



JUSTICE

**SUBMISSIONS ON THE DRAFT CODES OF PRACTICE
UNDER THE REGULATION OF INVESTIGATORY
POWERS ACT 2000**

November 2000

THE INTERCEPTION OF COMMUNICATIONS

Draft Code of Practice under RIPA¹

November 2000

General comments

1. JUSTICE believes that it is preferable for the draft Codes to have a consistent format as far as possible. This means including a foreword in each that places the need for authorisation under RIPA for the use of interceptions and surveillance in the context of the Human Rights Act and particularly the need to protect Article 8 privacy rights.

Proportionality

2. As with the other draft Codes being consulted upon, reference is made to the principle of proportionality being important but no further explanation is given of the principle nor how it should be applied. As a key requirement of Article 8, its purpose should be spelt out in more detail, emphasising that the least intrusive conduct should be used wherever possible.

Specific comments

3. Under Para 2.3: JUSTICE has expressed concern that the allocation of 'participant monitoring' to the lesser authorisation procedures of 'directed surveillance' may be insufficient to comply with Article 8 ECHR. We have therefore recommended that the codes highlight the need for greater safeguards in this kind of operation (see paragraph 21 of JUSTICE's response to the draft Covert Surveillance Code).

Communications subject to legal privilege

4. Under Para 3.6: Unlike Part III of the Police Act, the safeguards for material that attracts legal privilege are only in the Code and not in the body of the Act. We continue

¹ JUSTICE would like to acknowledge the assistance of Quincy Whitaker and Rebecca Trowler of Dougherty Street Chambers in drafting these comments.

to question whether this is sufficient to comply with Article 8 in light of the ECtHR's decisions requiring a particularly high level of protection to be accorded to such material. In these circumstances, it is essential that the Code sets out a high standard of safeguards, with detailed advice on the procedures to be followed.

5. For example, the Code should make clear that the person applying for the warrant is personally responsible for ensuring that a proper assessment of the likelihood of legally privileged material being intercepted has taken place and that the results are properly reflected in the application. This would mean the Director General of NCIS having personal responsibility for this in the case of police applications. Similarly, the Secretary of State should not merely take the likelihood of privileged material being intercepted 'into account'; he should be satisfied that the Article 8 principles of necessity and proportionality are complied with in relation to this particular matter. In order to comply with proportionality, applications where there is a significant likelihood of privileged legal material being intercepted should only be authorised in exceptional and compelling circumstances.

6. Under Para 3.9: JUSTICE believes that the Code should explicitly prohibit the interception of a lawyer's communications in any situation other than where the lawyer themselves are the object of criminal suspicions. Even then, valid legal privilege will endure in respect of clients who are not involved in a criminal conspiracy with the lawyer. The safeguards necessary to protect this material should therefore be spelt out, including a restriction that a warrant is only to be granted in 'exceptional and compelling circumstances, irrespective of whether this other material represents a 'substantial proportion' or not of the overall material intercepted.

7. Under Para 3.10: The draft Code states that intercepted material should not be transcribed 'unless it is necessary for a specified purpose'. The Code however does not stipulate either what are the specified purposes or the seniority of the person who is authorised to make such a decision. It is submitted that the grant of such authority should be at a very senior level and preferably by someone who is unconnected with the particular investigation. In addition such authorisations should be subject to a strict recording requirement and all records submitted to the Interception of Communications

Commissioner. Similar requirements should apply in relation to any dissemination and retention of such material.

8. The draft Code states that legally privileged material should be further safeguarded by taking reasonable steps to ensure there is no possibility of its contents becoming known to any person whose possession of it might prejudice any criminal proceedings related to the information. The Code should state how this safeguard is to operate in practice, because police awareness alone has the potential to prejudice criminal proceedings.

9. Under Para 3.11: It is essential that the Code includes definitions and descriptions as to what amounts to confidential medical, religious and journalistic material. Such definitions are included in the draft Covert Surveillance Code based on Part III of the Police Act. As regards confidential journalistic material, advice should be given that the Secretary of State (when authorising the warrant) and the police officers who handle such material should pay particular attention to ensuring that the confidentiality of journalistic sources are maintained in accordance with the requirements under Article 10. It is submitted that many of the comments regarding legally privileged material mentioned above apply equally to these other sensitive areas.

