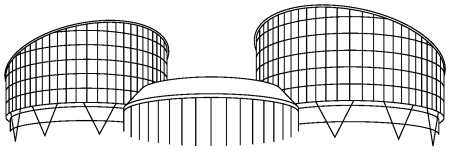

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

CASE OF R.E. v. THE UNITED KINGDOM

(Application no. 62498/11)

JUDGMENT

STRASBOURG

27 October 2015

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of R.E. v. the United Kingdom,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Guido Raimondi, *President,*
Päivi Hirvelä,
George Nicolaou,
Nona Tsotsoria,
Paul Mahoney,
Krzysztof Wojtyczek,
Faris Vehabović, *judges,*
and Fatoş Aracı, *Deputy Section Registrar,*

Having deliberated in private on 6 October 2015,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 62498/11) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by an Irish national, Mr R.E. ("the applicant"), on 7 October 2011. The President of the Section acceded to the applicant's request not to have his name disclosed (Rule 47 § 4 of the Rules of Court).

2. The applicant was represented by Ms Nichola Harte of Harte Coyle Collins, a lawyer practising in Belfast. The United Kingdom Government ("the Government") were represented by their Agent, Ms M. Addis of the Foreign & Commonwealth Office.

3. On 11 April 2013 the application was communicated to the Government.

4. By letter dated 2 July 2013 the Irish Government confirmed that they did not wish to exercise their right to intervene.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

5. The applicant was born in 1989 and lives in Newtownabbey, Northern Ireland.

A. Background

6. In 2006 a solicitor in Northern Ireland was arrested and charged with a number of offences, including inciting paramilitaries to murder and perverting the course of justice. The case arose out of the covert recording of his consultations with clients at Antrim police station. As a direct consequence of the criminal proceedings, solicitors in Northern Ireland became aware that their private consultations with detainees in police stations and prisons could be the subject of covert surveillance. Thereafter, solicitors attending detainees in police stations and prisons began to seek assurances from the police that their consultations would not be the subject of such surveillance.

7. When the police refused to give assurances, judicial review proceedings were initiated on the basis that there had been a breach of the common law right to legal and professional privilege, the statutory right to a private consultation with a lawyer, and Articles 6 and 8 of the Convention.

8. In the case of *Re C & Others* [2007] NIQB 101A the Divisional Court of the High Court of Justice in Northern Ireland found that, despite the express statutory right to private consultations, the covert surveillance of lawyer-client consultations was permitted by the Regulation of Investigatory Powers Act 2000 ("RIPA"). However, RIPA provided for two principal surveillance schemes: intrusive surveillance and directed surveillance. At the time of the hearing, covert surveillance of legal consultations was being treated as directed surveillance, which was the least restrictive of the two schemes. The Divisional Court held that the fundamental right of a detained person to consult a legal adviser privately necessitated an enhanced authorisation scheme and that protections afforded by the directed as opposed to the intrusive surveillance scheme offered insufficient protection. If the surveillance of consultations between legal advisers and clients in police custody was to be lawful for the purposes of Article 8 of the Convention, the safeguards for the carrying out of intrusive surveillance had to apply.

9. The applicants in these judicial review proceedings appealed against the court's ruling that the surveillance was permitted by the domestic legislation. The appeal went to the House of Lords, where it was referred to as *Re McE (Northern Ireland)* [2009] UKHL 15. The House of Lords agreed with the Divisional Court that although the provisions of RIPA could override, *inter alia*, legal professional privilege, the higher level of authority necessary for an intrusive surveillance warrant was required rather than the directed surveillance warrants that had, until then, been issued.

10. As the Police Service of Northern Ireland ("PSNI") had not appealed against the Divisional Court's ruling that the use of the directed surveillance scheme had breached Article 8 of the Convention, the House of Lords criticised the Secretary of State for not having taken any steps to ensure that

covert surveillance of legal consultations was not treated as directed surveillance.

11. Following the decision of the House of Lords in *Re McE* the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 ("the 2010 Order") was adopted and on 6 April 2010 a revised Covert Surveillance Code of Practice ("the Revised Code") came into effect. Pursuant to the 2010 Order, directed surveillance of consultations between a detainee and his or her professional legal adviser, representative or medical practitioner in connection with legal proceedings was to be treated, for the purposes of RIPA, as intrusive surveillance.

B. The facts of the present case

12. On 15 March 2009 the applicant was arrested in connection with the murder of a Police Constable believed to have been killed by dissident Republicans.

13. When first arrested the applicant was assessed by the Forensic Medical Officer as a "vulnerable person" within the meaning of the Terrorism Act Code of Practice. Pursuant to paragraph 11.9 of that Code of Practice, he could not be interviewed, save in exceptional circumstances, in the absence of an "appropriate adult". In the case of a person who was mentally vulnerable, an appropriate adult could be a relative or guardian, or a person experienced in dealing with mentally disordered or mentally vulnerable people. However, prior to being seen by either a solicitor or an appropriate adult, the applicant asked to speak to the officers in charge of the investigation "off the record". He was interviewed by police officers in the absence of a solicitor or an appropriate adult and during the course of that interview he gave information which led to the recovery of the gun used in the Constable's murder.

14. The applicant was detained in custody for twelve days. During this time he was twice seen by a Consultant Psychiatrist and on each occasion he was assessed as being vulnerable and requiring the presence of an appropriate adult. Also during this time his solicitor obtained an assurance from the PSNI that his consultations with the applicant would not be subject to covert surveillance.

15. On 25 March 2009 the applicant was charged with withholding information about the Constable's murder.

16. Following the charge the applicant was detained in custody on the ground that if released he would be at risk of harm from dissident Republicans.

17. The applicant was released on bail on 8 June 2009. He was arrested and questioned on a further occasion in October 2009 but was subsequently released without charge.

18. On 4 May 2010 the applicant was arrested for a third time in connection with the Constable's murder. Following his arrest his solicitor again sought an assurance from the PSNI that his consultations would not be subjected to covert surveillance. The PSNI informed him that

> "[they could] neither confirm nor deny whether any form of covert surveillance has been conducted in any instance. Covert surveillance is regulated by the Regulation of Investigatory Powers Act 2000, related statutory instruments and the Revised [Covert Surveillance] Code of Practice".

