUSTICE believes that in order to comply with the requirements of Art 8 ECHR the Bill needs to draw a distinction between different categories of informers and undercover police work.** Currently under cl.25(7) of the Bill, a covert human intelligence source is defined in relatively benign terms: essentially it is a person (informer or police officer) who maintains a covert relationship with a suspected criminal in order to obtain and pass on information. It does not specifically recognise the conduct of participating informers who are persons 'engaged in a course of action which, without authority, could lead or could have led to his/her arrest and prosecution'<sup>12</sup> or undercover officers who actively set up a 'buy and bust' or 'sting' operation.
- 5.21 In the recent case of Kopp v Switzerland (1998), the ECtHR severely criticised the practice of internal, executive authorisation, without supervision by an independent judge, in relation to surveillance activities. It is therefore questionable whether self-authorisation within an agency would be considered a sufficient safeguard in relation to the activities of participating informers and undercover officers in serious crime cases. It could also be argued that the case of Teixeira de Castro v Portugal places additional weight on the need for independent authorisation and supervision in undercover operations if the exercise is not to breach ECHR rights. **JUSTICE believes that it may therefore be necessary to draw a distinction whereby the use of participating informers and undercover officers in serious crime cases be made subject to prior authorisation by a judge.** This should apply equally to agents run by the intelligence services.
- 5.22 In any event, as the Bill is presently drafted, it creates certain anomalies. For instance, under cl.45(3)(a) an informer who is 'wired-up' to record a conversation in a suspect's home is only to be subject to the lesser, self-authorisation procedures governing covert human intelligence sources. However, if the recording had been obtained by placing a bug on or outside the suspect's home, prior approval from a Commissioner would have been required under either Part III of the Police Act 1997 or under Part II of this Bill. **JUSTICE believes that the authorisation procedures should properly reflect the nature of the operation and its intrusiveness and, as far as possible, be consistent in relation to activities of a similarly intrusive nature.**
- 5.23 The duration of an authorisation to use a covert human intelligence source is twelve months, with a similar period for renewal (cl.41(3)(b)). **JUSTICE believes that this is too long, especially in the case of participating informers and undercover operations.**

---

<sup>12</sup> ACPO Code of Practice, 1999.

## **PART IV: SCRUTINY OF INVESTIGATORY POWERS**

### *Commissioners*

- 6.1 The existing oversight by Commissioners is to extend to these new areas of surveillance, backed by a single Tribunal to hear complaints in relation to all surveillance conduct, including that of the intelligence services.
- 6.2 JUSTICE welcomes the recently announced proposal for a general secretariat for all the Commissioners. However, we also believe that there should be a statutory obligation to provide the Commissioners with sufficient resources to undertake comprehensive monitoring and investigations. In this context, the Home Secretary should be asked for an indication of the expected workload of say, the Covert Investigations Commissioner, who is to be responsible for keeping under review all those surveillance operations which fall within 'directed surveillance' (see above) and the use of covert human intelligence resources in Part II.
- 6.3 **However, as mentioned above, it is important also to clarify how the Commissioner is to monitor certain surveillance activities in the absence of any requirement on the person authorising the activity to inform the Commissioner.** This is the position in relation to:
- 'direct surveillance' under Part II;
  - the use and conduct of covert human intelligence sources under Part II; and
  - the acquisition and disclosure of communications data under Part I.
- 6.4 **JUSTICE has long argued that proper accountability requires greater transparency through the publication of more detailed annual reports by the Commissioners.** In countries such as Australia, New Zealand and the United States, the law requires publication of information on such matters as the number of applications refused, the average duration of warrants and their extension, the categories of serious crime involved. They also include statistics on the effectiveness of the operations in terms of arrests, prosecutions and convictions and the cost of the operations. This is seen as a necessary and important form of accountability. We would specifically refer to the United States annual 'Wiretap Report' which contains information on all these issues, together with an Annex containing a breakdown of each warrant. It is available at: <http://www.uscourts.gov/wiretap98/contents.html>.

### *The Tribunal*

- 6.5 We welcome the rationalisation of the surveillance complaint system into one Tribunal. **However, we remain concerned that the Tribunal is not just a piece of human rights 'window dressing' which in practice does not provide an effective remedy for individuals.** The failure of the existing surveillance tribunals ever to uphold a complaint demonstrates that this is a serious and legitimate concern.
- 6.6 JUSTICE has criticised the existing surveillance tribunals for:<sup>13</sup>

---

<sup>13</sup> See pages 24 –27 of the report, [Under Surveillance](#).

- having no jurisdiction over a surveillance operation that is not authorised (i.e. by a warrant or Commissioner)
- having to apply judicial review principles
- applicants having no right to an oral hearing
- very limited disclosure of evidence
- no reasoned decision
- no appeal or judicial review of the decision in the courts

6.7 Apart from extending the remit of the Tribunal to unauthorised conduct under cl.56(7), the other shortcomings mentioned above either remain the same or are subject to delegated legislation and therefore difficult to assess. We look at each separately.