Interception warrants

10. Under Para 4.14: As with similar provisions in the other draft Codes, it is unclear how the Secretary of State exercises this duty of cancellation. We assume that in practice he or she is notified when a warrant is no longer necessary. However, we believe that this should be spelt out in the Code particularly as the Human Rights Act places a duty on those conducting the operation to ensure its cancellation as soon as it is no longer necessary in order to comply with Article 8.

11. Under Para 4.16: JUSTICE has consistently made the point that the records held should include the outcome of the interception operation in terms of its affect on subsequent arrests, prosecutions and convictions. This is in order to assess the effectiveness of the operations which, in turn, is relevant to determining the necessity

and proportionality requirements of Article 8 in relation to future operations. These comments are equally applicable to the records kept of Section 8(4) warrants.

Interceptions under mutual legal assistance agreements

12. Under Para 5.1: It should be mentioned that the two circumstances described are governed by the Convention on Mutual Assistance in Criminal Matters 2000. We would also question why the third circumstance in which interception assistance is sought under this Convention has been omitted from the Code. This covers interceptions under Article 20 which take place in relation to a telecommunication address in another country but without the need for technical assistance from that country. Although this does not require a warrant to be issued by the Secretary of State, it nevertheless requires consent to be given that the interception may take place and under what conditions so as to apply the same safeguards as would be applied to a similar domestic case.

Safeguards

13. Under Para 7.1: JUSTICE would question why the nature of the safeguards for handling intercept material are 'necessarily classified'. In particular, we question why this needs to be a 'blanket' approach according such status to all safeguards, regardless of their nature or of the extent to which they can properly be treated as sensitive. Moreover, if all safeguards remain classified, then the basis upon which it is possible to assess the extent to which the Interception Commissioner properly complies with his duty to review the adequacy of the safeguards is severely restricted.

14. By way of example, section 15 (2) of the Act provides that the number of persons to whom intercept material is disclosed and the extent of disclosure must be limited to the minimum that is necessary for the authorised purposes set out in s.15 (4). Paragraph 7.4 of the draft code makes it clear that dissemination will only take place on a need to know basis and that this applies equally to dissemination inside or outside the intercept agency. The draft code proposes that in some cases this will be achieved by the person to whom material is subsequently disclosed being required to obtain the permission of the original interceptor before disclosing further. However, the draft code fails to identify which cases will give rise to a requirement of permission from the original interceptor or

by whom and how such cases will be identified. JUSTICE believes that the absence of explicit and accessible safeguards will, in relation to the majority of safeguards, create an unjustified lack of transparency and thereby limit the extent to which the scheme created by the Act, and in particular the performance of the Commissioner and the Tribunal, can be monitored and assessed.

15. In any event, whether the safeguards are classified or not, we would hope that the Data Protection Commissioner has been consulted and her recommendations fully implemented. Although the Data Protection Act does not apply to data certified to be held on national security grounds, it does apply to that held for crime investigation purposes.

Disclosure to ensure trial fairness

16. Under Para 8.8: We seriously question the grounds for saying that much intercepted material will not survive to the prosecution stage as it will have been destroyed in accordance with the s. 15 (3) safeguards of the Act. Apart from the draft Code stating that s. 18 (7)(a) does not mean that material should be retained against a remote possibility that it might be relevant to future proceedings, there is nothing to indicate on what basis a decision will be taken. That is, either to retain material for the authorised purpose of ensuring that the person prosecuting can carry out the duty of securing the fairness of the prosecution contained in s.15 (4)(d) or conversely to destroy it as being no longer necessary to retain it for that purpose.

17. While there remains a real possibility of prosecution arising out of the intercept material, or to which the material might be relevant, JUSTICE does not believe that it would be possible to conclude that it was not necessary to retain the material for the s.15(4)(d) purpose before the nature of the charges, the nature of the defence and issues in the trial are known. As it stands, inevitably there will be cases in which intercept material that has been destroyed would, had it been retained, have been sufficiently material to the issues in the trial to cause the prosecutor to seek to disclose it to the trial judge pursuant to s.18 (7)(b) and to cause the trial judge to order the prosecution to make an admission arising out of the material in the interest of justice. In

some cases the arbitrary destruction of intercept material whilst there remains a real possibility of prosecution will lead to a denial of the accused 's Article 6 fair trial rights.