19. The applicant sought permission to apply for judicial review of the PSNI's refusal to give an undertaking that his consultations with his solicitor would not be subjected to covert surveillance. In particular, he alleged that the grounds upon which the authorisation of such surveillance would be appropriate were not sufficiently clearly defined and that the guidance concerning the securing and destruction of legally privileged confidential information was not sufficiently clear or precise.

20. On 6 May 2010 he was granted permission to apply for judicial review. In granting permission, the court directed that any subsequent consultations with his solicitor and his medical adviser should not be subject to covert surveillance.

21. On 7 May 2010 the applicant had his first consultation with a Consultant Psychiatrist.

22. The applicant was released without charge on 8 May 2010.

23. The charge of withholding evidence appears to have concluded without trial.

C. The domestic proceedings

24. The hearing of the judicial review application took place before a Divisional Court of the High Court of Justice in Northern Ireland on 28 June 2010. On 21 September 2010 the Divisional Court dismissed the applicant's claim.

25. In dismissing the claim, the court relied on *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010, which found that the regime under Part I of RIPA was compatible with Articles 6 and 8 of the Convention. Although it noted that *Kennedy* was concerned only with Part I of RIPA, the court considered that the reasoning expressed was "very relevant in view of the parallels between Part I and Part II of the surveillance legal regimes".

26. The court found, in particular, that reading RIPA, the 2010 Order and the Revised Code together it was clear that a surveillance operation could only properly be justified if it was a truly proportionate response to a real risk posed by the individual who was the subject of the surveillance, and if the potential usefulness of the surveillance was demonstrably shown. As the Court had indicated in *Kennedy*, the requirement of foreseeability did not require an exhaustive definition of all conduct that might justify a

decision on, for example, national security grounds, and similar reasoning applied in the present case. Consequently, the court held that the wording in the Revised Code was sufficiently clear.

27. With regard to the applicant's second allegation, the court accepted that the statutory provisions under Part I of RIPA, which had been considered by the Court in *Kennedy*, were more detailed, prescriptive and precise than those in Part II. However, taking together the 2010 Order, the Revised Code and the PSNI Service Procedure Implementing Code, the arrangements in place for the use, retention and destruction of retained material in the context of legal consultations was compliant with the Article 8 rights of persons in custody. Moreover, as the Revised Code made it clear that material subject to legal professional privilege was not admissible in court and should be safeguarded by the taking of steps to ensure that it did not prejudice any criminal or civil proceedings, a breach of Article 6 of the Convention would not occur. While there was a risk of a potential "chill factor" (insofar as clients might be less than frank with their solicitors if they were concerned that they were under covert surveillance), the court considered that the revised Code was sufficiently detailed and precise to reassure those in custody that, save in exceptional circumstances, their consultations with lawyers would be in private.

28. Finally, the court observed that the special considerations which applied to consultations with lawyers or doctors did not apply in the case of meetings with an appropriate adult. It therefore followed that surveillance of such meetings could be authorised as directed surveillance rather than intrusive surveillance.

29. On 9 November 2010 the Divisional Court heard an application for leave to appeal to the Supreme Court. Leave to appeal was refused although the court certified four questions of law of general public importance. These were as follows:

> "a. Do the current arrangements for authorisation of covert surveillance of consultations between a detained person and (i) his/her solicitor (ii) his/her medical practitioner and/or (iii) an appropriate adult violate Article 6 ECHR in as much as they permit the covert surveillance of legally privileged consultations and the retention of material deriving from legally privileged consultations?
>
> b. Do the current arrangements for authorisation of covert surveillance of consultations between a detained person and (i) his/her solicitor (ii) his/her medical practitioner and/or (iii) an appropriate adult violate Article 8 ECHR as a result of:-
>
> (i) a lack of precision and clarity in the guidance governing the authorisation of such surveillance; and/or
>
> (ii) inadequate guidance as to how and when legally privileged material obtained from such surveillance should be handled, stored, used and destroyed.
>
> c. Is the Police Service of Northern Ireland's Service Procedure "in accordance with the law" within the meaning of Article 8 ECHR?

d. Do the current arrangements for authorisation of covert surveillance of consultations between a detained person and an appropriate adult violate Article 8 ECHR because such surveillance can be authorised as *directed* rather than *intrusive* surveillance?"

30. An application for permission to appeal to the Supreme Court was refused by the Supreme Court on 11 April 2011.

II. RELEVANT DOMESTIC LAW AND PRACTICE

A. The interception, acquisition and disclosure of communication data

31. The provisions of domestic law which govern the interception, acquisition and disclosure of communication data (including Part I of the Regulation of Investigatory Powers Act 2000 ("RIPA") together with the relevant sections of the Code) are set out in *Kennedy v. the United Kingdom*, no. 26839/05, §§ 25 – 61, 18 May 2010.

B. Surveillance

1. *Re McE (Northern Ireland) [2009] UKHL 15 and Re C and Others [2007] NIQB 101*

32. Like the applicant in the present case, the claimants in *Re McE* had sought to judicially review the PSNI's refusal to grant assurances that their consultations with their legal representatives while in detention would not be the subject of covert surveillance. They asserted that the failure to provide assurances was incompatible with Articles 6 and 8 of the Convention; and that it breached both their common law right to legal professional privilege ("LPP") and their statutory right to consult a legal advisor in private.

33. In the Divisional Court, where the case was referred to as *Re C and Others* [2007] NIQB 101, Kerr LCJ, giving the leading judgment, held that RIPA imposed limits on both the common law right of legal professional privilege and the statutory right to consult a lawyer privately while in detention. In relation to the claimants' Convention rights, he did not find any evidence that the possibility of surveillance in any way affected the fairness of their trials contrary to Article 6 §§ 1 or 3 (b). He did, however, consider that insufficient reasons had been given to justify why this form of surveillance was not subject to the enhanced safeguarding regime used in respect of intrusive surveillance. He therefore found that there had been a violation of Article 8 of the Convention.

