REGULATION OF INVESTIGATORY POWERS BILL

SECOND READING BRIEFING

INTRODUCTION

1.1. In its report, *Under Surveillance*, JUSTICE came to the overall conclusion that the present legislative and procedural framework governing the use of covert surveillance methods by the police and others is out of date, inconsistent and unable to provide the safeguards required to comply with the Human Rights Act 1998. We therefore welcome this Bill whose purpose is to ensure such compatibility, particularly with regard to Art. 8 ECHR (the right to respect for private life).

1.2 However, in providing for future regulation, we urged the Government to take an integrated approach so as to bring consistency and cohesion to this area of law. Unfortunately, this Bill does not do so and therefore represents a missed opportunity to rationalise a patch-work of legal measures. Though it is a difficult task to balance law enforcement needs with individual privacy rights, the Bill 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 1)**. An investigation may well require authorisation under more than one regime.

1.3 Another general problem with the Bill's structure is that it contains a number of provisions for secondary legislation (orders, regulations, codes of practice) where the scope, intent and safeguards of the delegated powers are insufficiently set out in the statute. This makes it difficult to assess whether some of the provisions will, in fact, operate in a way that is human rights compliant. It is essential therefore that the Home Secretary be urged to publish drafts of any secondary legislation during the course of the parliamentary process.

1.4 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. **This briefing raises only those major points that we believe would benefit from debate and clarification at Second Reading.[1] JUSTICE is preparing a detailed human rights audit of the Bill for Committee stage.**

PART 1: INTERCEPTION OF COMMUNICATIONS

2.1 This repeals the Interception of Communications Act 1985 (IOCA) and replaces it with a similar warrant procedure requiring authorisation from the Secretary of State. It is intended to cover all forms of communication including

[1] For comments on Part III of the Bill dealing with the decryption of protected material, see the briefing published by the Foundation for Information Policy Research (FIPR) and available from http://www.fipr.org.

e-mails, faxes and pagers. With certain exceptions, it extends to interceptions on private telecommunication systems so that, for example, phones in offices and police stations are covered. It also deals with the acquisition and disclosure of communications data.

Executive authorisation

2.2 The question of who authorises 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'. Likewise, in discussing the safeguards offered by French law on telecommunications interceptions, it placed considerable emphasis on the safeguard of prior judicial authorisation.[2]

2.3 This is a debate that has taken place several times before. Putting it simply, 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.

2.4 **JUSTICE's position is that the most intrusive surveillance operations, including interceptions, should all be subject to the same warrant procedures with authorisation by a High Court Judge (whether acting as a Commissioner or not).** This is the practice in a great number of other countries. It would also bring the law on interceptions in line with similarly intrusive surveillance methods under Part III of the Police Act 1997 and Part II of this Bill (see Annex 1).

Exemptions for business monitoring

2.5 The Bill allows a person with a right to control a private communications network to intercept on their own network without committing an offence, although they may be liable for the civil tort of unlawful interception (cl.1(6)). This allows, for example, a company to monitor and record telephone calls made from the public.

2.6 We question whether this is too wide an exemption in certain circumstances. As the ECtHR has emphasised, the notion of private life under Art. 8 can extend to the office and to business and professional activities.[3] This means that telephone conversations and e-mail at work can fall within Art. 8 and therefore safeguards for individuals are required. **We believe that this provision should, at the very least, be subject to the regulations that the Secretary of State is to make in relation to lawful interceptions carried out for business purposes (cl.4(2)). These should specifically cover the private interests of employees whilst at work.**

Exemption for privileged material

2.7 There are no provisions for special procedures covering intercept material that is legally or otherwise privileged material. The ECtHR in Campbell v UK

[2] Huvig v France (1990)
[3] Neimitz v Germany (1992); Halford v UK (1994)

stated that a high level of protection is to be accorded to these sensitive categories of material. Although, it may be the intention to address these in a code of practice, **JUSTICE considers that the provisions should be included on the face of the Bill in relation to both Parts I and II (like the Police Act 1997).**

Intercept material as evidence

2.8 Generally, the present position of prohibiting the use of intercept material as evidence is to remain (see cls.16 and17). However, under cl.17(5) the prosecution may be ordered to make disclosure of the material to the trial judge who, in turn, may direct the making of an admission of fact. There is no provision for disclosure to the defence (other than for specific intercept offences). This is likely to raise fair trial arguments under Art. 6 ECHR particularly in relation to the 'equality of arms' principle.

2.9 **JUSTICE believes that lawfully intercepted material should be *prima facie* admissible as evidence in criminal proceedings, subject to the usual disclosure of evidence rules and judicial discretion**. This is the position under Part III of the Police Act 1997 in relation to material obtained by technical bugging devices; 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.

Acquisition and disclosure of communications data.

2.10 Communications (or 'metering') data is to cover all information other than the contents of the communication itself. It includes, for example, a subscriber's details, the names, numbers and e-mail addresses 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.

2.11 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.