18. JUSTICE believes that, where it is apparent that intercept material could or might be relevant to a future prosecution, then it will always be necessary to retain the material. It should be retained until either a decision is taken not to prosecute or, where a decision is taken to prosecute, the prosecutor has had sight of the material and carried out his or her duty in accordance with s. 18(7)(a). The draft Code should be amended accordingly.

19. Under Para 8.4: As JUSTICE has said before, we believe that the arrangements under s.18 of the Act for disclosure of the intercept material to the prosecutor and trial judge may breach the defendant's Article 6 fair trial rights.² We do not therefore agree with the statement that the general rule prohibiting use of intercept material under s.17 preserves equality of arms as required by Article 6 of the ECHR. In fact, because of the arrangements under s.18, we believe that the opposite is true.

20. It is clearly envisaged at paragraph 8.10 of the draft Code that in every case in which the intercept material has been retained the prosecutor 'should be informed' of the warrant and the material and be asked 'to assess the material's potential relevance' on the basis of the tests under the Criminal Procedure and Investigations Act 1996. It is also clearly anticipated that in most cases the prosecutor will not take the matter further and invite the trial judge to order the material to be disclosed to himself. The draft code anticipates that normally, the prosecutor's functions under s.18 (7)(a) will not fall to be reviewed by the judge (paragraph 8.13). Moreover, even where the prosecutor considers that the material affects or might reasonably affect the issues in the trial, he is bound by the draft Code to do no more than 'decide how the prosecution, if it proceeds, should be presented' (8.11).

21. It is at this point that we disagree. In our view, the Code should provide that where the prosecutor concludes that the material either undermines the prosecution case or assists the defence then the circumstances of the case will amount to 'exceptional circumstances' and disclosure of the material to the judge will be 'essential'

in the interests of justice. In other words, the prosecutor should be obliged to invite the judge to make an order for disclosure to himself in these circumstances. The code should also provide that the same interpretation should be given to 'exceptional circumstances' and 'essential in the interests of justice' in relation to the making of admissions pursuant to s.18 (9) of the Act.

22. We also believe that the prosecution would achieve an unfair advantage (contrary to what is stated in paragraph 8.7 of the draft Code) in those cases in which the prosecutor has had access to intercept material which does affect the issues in the trial but which has not been disclosed to the judge and therefore there is no possibility of the prosecution being ordered to make admissions in the interests of justice.

² See paras. 3.15- 3.21 of JUSTICE's Human Rights Audit of RIPA, May 2000.

THE COVERT SURVEILLANCE

draft Code of Practice under RIPA

General Comments

Purpose of the Legislation

1. Given the importance of the RIPA regulatory framework in ensuring compliance with the Human Rights Act, it would be appropriate to emphasise this in the foreword to the Code. It should be made particularly clear that the system of authorisations for covert surveillance is to protect the right to respect for private life of those subject to surveillance, as well as their fair trial rights under Article 6.

The Scope of the Legislation and the Relationship with the Police Act

2. Also in the foreword, there should be a clear statement of the different conduct that is regulated by Part II of RIPA, by Part III of the Police Act 1997 and the relationship between the two provisions. Furthermore, it is not always clear throughout the body of the draft Code that this is a joint Code, replacing the existing one under the Police Act. For example, when dealing with what appear to be general sections on 'Authorisations and Product' (p.9), there is only reference to surveillance under RIPA.

Proportionality

3. Throughout, the draft Code makes reference to the principle of proportionality, and the need to assess surveillance in accordance with it. However, no further explanation is given of the principle, or of how it should be applied. As this is a key requirement of Article 8, it should be spelt out in more detail, emphasising that the least intrusive conduct should be used.

Urgency

4. At several points, the draft Code makes reference to the particular procedures that apply under the Act in cases of urgency, but little further guidance is given as to how these are to be applied. JUSTICE has queried the provisions of RIPA which allow for normal safeguards to be circumvented in situations which are regarded as urgent. In our human rights audit of RIPA as a Bill, we pointed out that, in an age of new technology, it should not be necessary to treat urgent applications differently, and to apply lesser safeguards in urgent cases. In particular, the circumvention of the need for judicial approval of intrusive surveillance in cases which are considered to be urgent gives cause for concern.