34. Somewhat unusually, the claimants were granted leave to appeal to the House of Lords, where the case was referred to as *Re McE (Northern*

Ireland) [2009] UKHL 15. Before the House of Lords, the sole issue was whether RIPA permitted covert surveillance of consultations with legal and medical advisors notwithstanding that such communication enjoyed LPP and there was a statutory right to consult these advisors in private. Lord Carswell, with whom Lords Hope and Neuberger and Lady Hale agreed, observed that RIPA and the relevant Code of Practice had clearly envisaged the surveillance of legal consultations. Relying on the Court's case-law, he accepted that "covert surveillance of legal consultations should not be regarded as prohibited and unlawful in all possible circumstances" and found that in the present case there was a need to incorporate exceptions to the inviolability of privileged consultations.

35. Their Lordships unanimously agreed with the Divisional Court judgment that the authorisation regime relating to directed surveillance could not be considered to be adequate when put against the intrusiveness of covert surveillance of legal or medical consultations.

36. In respect of the Code of Practice, Lord Phillips of Worth Matravers noted that

> "The draughtsman of the Code appears to have preceded on the premise that: (i) it is undesirable that communications subject to LPP which are disclosed in consequence of authorised surveillance should be used in criminal or civil proceedings; (ii) such communications would not be admissible in criminal proceedings; (iii) knowledge of such communications could prejudice criminal or civil proceedings.
>
> None of these premises is axiomatic. I would expect the Strasbourg Court to require English law to state clearly what use, if any, is permitted to be made of material covered by LLP that is disclosed by surveillance.
>
> The majority have held that RIPA permits the Code to authorise surveillance of communications between solicitors and their clients both in custody and outside it in those exceptional circumstances where this will be compatible with the Convention. The Code does not at present do so in a manner which is compliant with the Convention. I would make this observation. Covert surveillance is of no value if those subject to it suspect that it may be taking place. If it is to take place in respect of consultations between solicitors and their clients in prison or the police station, it will be of no value unless this is such a rare occurrence that its possibility will not inhibit the frankness with which those in custody speak with their lawyers. It would seem desirable, if not essential, that the provisions of the Code should be such as to reassure those in custody that, save in exceptional circumstances, their consultations with their lawyers will take place in private. The chilling factor that LLP is intended to prevent will not then occur."

37. Likewise, Lord Neuberger of Abbotsbury indicated that:

> "Lord Phillips has characterised the nature of the decision of the majority of your Lordships as being that RIPA permits the Code to authorise surveillance of communications between lawyers and their clients, whether or not in custody. That is indeed as far as our decision in this case goes, and we should not, I think, be taken as thereby endorsing the provisions of the Code, as we are not directly concerned with those provisions, and, in particular, whether they comply with the requirements of the Convention. Indeed, in my view, it must be highly questionable whether the Code sufficiently clearly identifies (or limits) either the circumstances in which surveillance

> may or may not occur, or how the information thereby obtained may or may not be used. At least as at present advised I share the doubts and concerns about the Code expressed by Lord Phillips [...]."

2. Amendments to the RIPA regime following Re McE (Northern Ireland) *[2009] UKHL 15*

38. As a consequence of the decision of the House of Lords in *Re McE* the Secretary of State produced the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 ("the 2010 Order"). So far as relevant the 2010 Order provides, under Article 3, that directed surveillance carried out in relation to anything taking place in, *inter alia*, a police station used for the purpose of legal consultations should be treated, for the purposes of Part II of RIPA, as intrusive surveillance.

39. A Revised Code of Practice "the Revised Code") was also drawn up and duly approved by both Houses of Parliament. Chapter 4 of the Revised Code specifically addressed legally privileged and confidential information (see paragraph 75 below).

3. The regime in place at the date of the applicant's detention

a. Directed and intrusive surveillance

40. Section 26 of RIPA defines directed and intrusive surveillance as follows:

> "(2) Subject to subsection (6), surveillance is directed for the purposes of this Part if it is covert but not intrusive and is undertaken —
>
> (a) for the purposes of a specific investigation or a specific operation;
>
> (b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
>
> (c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.
>
> (3) Subject to subsections (4) to (6), surveillance is intrusive for the purposes of this Part if, and only if, it is covert surveillance that —
>
> (a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
>
> (b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.
>
> (4) For the purposes of this Part surveillance is not intrusive to the extent that—
>
> (a) it is carried out by means only of a surveillance device designed or adapted principally for the purpose of providing information about the location of a vehicle; or

(b) it is surveillance consisting in any such interception of a communication as falls within section 48(4).

(5) For the purposes of this Part surveillance which—

(a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle, but

(b) is carried out without that device being present on the premises or in the vehicle,

is not intrusive unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

(6) For the purposes of this Part surveillance which—

(a) is carried out by means of apparatus designed or adapted for the purpose of detecting the installation or use in any residential or other premises of a television receiver (within the meaning of the Wirelss Telegraphy Act 1949) and

(b) is carried out from outside those premises exclusively for that purpose,

is neither directed nor intrusive.

...

(9) For the purposes of this section—

(a) surveillance is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place;

(b) a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose; and

(c) a relationship is used covertly, and information obtained as mentioned in subsection (8)(c) is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

(10) In this section "private information", in relation to a person, includes any information relating to his private or family life.

(11) References in this section, in relation to a vehicle, to the presence of a surveillance device in the vehicle include references to its being located on or under the vehicle and also include references to its being attached to it."

b. Authorisation

α. Directed surveillance

41. According to paragraph 5.8 of the Revised Code, a written application for a directed surveillance authorisation should describe any conduct to be authorised and the purpose of the investigation or operation. The application should include the reasons why the authorisation is necessary in the particular case and on the grounds listed in section 28(3) of RIPA; the nature of the surveillance; the identities, where known, of those

to be the subject of the surveillance; a summary of the intelligence case and appropriate unique intelligence references where applicable; an explanation of the information which it is desired to obtain as a result of the surveillance; the details of any potential collateral intrusion and why the intrusion is justified; the details of any confidential information that is likely to be obtained as a consequence of the surveillance; the reasons why the surveillance is considered proportionate to what it seeks to achieve; and the level of authority required (or recommended where that is different) for the surveillance. A subsequent record should be made of whether authorisation was given or refused, by whom, and the time and date this happened.