#### *Limited to judicial review principles*

6.8 Under cl.58(2) and (3) the Tribunal has to apply the principles of judicial review when hearing proceedings under the Human Rights Act (cl.56(2)(a)) and when considering a surveillance complaint (cl.56(2)(b)). Under current procedures, it effectively means that the Tribunal may only decide whether the authorisation for the conduct was manifestly unreasonable in the circumstances or was based on procedural irregularity. **The Tribunal cannot consider, for example, either the accuracy or the merits of the evidence put forward in support of a warrant or other form of authorisation.**

6.9 It is not clear why the Tribunal should be limited in this way. In the recent cases of Chahal v UK and Tinnelly v UK, the ECtHR 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 is also questionable whether these principles are compatible with the Human Rights Act proceedings, particularly as Art 8 ECHR requires a test of proportionality not presently found in the judicial review principles.

#### *Oral hearing and disclosure*

6.10 The Bill does not give an applicant an automatic right to an oral hearing. This will depend on the rules to be made under cl.60(4). It is also unclear to what extent the delegated legislation will include procedures for appointing a special advocate (as applies in the Special Immigration Appeals Tribunal) when material cannot be disclosed to the applicant on national security or other sensitive grounds.<sup>14</sup> **As these are important matters for ensuring that applicants are accorded procedural justice in accordance with Art 6 ECHR, the Home Secretary should be asked to detail his intentions for the content of such rules.**

#### *Reasoned decision*

6.11 At present, cl.59(4) prohibits the Tribunal from giving reasons for its decision, although the Secretary of State may make rules permitting it to give fuller information (cl.60(2)(i)). It is strongly arguable that a blanket prohibition against ever giving reasons is disproportionate and incompatible with the Human Rights Act. **Since the Tribunal is to rule on potential**

---

<sup>14</sup> This was introduced following the ECtHR decision in *Chahal v UK* when the Court made it clear that it should be possible to employ procedures which both accommodate legitimate security concerns and which also accord individuals a substantial measure of procedural justice.

**infringements of privacy under Art 8 (and probably determine civil rights for the purpose of Art 6) the Human Rights Act may well require that reasons are only withheld when there is a sufficient and proportionate reason for doing so.** JUSTICE believes that this should be recognised on the face of the Bill or, at the very least, in the delegated rules.

### *Appeals*

- 6.12 There is no appeal from a Tribunal decision, other than in circumstances as to be ordered by the Secretary of State (Cl.58(7)). **No indication is given either in the Bill or in the Explanatory Memorandum as to the circumstances when appeal may be permitted.** It is questionable whether the prohibition is compatible with the Human Rights Act in so far as it excludes an appeal in proceedings taken under cl.56(2)(a) for conduct alleged to be incompatible with ECHR rights.

### *Notification*

- 6.13 Any complaints procedure will inevitably offer only limited possibilities of an effective remedy (as required by Art.8 ECHR) since, by definition, in most cases people are unaware that they have been the subject of an interception or other form of surveillance.
- 6.14 A number of countries have dealt with this problem by adopting some form of notification. For example, in the United States and Canada, the judge granting the warrant has the discretion to notify the named individuals within 90 days of its expiry so long as the 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 Solicitor General's annual report on the use of electronic surveillance in Canada shows that 515 people were notified during the period of 1997- 98. Many European countries including Denmark, Germany and the Netherlands have some form of notification. It is also a requirement of the 1987 Council of Europe's Recommendation on the use of data in the police sector.
- 6.15 The ECtHR looked at the issue of notification in the leading surveillance 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 on the facts, the Court placed considerable emphasis on the fact that Germany law required notification of the individuals as soon as this was possible without prejudicing police activities.
- 6.16 We fully acknowledge that this is a difficult issue but it is important that it is tackled. **JUSTICE believes that, as a minimum, notification is required where there has been a breach of the statutory requirements covering surveillance operations, subject to an exception on grounds of prejudicing police operations.** This means that there should be a duty on the authorising official (i.e. Secretary of State, Commissioner or designated person) to notify an individual where, for example, a warrant or other form of authorisation has been improperly or erroneously issued or complied with.

## **ANNEX 1**

### **Article 6 : Right to a fair trial**

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.
2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
3. Everyone charged with a criminal offence has the following minimum rights:
  - (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
  - (b) to have adequate time and facilities for the preparation of his defence;
  - (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
  - (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
  - (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

### **Article 8: Right to respect for private and family life**

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

## ANNEX 2

Statutory regimes covering surveillance include:

- interception of communications under Part I RIP Bill [Secretary of State authorisation]
- the acquisition and disclosure of communications data under Part I RIP Bill ['designated persons' authorisation]
- the decryption of protected material under Part III of RIP Bill [Circuit judge authorisation]
- 'intrusive surveillance' by the police and other law enforcement agencies under Part II of RIP Bill [approval by Commissioner]
- 'intrusive surveillance' by the intelligence services and armed forces under Part II of RIP Bill [Secretary of State authorisation]
- intrusive surveillance (involving trespass or criminal damage) by the police and other law enforcement agencies under Part III of the Police Act 1997 [approval by Commissioner]
- intrusive surveillance ('bugging and burglary') by the intelligence services under the Intelligence Services Act 1994 [Secretary of State authorisation]
- 'directed surveillance' by the police and other law enforcement agencies under Part II of RIP Bill [self-authorisation by prescribed persons]
- surveillance by covert human intelligence sources (informers etc) under Part II of RIP Bill [self-authorisation by prescribed persons].