5. We therefore believe that the designation of situations of urgency should be approached with caution, and that the principle of proportionality should be strictly applied to such designations. This means giving greater guidance in the Code as to the situations which can be considered to be urgent, to prevent the urgency provisions being used routinely. Although the draft Code makes clear at one point that these provisions should not be used as a matter of practice (para 4.19), the means for achieving this need to be spelt out. For example, it should be specified that authorisation without approval of the Surveillance Commissioner should not be given unless it is impossible for the Commissioner to provide authorisation in time.

Specific Comments

6. Under Para.1.5: JUSTICE would query the accuracy in practice of the general statement that authorisations may be made under RIPA for surveillance conduct to take place on territory outside the UK. Although s 27(3) of RIPA states this to be so, it has to be put in the context of mutual assistance arrangements as they exist now and may be in the future. Without this context, it suggests that a UK law enforcement agency may presently conduct (or ask someone else to conduct) surveillance in another country on the basis of a RIPA authorisation. Apart from the UK's particular arrangements with France in relation to the Channel Tunnel, we are unaware of any other bilateral agreement at present that allows UK agencies to conduct surveillance on foreign territory. It is yet clear to what extent RIPA authorisations will apply to the UK's future

participation in the Schengen *acquis* dealing with cooperation over surveillance operations, particularly Art 40 cross-border surveillance. Similarly, apart from the specific Part I RIPA provisions on interceptions, it is unclear how far Part II authorisations will apply, for example, to joint investigatory teams operating outside the UK under the Mutual Assistance Convention on Criminal Matters 2000 when it is in force.

7. Under Para 2.1: It is not clear from the wording of this paragraph that public authorities have also a positive obligation under Article 8 ECHR to protect privacy rights. This is well established in the jurisprudence of the ECtHR (*Lopez Ostra v Spain* (1995) 20 EHRR 277, *Osman v UK* (2000) EHRR 255). This places an even stronger duty on public authorities to obtain authorisation for surveillance that interferes with privacy; it is not just a question of using authorisation as a defence against a possible legal challenge, as presently drafted.

8. Under Paras.2.3 and 2.4: The possibility of collateral intrusions into privacy needs to be strengthened. At present the draft Code states only that 'particular consideration should be given ...'. It would be more useful to spell out the need for justification of any intrusion on third party privacy rights by surveillance, on the basis of Article 8.2 ECHR.

9. Under Para 2.7: This paragraph seems to be particularly vague in its wording and its message is unclear. For example, what is meant by the phrase 'the fullest consideration should be given' particularly in the example given of a person's home? As this would fall within 'intrusive surveillance', it would necessarily have to go through stringent tests as it requires the judicial approval of a Commissioner.

10. In order to give proper guidance, this paragraph should be used to set out a sliding scale of places 'where there are special sensitivities' and where the expectations of privacy may be greater. This should specifically include advice on surveillance in offices.³ As JUSTICE pointed out in its human rights audit of the Bill, the jurisprudence of the ECtHR has held that privacy rights may arise in relation to business premises

³ It will be necessary to ensure that there is consistency in the advice given in this Code and the Code or Practice on the Use of Personal Data in Employer/Employee Relationships, currently under consultation from the Data Protection Commissioner's office.

(*Niemitz v Germany* (1992) 16 EHRR 97). Although this is fully recognised under Part III of the Police Act 1997 by requiring prior judicial approval of the surveillance conduct, such premises fall within the lesser safeguards of ‘directed surveillance’ under RIPA. In the light of this, it should be made clear in the Code that particular care should be exercised to comply with the Convention standards of necessity and proportionality when authorising surveillance in offices and any other special places where there may be a greater expectation of privacy.

Confidential material

11. Under Para 2.9: This need to be clarified as the language of this paragraph appears to address the use of covert intelligence sources rather than the use of surveillance.

12. It should be noted that the ECtHR decisions require a particularly high level of protection to be accorded to legally privileged material under Article 8 (*Campbell v UK* (1992) 15 EHRR 137). In *Kopp v Switzerland* (1999) 27 EHRR 91 the Court considered that the ‘prescribed by law’ requirement in Article 8.2 meant that the law should make clear how legally privileged material was to be protected in practice. We would therefore have preferred to see these protections being included in the primary legislation, as they are in Part III of the Police Act. However, given that it is now to be dealt with solely in a Code of Practice, it is important that, at a minimum, it should set out clearly (and in more detail than at present) the particular measures necessary to comply with the ECHR and the Human Rights Act.