42. Section 30 of RIPA permits directed surveillance to be authorised by individuals holding such office, rank or position with relevant public authorities as prescribed by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010. In the case of the PSNI, only an officer of (or above) the rank of Superintendent may authorise directed surveillance.

43. Pursuant to paragraph 5.5 of the Revised Code, except in urgent cases the authorising officer must give authorisation in writing.

44. Section 28 of RIPA sets out the requirements for granting the authorisation of directed surveillance:

> "(1) Subject to the following provisions of this Part, the persons designated for the purposes of this section shall each have power to grant authorisations for the carrying out of directed surveillance.
>
> (2) A person shall not grant an authorisation for the carrying out of directed surveillance unless he believes—
>
> (a) that the authorisation is necessary on grounds falling within subsection (3); and
>
> (b) that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.
>
> (3) An authorisation is necessary on grounds falling within this subsection if it is necessary —
>
> (a) in the interests of national security;
>
> (b) for the purpose of preventing or detecting crime or of preventing disorder;
>
> (c) in the interests of the economic well-being of the United Kingdom;
>
> (d) in the interests of public safety;
>
> (e) for the purpose of protecting public health;
>
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
>
> (g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.
>
> (4) The conduct that is authorised by an authorisation for the carrying out of directed surveillance is any conduct that —

(a) consists in the carrying out of directed surveillance of any such description as is specified in the authorisation; and

(b) is carried out in the circumstances described in the authorisation and for the purposes of the investigation or operation specified or described in the authorisation.

(5) The Secretary of State shall not make an order under subsection (3)(g) unless a draft of the order has been laid before Parliament and approved by a resolution of each House."

45. In urgent cases paragraph 5.9 permits the necessary information to be supplied orally. Where this happens the authorising officer and the applicant should also record the following information as soon as it is reasonably practicable to do so: the identities of those subject to surveillance; the nature of the surveillance; the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was given; and where the officer entitled to act in urgent cases has given written authority, the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

46. In such cases authorisation may be given orally by the authorising officer or in writing by an officer entitled to act in urgent cases. A record that the authorising officer has expressly authorised the action should be recorded in writing by both the authorising officer and applicant as soon as reasonably practicable.

47. Paragraph 5.6 of the Revised Code states that a case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgment of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation had been given. An application was not to be regarded as urgent where the need for an authorisation had been neglected or the urgency was of the authorising officer or the applicant's own making.

β. Intrusive surveillance

48. According to paragraph 6.19 of the Revised Code, applications for intrusive surveillance operations need to set out a wide range of information about the authorisation in question, including the reasons why the authorisation is necessary in the particular case and on the grounds listed in section 32(3) of the 2000 Act; the nature of the surveillance; the residential premises or private vehicle in relation to which the surveillance will take place, where known; the identities, where known, of those to be the subject of the surveillance; an explanation of the information which it is desired to obtain as a result of the surveillance; details of any potential collateral intrusion and why the intrusion is justified; details of any confidential information that is likely to be obtained as a consequence of the surveillance; and the reasons why the surveillance is considered proportionate to what it seeks to achieve. A record should be made of

whether the authorisation was given or refused, by whom and the time and date at which this happened.

49. Section 32 of RIPA sets out the requirements for granting the authorisation of intrusive surveillance:

> "(1) Subject to the following provisions of this Part, the Secretary of State and each of the senior authorising officers shall have power to grant authorisations for the carrying out of intrusive surveillance.
>
> (2) Neither the Secretary of State nor any senior authorising officer shall grant an authorisation for the carrying out of intrusive surveillance unless he believes—
>
> (a) that the authorisation is necessary on grounds falling within subsection (3); and
>
> (b) that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.
>
> (3) Subject to the following provisions of this section, an authorisation is necessary on grounds falling within this subsection if it is necessary—
>
> (a) in the interests of national security;
>
> (b) for the purpose of preventing or detecting serious crime; or
>
> (c) in the interests of the economic well-being of the United Kingdom.
>
> (4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any authorisation shall include whether the information which it is thought necessary to obtain by the authorised conduct could reasonably be obtained by other means.
>
> (5) The conduct that is authorised by an authorisation for the carrying out of intrusive surveillance is any conduct that—
>
> (a) consists in the carrying out of intrusive surveillance of any such description as is specified in the authorisation;
>
> (b) is carried out in relation to the residential premises specified or described in the authorisation or in relation to the private vehicle so specified or described; and
>
> (c) is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.
>
> (6) For the purposes of this section the senior authorising officers are—
>
> ... ...
>
> (e) the Chief Constable of the Royal Ulster Constabulary and the Deputy Chief Constable of the Royal Ulster Constabulary; ..."

50. Section 32(6) of RIPA provides a list of senior authorising officers. In the case of the PSNI, the senior authorising officer is the Chief Constable.

51. Paragraph 6.6 of the Revised Code provides that the senior authorising officer or designated deputy should generally give authorisations in writing.

52. According to section 35(1), once authorisation is granted notice of the grant must be given to a Surveillance Commissioner. The Surveillance

Commissioner must then scrutinise the authorisation and decide whether or not to approve it (section 35(4)). Unless the case is one of urgency, the authorisation of intrusive surveillance by a senior authorising officer will not take effect until a Surveillance Commissioner has given written notice of his approval (section 36(2) and (3)).

53. In urgent cases paragraph 6.20 of the Revised Code allows information required at the time of application to be supplied orally. Where this occurs the applicant should record the following information as soon as reasonably practicable: the identities of those subject to the surveillance; the nature and location of the surveillance; the reasons why the authorising officer or the officer entitled to act in urgent cases considered the case so urgent that an oral instead of written authorisation was given; and/or the reasons why it was not reasonably practicable for the application to be considered by the authorising officer.