2.12 Although, under the Bill, the disclosure of such data is to be authorised by a 'designated person' from one of the 'relevant authorities', no indication is given as to the rank or position of this person (Cl.24(2)). **As this is a key safeguard, the Home Secretary should specifically be asked to give details of who is to be prescribed.**

2.13 In addition, the Bill does not provide for any specific safeguards for the holding and destruction of this data, as it does for interceptions material (see cl.14). And, although the Interception of Communications Commissioner is required to review the working of these provisions, 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.[4]

[4] 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

3.1 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)

Directed surveillance v intrusive surveillance

3.2 'Directed surveillance' is surveillance of individuals during a specific but non-intrusive investigation. It is subject only to self-authorisation within the agency undertaking the action by persons who are yet to be identified. 'Intrusive surveillance' is action by a person or device on or outside residential premises or in a private vehicle. This is intended to remedy the gaps in Part III of the Police Act 1997 which is limited to surveillance devices whose placement involves either trespass or criminal damage. Other than in cases to be authorised by the Secretary of State,[5] the authorisation is to follow that of the Police Act: initially by a chief constable with approval required from a High Court judge appointed as a Commissioner (cl.34).

3.3 **JUSTICE believes that the provisions in the Bill which attempt to relegate certain conduct under the lesser controls of 'directed surveillance' rather than the more stringent ones covering 'intrusive surveillance' need to be seriously questioned for their compliance with Art.8 requirements.** We also believe that the wide powers given to the Secretary of State under cl.44 to order that any conduct falling within directed surveillance be treated as intrusive surveillance and vice versa are wholly misplaced**.**

3.4 For example, a surveillance device used from outside residential premises or a private vehicle which 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 (cl.25(4)). Thus using a remote listening device located away from a house to listen in to conversations in the house may not amount to 'intrusive surveillance' but only to 'directed surveillance', depending on its quality.

3.5 **However, if the intention is to observe, listen to or capture images of a person in residential premises through the use of such a device, it must be assumed that the action is intended to be intrusive, irrespective of the quality of the material actually obtained.** And, in any event, how is the quality of the information to be anticipated in advance, so as to know which statutory regime to follow? Following the wrong regime risks the conduct being unlawful and the material inadmissible as evidence.

3.6 Similarly, the interception of a communication with the consent of one of the parties to the communication is to continue to be exempted from the interception regime of Part I and also the new 'intrusive surveillance' provisions of Part II (cls.25(4)and 45(4)). This practice is known as 'participant monitoring' and is especially relied upon with informers giving the necessary

[5] Only on an application by a member of the intelligence services, official of Ministry of Defence or member of armed forces.

consent to the interception. Although unclear, it may be intended that such conduct is now to come under the lesser controls of 'directed surveillance'. **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 communication is being intercepted by a state agency.**

Covert human intelligence sources

3.7 JUSTICE particularly welcomes the provisions placing the use and conduct of informers and undercover officers under statutory control. However, we question whether it is sufficient to rely solely on the lesser control of an agency's self-authorisation, especially in relation to *participating* informers and undercover officers (i.e. those actively involved in the criminal conduct). The EctHR has strongly criticised this practice in the case of Kopp v Switzerland (1998): '*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…'*

3.8 Many of the detailed controls in this and the other areas covering surveillance conduct are to be set out in orders and codes of practice. As mentioned before, this poses problems in assuming that the Bill will operate in a way that is human rights compliant. For example, cl.28 gives the Secretary of State the apparently unfettered power to add to the permitted grounds for authorising the use of informers and undercover officers. **In these circumstances, the Home Secretary should be asked to specify the nature of the other grounds that he envisages may be included in the future so as to ensure that they are within the scope of Art 8(2) ECHR.**

PART IV: SCRUTINY BY COMMISSIONERS AND COMPLAINTS TRIBUNAL

4.1 The existing system of oversight by Commissioners is to extend to these new areas of covert surveillance, backed by a single Tribunal to hear complaints in relation to *all* surveillance conduct, including that of the intelligence services.

4.2 JUSTICE has long argued that proper accountability requires greater transparency of these processes through the publication of more detailed annual reports by the Commissioners. As in other countries, it should be a requirement to include information on such matters as the cost and effectiveness of the particular surveillance method in terms of arrests, prosecutions and convictions.

4.3 As the Tribunal's procedure is to be determined largely by delegated legislation, it is difficult to assess how far current shortcomings – the lack of an oral hearing, withholding of evidence from the complainant and no reasoned decision – will be remedied. **Up to now, not one application to any of the existing tribunals has been upheld**.

4.4 A complaints procedure can only offer limited possibilities of an effective remedy if, in the main, people are unaware that they have been the subject of an interception or intrusive surveillance. Although we acknowledge that this is a difficult issue, many other countries including the United States, Canada, Germany, Denmark and the Netherlands have some form of notification after

the event subject to police investigations not being prejudiced. **JUSTICE believes that this should be properly debated in the context of this Bill.**

ANNEX 1

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 l 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].