Handling and Disclosure of Product

13. Under Para 2.16: The test for holding on to material obtained through a surveillance exercise seems to be if ‘it might be relevant’ to another investigation or to future civil or criminal proceedings. When it comes to the interests of national security or the economic well-being of the UK, the test to be applied is whether it ‘may be of use’.

14. In our view these tests fall far short of the standard required by the Data Protection Act 1998, the Human Rights Act 1998 and the Council of Europe's Recommendation R 87(15) on data protection in the police sector. In general, these require that the standard to be applied is 'necessity': see the fifth Data Protection Principle, the principle of 'necessity' under Article 8.2 ECHR and Principle 3.1 of the Recommendation.

15. We would also question the assertion that material that is obtained for a criminal investigation may automatically be used in civil proceedings. This needs to be clarified if it is to comply with the 'purpose limitation' restrictions of data protection legislation.

16. Under Para 2.18: This issue of disclosure of material outside of the public authority that lawfully obtained it is a complex one. Some disclosures are required by statute: an example of this is the enhanced criminal record certificate under the Police Act 1997. At the same time, the courts have allowed disclosure of police material to private individuals where it can be shown that there is a pressing need to do so (*R v Chief Constable of North Wales, ex parte Thorpe* 1995 1WLR 804). This is a lesser test than that recommended in Recommendation R (87) 15 which says that disclosures to private persons may only occur, inter alia, 'in exceptional circumstances....necessary for preventing a serious and imminent danger' (see also Principle 5).

17. The Code should more closely reflect these standards. At the same time, it needs to give guidance on the other considerations that must be taken into account including the common law duty of confidence and the tests of necessity and proportionality under Article 8.2.

Directed Surveillance

18. Under Para 3.3: As we point out at para. 10 above, there are particular places where it is justified to have a greater expectation of privacy. This should be emphasised and repeated here with particular reference to office premises.

19. Under Para 3.6: It would be useful to elaborate on the meaning of proportionality, and to stipulate, for example, that the authorisation can only be granted if its purpose could not be achieved by less intrusive means.

20. Under Para 3.10: The undesirability of self-authorisation should be stated in considerably stronger terms. In principle, in order to safeguard against abuse or the appearance of it, authorising officers should never be responsible for authorising their own activities, other than in truly exceptional circumstances in small organisations. In large organisations, such as the police, there should be no circumstances under which officers authorise their own surveillance activities as this would entirely defeat the purpose of the safeguards.

21. Under Para 3.16: JUSTICE has consistently expressed concern that interception of a communication with the consent of one of the parties is treated as anything other than another form of interception. We believe that the non-consenting party whose privacy is infringed is entitled to the same level of safeguards as any other person whose communications are intercepted. We therefore remain of the view that the allocation of participant monitoring to 'directed surveillance' under RIPA may be insufficient in practice to ensure compliance with Article 8. However, in order to highlight the need for greater safeguards, the Code should state that particular caution should be exercised in granting an authorisation in such circumstances due to the privacy rights of the non-consenting person.

Intrusive Surveillance

22. Under Para 4.2: There should be further guidance in this paragraph on the meaning of 'information of the same quality and detail' as from a device present on the premises. There should be some guidance given as to the clarity in a picture, for example, that would be considered to amount to an 'intrusive' surveillance.

23. Under Para 4.22: It is noted here that the Act permits authorisation from any Secretary of State and therefore not necessarily from the relevant department. We believe that it would be proper for the Code to ensure that authorisation should always

be gained from the Secretary of State for the relevant department, other than in the most exceptional circumstances.

24. Under Para 4.42: The Code should specify that the authority should also maintain a record of the outcome of any surveillance operation, including whether the surveillance has led to arrests, prosecutions and convictions as a result of the material gained from the surveillance operation. This will enable an assessment to be made of the effectiveness of the operations conducted which, in turn, is relevant to determining the necessity and proportionality of future surveillance operations.