54. Pursuant to paragraph 6.6, oral authorisations may be given by the senior authorising officer or designated deputy and a statement that he or she has expressly authorised the conduct should be recorded in writing by the applicant as soon as reasonably practicable. Where it is not reasonably practicable having regard to the urgency of the case for either the senior authorising officer or the designated deputy to consider the application, paragraph 6.7 provides that an authorisation may be granted in writing by a person entitled to act only in urgent cases by section 34(4) of RIPA.

55. Pursuant to paragraph 6.8, a case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgment of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation had been given. An application was not to be regarded as urgent where the need for an authorisation had been neglected or the urgency was of the authorising officer or the applicant's own making.

56. When the authorisation is urgent it will take effect from the time it is granted provided notice is given to a Surveillance Commissioner.

γ. Rules and guidance applicable to both

57. Section 81(2)(b) RIPA defines "serious crime" as crime which satisfies one of the following criteria:

> "(a) that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;
>
> (b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose."

58. Section 81(5) provides:

"For the purposes of this Act detecting crime shall be taken to include–

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and

(b) the apprehension of the person by whom any crime was committed;

and any reference in this Act to preventing or detecting serious crime shall be construed accordingly ..."

59. Paragraphs 3.1 to 3.7 of the Revised Code provide additional guidance on the application of the necessity and proportionality test in respect of both directed and intrusive surveillance:

"The 2000 Act, 1997 Act and 1994 Act stipulate that the person granting an authorisation or warrant for directed or intrusive surveillance, or interference with property, must believe that the activities to be authorised are necessary on one or more statutory grounds.

If the activities are deemed necessary on one of more of the statutory grounds, the person granting the authorisation or warrant must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

It is important therefore that all those involved in undertaking directed or intrusive surveillance activities or interference with property under the 2000 Act, 1997 Act or 1994 Act are fully aware of the extent and limits of the authorisation or warrant in question."

60. With regard to collateral intrusion, paragraphs 3.8 to 3.10 of the Revised Code provide that:

"Before authorising applications for directed or intrusive surveillance, the authorising officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance or property interference activity (collateral intrusion).

Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed actions."

61. Pursuant to paragraph 3.27 of the Revised Code, where authorisations were granted orally under urgency procedures a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the applicant and the authorising officer as a priority. There would then be no requirement to submit a full written application.

c. Review of authoritsations

62. Paragraphs 3.22 to 3.26 of the Revised Code provides for the regular review of authorisations:

"Regular reviews of all authorisations should be undertaken to assess the need for the surveillance or property interference activity to continue. The results of a review should be retained for at least three years (see Chapter 8). Particular attention is drawn to the need to review authorisations frequently where the surveillance or property interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

In each case the frequency of reviews should be considered at the outset by the authorising officer or, for those subject to authorisation by the Secretary of State, the member or officer who made the application within the public authority concerned. This should be as frequently as is considered necessary and practicable.

In some cases it may be appropriate for an authorising officer to delegate the responsibility for conducting any reviews to a subordinate officer. The authorising officer is, however, usually best placed to assess whether the authorisation should continue or whether the criteria on which he based the original decision to grant an authorisation have changed sufficiently to cause the authorisation to be revoked. Support staff can do the necessary research and prepare the review process but the actual review is the responsibility of the original authorising officer and should, as a matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms.

Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in the further or greater intrusion into the private life of any person should also be brought to the attention of the authorising officer by means of a review. The authorising officer should consider whether the proposed changes are

proportionate (bearing in mind any extra intended intrusion into privacy or collateral intrusion), before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed.

Where a directed or intrusive surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a review to include the identity of these individuals. It would be appropriate to convene such a review specifically for this purpose. This process will not require a fresh authorisation, providing the scope of the original authorisation envisaged surveillance of such individuals. Such changes must be highlighted at the next renewal if the authorisation is to be renewed."

d. Duration and renewal of authorisation

α. Directed surveillance

63. Pursuant to paragraphs 5.10 and 5.11 of the Revised Code, a written authorisation granted by an authorising officer will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the time at which it took effect, while urgent oral authorisations or written authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after seventy-two hours beginning with the time the authorisation was granted.

64. Paragraph 5.13 provides that at any time before a directed surveillance authorisation (other than one granted by a member of the intelligence services) would cease to have effect, the authorising officer may renew it in writing for a period of three months if he or she considers it necessary for the authorisation to continue for the purpose for which it was given. Renewals may also be granted orally in urgent cases and last for a period of seventy-two hours. The renewal will take effect at the time at which the authorisation would have ceased to have effect but for the renewal.

65. According to paragraph 5.15 of the Revised Code all applications for the renewal of a directed surveillance authorisation should record, either at the time of authorisation or, in the case of urgent cases renewed orally, when reasonably practicable: whether it is the first renewal or every occasion on which renewal was previously authorised; any significant changes to the information in the initial application; the reasons why the authorisation should continue; the content and value to the investigation or operation of the information so far obtained by the surveillance; and the results of regular reviews of the investigation or operation.

β. Intrusive surveillance

66. Paragraph 6.23 of the Revised Code provides that a written authorisation granted by the Secretary of State, a senior authorising officer or a designated deputy will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect.

Oral authorisations given in urgent cases by the Secretary of State, a senior authorising officer or designated deputy, and written authorisations given by those entitled to act in urgent cases, will cease to have effect (unless renewed) at the end of the period of seventy-two hours beginning with the time when they took effect.

67. If, at any time before the authorisation expires, the senior authorising officer or, in his absence, the designated deputy considers that the authorisation should continue to have effect for the purpose for which it was issued, paragraph 6.27 of the Revised Code permits him to renew it in writing for a further period of three months. As with the initial authorisation, paragraph 6.28 requires the senior authorising officer to seek the approval of a Surveillance Commissioner. The renewal will not take effect until the notice of the Surveillance Commissioner's approval has been received in the office of the person who granted the authorisation within the relevant force or organisation (but not before the day on which the authorisation would otherwise have ceased to have effect). In urgent cases, paragraph 6.29 permits a renewal to take effect immediately, provided that this is not before the day on which the authorisation would otherwise have ceased to have effect.