25. Under Para 5.5: JUSTICE expressed concern in relation to the Code drawn up under Part III of the Police Act, that there might be considerable difficulties with identifying the relevant person whose consent should be obtained in respect of interference with property by the police or other similar authorities, given the complex nature of landlord and tenant law. We noted that a mistake as to the person whose consent was necessary would almost certainly result in a breach of Article 8 privacy rights. In the light of this, it may be advisable to advise that an authorisation should be sought in cases where there is ambiguity as to the person whose consent should be sought, in addition to any authorisation that may be necessary under RIPA.

Oversight by Commissioners

26. Under Para 6.3: JUSTICE has previously raised the question of how the Surveillance Commissioner is to exercise proper oversight over those surveillance operations which are subject only to internal authorisation (i.e. directed surveillance and use of human intelligence sources) in the absence of any obligation to notify the Commissioner's office of such authorisations. In fact, there does not appear even to be an obligation on those bodies to notify the Commissioner of their intention to undertake such operations.

27. This is a serious omission that needs to be covered in the Code. The alternatives seem to be that every body intending to undertake such surveillance should inform the Surveillance Commissioner:

- of this intention, preferably prior to undertaking any operations so that the Commissioner can be assured that they fall within an authorised body under RIPA;
- of the number and nature of surveillance operations carried out by it on a regular basis (including certain prescribed information such as the numbers authorised, the period of authorisation, renewals etc.); and
- of any operation involving privileged material as it occurs.

THE COVERT HUMAN INTELLIGENCE SOURCES

draft Code of Practice under RIPA⁴

General Comments

Purpose of legislation

1. As with the other draft Codes, JUSTICE would like to see a clear statement in the foreword that the Regulation of Investigatory Powers Act (RIPA) is aimed at ensuring compliance with the Human Rights Act 1998. Although there is reference to Article 8 in para.1.4, it would be preferable to have a clearer statement in the foreword which emphasises the importance of the system of authorisation for covert human intelligence sources for protecting the right to respect for private life under Article 8 ECHR.

Proportionality

2. Reference is made throughout the draft Code to the principle of proportionality but little or no guidance is given as to how it should be applied. As we comment in response to the draft Covert Surveillance code, the principle is a key requirement of Article 8 and should be spelt out in more detail, emphasising that the least intrusive conduct should be used.

Urgency

3. From comparative research undertaken around the time of the introduction of Part III of the Police Act, JUSTICE came to the conclusion that special provisions for urgent applications that circumvent the normal safeguards should not be necessary in an age of new technology. We therefore believe that the Code must be much clearer in ensuring that the urgency provisions are only used in the most exceptional

⁴ JUSTICE would like to acknowledge the assistance of Professor Michael Maguire, Cardiff University, in drafting these comments.

circumstances. (See also paragraphs 4 and 5 of JUSTICE's response to the draft Surveillance code).

Rewards

4. A striking omission from the draft Code is any discussion about rewards for sources (other than a reference under record keeping). As the incentive to act as a source has implications for the processes of recruitment and tasking, it is important that the ethical and practical issues are covered. Even if it is more appropriate that detailed guidance is included in ACPO guidelines, the fact that RIPA itself refers to 'inducing' a source (s 26(7)) means some guidance has to be given. As our report, *Under Surveillance*, shows there are serious ethical issues particularly around non-financial rewards that may affect the conduct of a source.

Participating sources

5. In JUSTICE's human rights audit of the Bill we recommended that a distinction be drawn between different categories of informers and undercover police work in order to comply with Article 8 (see paragraph 5.20). We believe that participating sources who not only 'befriend' but are also actively engaged in criminal conduct, potentially pose risks for greater intrusion. We would therefore like to see the Code reflecting such a distinction in the safeguards generally but particularly in the requirement for an authorising officer from a more senior rank.

Specific comments

6. Under Para 1.5: We have questioned the accuracy of a similar statement in the draft Code on Covert Surveillance (see para. 6). For example, we are unaware of any current bilateral agreements that allow an undercover officer authorised under UK law to operate in the territory of another country. We also question the position under the forthcoming legislation of the Schengen *acquis* and the Mutual Assistance Convention 2000.

Authorisation

7. Under Para 2.4: As it is critical to what extent a source – particularly an undercover officer - may participate in the commission of a crime, it is essential that the phrase ‘within the limits of the law’ is spelt out. This is also relevant to the tasking of a source.