68. Pursuant to paragraph 6.30, all applications for a renewal of an intrusive surveillance should record whether it is the first renewal or every occasion on which the authorisation was previously renewed; any significant changes to the information provided in the original application; the reason why it is necessary to continue with intrusive surveillance; the content and value to the investigation or operation of the product so far obtained by the authorisation; and the results of any reviews of the investigation or operation.

e. Cancellation of authorisation

α. Directed surveillance

69. Paragraph 5.17 of the Revised Code provides that during a review, the authorising officer who granted or last renewed the authorisation may amend specific aspects of the authorisation. He or she must cancel an authorisation if satisfied that the directed surveillance as a whole no longer meets the criteria upon which it was authorised. According to paragraph 5.18, as soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject. The date that the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained.

β. Intrusive surveillance

70. According to paragraph 6.32, the senior authorising officer who granted or last renewed the authorisation must cancel it if he is satisfied that the surveillance no longer meets the criteria upon which it was authorised. Paragraph 6.33 further provides that as soon as the decision is taken that intrusive surveillance should be discontinued, the instruction must be given to those involved to stop the intrusive surveillance. The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained. Following cancellation of any intrusive surveillance, other than one granted by the Secretary of State, paragraph 6.34 requires that the Surveillance Commissioners be notified of the cancellation.

71. Where a police authorisation is quashed or cancelled by a Surveillance Commissioner, paragraph 6.35 requires that the senior authorising officer immediately instruct those involved to stop carrying out the intrusive surveillance.

f. Handling, use and destruction of material

72. Chapter 9 of the Revised Code provides, as relevant:

"**Use of material as evidence**

9.1 Subject to the provisions in chapter 4 of this Code, material obtained through directed or intrusive surveillance, or entry on, or interference with, property or wireless telegraphy, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

9.2 Any decisions by a Surveillance Commissioner in respect of granting prior approval for intrusive surveillance activity or entry on, or interference with, property or with wireless telegraphy, shall not be subject to appeal or be liable to be questioned in any court.

Retention and destruction of material

9.3 Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance or property interference. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

9.4 Where the product of surveillance or interference with property or wireless telegraphy could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

9.5 There is nothing in the 2000 Act, 1994 Act or 1997 Act which prevents material obtained under directed or intrusive surveillance or property interference authorisations from being used to further other investigations.

Law enforcement agencies

9.6 In the cases of the law enforcement agencies, particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained."

g. Records

73. Paragraphs 8.1 and 8.2 of the Revised Code provide:

"A record of the following information pertaining to all authorisations shall be centrally retrievable within each public authority for a period of at least three years from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request.

- the type of authorisation;
- the date the authorisation was given;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled.

The following documentation should also be centrally retrievable for at least three years from the ending of each authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction to cease surveillance was given;

- the date and time when any other instruction was given by the authorising officer."

h. Special rules on communications subject to legal privilege

74. Paragraph 2.18 of the Revised Code provides that:

"The 2010 Order provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in Article 3(2) of the Order as is, at any time during the surveillance, used for the purpose of legal consultations shall be treated for the purposes of Part II of the 2000 Act as intrusive surveillance. The premises identified in article 3(2) are:

(a) any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;

(b) any place in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Border Act 2007;

(c) police stations;

(d) hospitals where high security psychiatric services are provided;

(e) the place of business of any professional legal adviser; and

(f) any place used for the sittings and business of any court, tribunal, inquest or inquiry."

75. Chapter 4, which was added to the Revised Code following the judgment of the House of Lords in *Re McE*, provides further guidance in respect of legally privileged and confidential information:

"**Overview**

4.1 The 2000 Act does not provide any special protection for 'confidential information', although the 1997 Act makes special provision for certain categories of confidential information. Nevertheless, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of communications subject to legal privilege, communications between a Member of Parliament and another person on constituency matters, confidential personal information, or confidential journalistic material. So, for example, extra care should be taken where, through the use of surveillance, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual welfare, or between a Member of Parliament and a constituent relating to constituency matters, or wherever matters of medical or journalistic confidentiality or legal privilege may be involved. References to a Member of Parliament include references to Members of both Houses of the UK Parliament, the European Parliament, the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

4.2 Authorisations under the 1997 Act likely to result in the acquisition of knowledge of matters subject to legal privilege, confidential personal information or confidential journalistic material require (other than in urgent cases) the approval of a Surveillance Commissioner.

4.3 Authorisations for directed surveillance of legal consultations falling within the 2010 Order must comply with the enhanced authorisation regime described below. In cases where it is likely that knowledge of confidential information will be acquired, the use of covert surveillance is subject to a higher level of authorisation eg a Chief Officer. Annex A lists the authorising officer for each public authority permitted to authorise such surveillance.

Material subject to legal privilege: introduction

4.4 Covert surveillance likely or intended to result in the acquisition of knowledge of matters subject to legal privilege may take place in circumstances covered by the 2010 Order, or in other circumstances. Similarly, property interference may be necessary in order to effect surveillance described in the 2010 Order, or in other circumstances where knowledge of matters subject to legal privilege is likely to be obtained.

4.5 The 2010 Order provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified in article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of 'legal consultations' shall be treated for the purposes of Part II of the 2000 Act as intrusive surveillance.

4.6 The 2010 Order defines 'legal consultation' for these purposes. It means:

(a) a consultation between a professional legal adviser and his client or any person representing his client, or

(b) a consultation between a professional legal adviser or his client or any such representative and a medical practitioner made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

4.7 The definition of 'legal consultation' in the 2010 Order does not distinguish between legal consultations which are legally privileged, wholly or in part, and legal consultations which may be in furtherance of a criminal purpose are therefore not protected by legal privilege. Covert surveillance of all legal consultations covered by the 2010 Order (whether protected by legal privilege or not) is to be treated as intrusive surveillance.

4.8 'Legal privilege' is defined in section 98 of the 1997 Act. This definition should be used to determine how to handle material obtained through surveillance authorised under RIPA, including through surveillance which is treated as intrusive surveillance as a result of the 2010 Order. As discussed below, special safeguards apply to matters subject to legal privilege.

4.9 Under the definition in the 1997 Act, legal privilege does not apply to communications or items held, or oral communications made, with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications or items will lose their protection for these other purposes if the professional legal adviser intends to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. Tests to be applied when authorising or approving covert surveillance or property interference likely or intended to result in the acquisition of knowledge of matters subject to legal privilege

4.10 All applications for covert surveillance or property interference that may result in the acquisition of knowledge of matters subject to legal privilege should state whether the covert surveillance or property interference is intended to obtain

knowledge of matters subject to legal privilege as defined by section 98 of the 1997 Act.

4.11 If the covert surveillance or property interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it. If the risk cannot be removed entirely, the application should explain what steps will be taken to ensure that any knowledge of matters subject to legal privilege which is obtained is not used in law enforcement investigations or criminal prosecutions.

4.12 Where covert surveillance or property interference is likely or intended to result in the acquisition of knowledge of matters subject to legal privilege, an authorisation shall only be granted or approved if the authorising officer, Secretary of State or approving Surveillance Commissioner, as appropriate, is satisfied that there are exceptional and compelling circumstances that make the authorisation necessary:

- Where the surveillance or property interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege, such exceptional and compelling circumstances may arise in the interests of national security or the economic well-being of the UK, or for the purpose of preventing or detecting serious crime;
- Where the surveillance or property interference is intended to result in the acquisition of knowledge of matters subject to legal privilege, such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb, or to national security, and the surveillance or property interference is reasonably regarded as likely to yield intelligence necessary to counter the threat.

4.13 Further, in considering any authorisation for covert surveillance or property interference likely or intended to result in the acquisition of knowledge of matters subject to legal privilege, the authorising officer, Secretary of State or approving Surveillance Commissioner, as appropriate, must be satisfied that the proposed covert surveillance or property interference is proportionate to what is sought to be achieved. In relation to intrusive surveillance, including surveillance to be treated as intrusive as a result of the 2010 Order, section 32(4) will apply.

4.14 Directed surveillance likely to result in the acquisition of knowledge of matters subject to legal privilege may be authorised only by authorising officers entitled to grant authorisations in respect of confidential information. Intrusive surveillance, including surveillance which is treated as intrusive by virtue of the 2010 Order, or property interference likely to result in the acquisition of material subject to legal privilege may only be authorised by authorising officers entitled to grant intrusive surveillance or property interference authorisations.

4.15 Property interference likely to result in the acquisition of such material is subject to prior approval by a Surveillance Commissioner (unless the Secretary of State is the relevant authorising officer or the case is urgent). Intrusive surveillance, including surveillance which is treated as intrusive by virtue of the 2010 Order, is subject to prior approval by a Surveillance Commissioner (unless the Secretary of State is the relevant authorising officer or the case is urgent).

Surveillance under the 2010 Order

4.16 As noted above, the 2010 Order provides that directed surveillance that is carried out in relation to anything taking place on so much of any premises specified

in article 3(2) of the Order as is, at any time during the surveillance, used for the purposes of 'legal consultations' shall be treated for the purposes of Part II of the 2000 Act as intrusive surveillance.

4.17 As a result of the 2010 Order, such surveillance cannot be undertaken without the prior approval of a Surveillance Commissioner (with the exception of urgent authorisations or authorisations granted by the Secretary of State).

4.18 The locations specified in the Order are:

(a) any place in which persons who are serving sentences of imprisonment or detention, remanded in custody or committed in custody for trial or sentence may be detained;

(b) any place in which persons may be detained under paragraph 16(1), (1A) or (2) of Schedule 2 or paragraph 2(2) or (3) of Schedule 3 to the Immigration Act 1971 or section 36(1) of the UK Border Act 2007;

(c) any place in which persons may be detained under Part VI of the Criminal Procedure (Scotland) Act 1995, the Mental Health (Care and Treatment) (Scotland) Act 2003 or the Mental Health Act 1983;

(d) police stations;

(e) the place of business of any professional legal adviser;

(f) any place used for the sittings and business of any court, tribunal, inquest or inquiry.

4.19 With the exception of urgent applications and authorisations granted by the Secretary of State, authorisations for surveillance which is to be treated as intrusive surveillance as a result of the 2010 Order shall not take effect until such time as:

(a) the authorisation has been approved by a Surveillance Commissioner; and

b) written notice of the Commissioner's decision to approve the authorisation has been given to the authorising officer.

4.20 If an authorisation is to be granted by the Secretary of State, the provisions in Chapter 6 apply.

Property interference under the 1997 Act likely to result in the acquisition of knowledge of matters subject to legal privilege

4.21 With the exception of urgent authorisations, where it is believed that the action authorised is likely to result in the acquisition of knowledge of matters subject to legal privilege an authorisation under the 1997 Act shall not take effect until such time as:

(a) the authorisation has been approved by a Surveillance Commissioner; and

b) written notice of the Commissioner's decision to approve the authorisation has been given to the authorising officer.

The use and handling of matters subject to legal privilege

4.22 Matters subject to legal privilege are particularly sensitive and surveillance which acquires such material may give rise to issues under Article 6 of the ECHR (right to a fair trial) as well as engaging Article 8.

4.23 Where public authorities deliberately acquire knowledge of matters subject to legal privilege, they may use that knowledge to counter the threat which led them to acquire it, but it will not be admissible in court. Public authorities should ensure that

knowledge of matters subject to legal privilege, whether or not it is acquired deliberately, is kept separate from law enforcement investigations or criminal prosecutions.

4.24 In cases likely to result in the acquisition of knowledge of matters subject to legal privilege, the authorising officer or Surveillance Commissioner may require regular reporting so as to be able to decide whether the authorisation should continue. In those cases where legally privileged material has been acquired and retained, the matter should be reported to the authorising officer by means of a review and to the relevant Commissioner or Inspector during his next inspection (at which the material should be made available if requested).

4.25 A substantial proportion of the communications between a lawyer and his client(s) may be subject to legal privilege. Therefore, in any case where a lawyer is the subject of an investigation or operation, authorising officers should consider whether the special safeguards outlined in this chapter apply. Any material which has been retained from any such investigation or operation should be notified to the relevant Commissioner or Inspector during his next inspection and made available on request.