8. Under Paras 2.5 – 2.8: There is no indication of what weight to attach to such phrases as ‘take into account’, ‘give consideration to’ and ‘make an assessment of risk’. JUSTICE believes that as all the issues covered in these paragraphs are fundamental to the need for protection, decisions should be based on stronger considerations. For example, ‘ the privacy of persons other than the target should be intruded upon only where this is demonstrably unavoidable’ and ‘unless there are very strong reasons to make an exception, sources should not be exposed to high risk or injury’.

9. Under Para. 2.9: This is a rather benign description of ‘cultivating’ and recruiting a source. It fails to reflect the serious ethical issues that are often involved such as the use of inducements, manipulation and pressure. This is particularly relevant to the fact that recent research showed 84% of registered informers were either under arrest or subject to police enquiry at the time of recruitment.

10. As RIPA itself includes ‘inducing’ a source, it is essential that there is detailed guidance on what is acceptable and what is not (see para.4 above). Especially problematic is the practice of striking deals such as a concession over charge, sentence or bail.

11. Under Para. 2.15: The undesirability of authorising officers authorising their own activities is a matter that we have covered in relation to a similar provision under the draft Covert Surveillance Code (see para. 20). We do not believe that this should ever be necessary in a large organisation, such as the police. Even in small organisations, it should only be allowed when it is ‘organisationally impossible’ to do otherwise.

12. Under Para. 2.18: It is not clear how it is possible for an officer who is acting covertly to undertake the arrest of a suspected criminal.

13. Under Para. 2.19: We would question this statement for the same reasons as mentioned above at paragraph 6. If it is accurate, then the legal basis for such deployment of foreign law enforcement sources should be spelt out.

14. Under Para. 2.20: This is vague and unclear. For example, in what circumstances would this kind of action require authorisation and when not?

Special rules

15. Under Para. 2.28: Although this is a difficult question, JUSTICE is of the view that a person who is considered to be mentally impaired should never be authorised as a source.

16. Under Para. 2.29: In our report, *Under Surveillance*, we expressed our serious reservations about the practice of recruiting juveniles as informers. We recommended that their recruitment should be the exception rather than the norm: the lower the age of the juvenile, the more exceptional this should be. We note that some limitations are now included in the Regulation of Investigatory Powers (Juveniles) Order 2000 and these are to be welcomed. There should, however, also be a clear statement in the Code, either at this point or later in relation to tasking, that juveniles should not take part in a criminal activity as a participating informer other than in the most exceptional circumstances.

17. Although the above-mentioned Regulations provide that the authorising officer must be satisfied that the risks identified in the risk assessment are justified, there is no requirement that the authorising officer refuse authorisation where there is substantial risk to the juvenile concerned, irrespective of whether it has been explained and accepted by the juvenile.

18. Under Para 2.33: We have expressed our concern at the allocation of 'participant monitoring' to the lesser controls of 'directed surveillance' in our submissions to the draft Covert Surveillance Code (see paragraph 21).

19. Under Para. 2.34: The ‘wiring up’ of sources creates an extra intrusion of the targeted person, as well as an extra risk of discovery and reprisals for the source. Authorisations should therefore be at a higher level of assistant chief constable or equivalent.

20. Under Para. 2.35: Although the Act allows for an authorisation to last up to 12 months (s 43 (3)(b)), this is likely to be far too long a period, especially in the case of participating sources and undercover operations. Therefore the application for authorisation should also state the likely period required where a specific investigation or operation is involved. This will ensure that a proper review is carried out towards the end of this period; it will also ensure that authorisations are cancelled if they are no longer applicable. At the moment, it is difficult to see how authorising officers will know when the authorisation is no longer necessary as there is no obligation on anyone to inform them of this fact.

21. The principle of proportionality should be added to the list of things that need to be recorded under para. 2.35: that is, details of why it is necessary to use a source rather than less intrusive methods.

Management of sources

22. Under Para. 3.13: The records should also under (f) any inducement used for the source to be recruited. There should also be a requirement to record the outcome of using a source, particularly in relation to a specific operation. (See paragraph 24 of JUSTICE’s submission to the draft Covert Surveillance Code).

23. Under Para. 3.19: The test of ‘could be relevant’ does not comply with the requirements of data protection legislation or the Human Rights Act. In general, these require that the standard is one of ‘necessity’: see paragraphs 13-16 of JUSTICE’s submission to the draft Covert Surveillance Code.