4.26 Where there is any doubt as to the handling and dissemination of knowledge of matters which may be subject to legal privilege, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the information takes place. Similar advice should also be sought where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception. The retention of legally privileged material, or its dissemination to an outside body, should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates. Any dissemination of legally privileged material to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

Confidential information

4.27 Special consideration must also be given to authorisations that involve confidential personal information, confidential constituent information and confidential journalistic material. Where such material has been acquired and retained, the matter should be reported to the relevant Commissioner or Inspector during his next inspection and the material be made available to him if requested.

4.28 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples include consultations between a health professional and a patient, or information from a patient's medical records.

4.29 Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. Again, such information is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

4.30 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

4.31 Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from a legal adviser within the relevant public authority before any further dissemination of the material takes place."

i. Surveillance Commissioners

76. Section 91(2) of the Police Act 1997 ("the 1997 Act") provides that the ordinary Surveillance Commissioners and the Chief Surveillance Commissioner must hold or have held high judicial office. They are appointed for fixed terms of three years and they enjoy statutory protection from arbitrary removal from office.

77. Section 62(1) of RIPA requires the Chief Surveillance Commissioner to keep under review the exercise and performance of the powers and duties conferred by Part II of the Act. He may be assisted in the performance of his duties by Assistant Surveillance Commissioners.

78. The ordinary Surveillance Commissioners have power to quash authorisations and to order the destruction of any records relating to information obtained by the authorised conduct (section 37(1) – (5) of RIPA).

j. The Investigatory Powers Tribunal

79. The Investigatory Powers Tribunal ("IPT") was established under section 65(1) of RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by RIPA. Members of the IPT must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing. Any person may bring a claim before the IPT and, save for vexatious or frivolous applications, the IPT must determine all claims brought before it (sections 67(1), (4) and (5) RIPA).

80. Section 65(2) of RIPA provides that the IPT is the only appropriate forum in relation to proceedings for acts incompatible with Convention rights which are proceedings against any of the intelligence services and complaints by persons who allege to have been subject to the investigatory powers of RIPA. It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception. Sections 67(2) and 67(3)(c) provide that the IPT is to apply the principles applicable by a court on an application for judicial review.

81. Under section 67(8) of RIPA, there is no appeal from a decision of the IPT "except to such extent as the Secretary of State may by order otherwise provide". No order has been passed by the Secretary of State.

82. Under section 68(2), the IPT has the power to require a relevant Commissioner to provide it with all such assistance (including the Commissioner's opinion as to any issue falling to be determined by the IPT) as it thinks fit.

83. Section 68(4) deals with reasons for the IPT's decisions and provides that:

> "Where the Tribunal determine any proceedings, complaint or reference brought before or made to them, they shall give notice to the complainant which (subject to any rules made by virtue of section 69(2)(i)) shall be confined, as the case may be, to either—
>
> (a) a statement that they have made a determination in his favour; or
>
> (b) a statement that no determination has been made in his favour."

84. The IPT has the power to award compensation and to make such other orders as it thinks fit, including orders quashing or cancelling any warrant or authorisation and requiring the destruction of any records obtained (section 67(7) RIPA). In the event that a claim before the IPT is successful, the IPT is generally required to make a report to the Prime Minister (section 68(5)).

C. Police Service of Northern Ireland Service Procedure, "Covert Surveillance of Legal Consultations and the Handling of Legally Privileged Material"

85. The Service Procedure was issued and implemented on 22 June 2010. Its aim is to set out the position of the PSNI regarding the steps to be taken in relation to any material which is obtained by virtue of the covert surveillance of legal consultations.

86. Section 6 of the Service Procedure echoes the Revised Code in making clear that deliberately acquired knowledge of legally privileged matters cannot be admitted in court and is to be kept separate from law enforcement investigations and criminal prosecutions.

87. The section further provides guidance on the retention, destruction and handling of material subject to legal privilege. In particular, it provides that legally privileged material must clearly be marked as such and dissemination should be limited to authorised persons; the material should be handled in a manner consistent with the procedures set out for the storage and handling of classified material; legally privileged material that is deliberately acquired will only be disseminated for the purpose of countering the identified threat; legally privileged material that is acquired and is not deemed relevant must not be copied or disseminated; the master and working copy must be sealed and securely stored; material subject to legal privilege must not be used to further other investigations unless explicitly approved within the authorisation or any review; the copying and

handling of any material must be fully audited; material subject to legal privilege will not be recorded on the PSNI intelligence databases; dissemination to an outside body will only be considered when it is necessary and material so disseminated will retain any additional handling conditions which must be notified to that body as a condition of dissemination; any PSNI employee given access to the information will be required to sign to confirm that they will not disclose the material other than in accordance with the Dissemination Policy; material subject to legal privilege will only be retained as long as necessary to counter the threat in respect of which it was obtained or to comply with other statutory obligations; where any such obligations have been discharged the senior authorising officer will direct that the material be destroyed and disposal should be witnessed by a legal advisor; and, finally, a legal advisor will be consulted on all aspects of the acquisition, retention, handling, dissemination and disposal of legally privileged material.

D. The July 2005 Criminal Procedure and Investigations Act 1996 Code of Practice for Northern Ireland ("the CIPA Code")

88. The CIPA Code sets out the manner in which police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation which may be relevant to the investigation. Insofar as intrusive surveillance by the PSNI results in the acquisition of material that was not legally privileged, its retention and potential use or disclosure in any subsequent criminal proceedings is governed by CIPA.

E. The Data Protection Act 1998 ("DPA")

89. Material obtained as a result of intrusive surveillance of legal consultations will generally be "personal data" for the purposes of the DPA and in certain circumstances may amount to "sensitive personal data". Moreover, the PSNI is a "data controller" for the purposes of that Act. Therefore, the PSNI must in general comply with the data protection principles set out in Part I of Schedule 1.

90. As read with paragraph 5 of Schedule 2 to the DPA, the first data protection principle permits the PSNI to process personal data insofar as it is "necessary" for the exercise of any of its public functions. More restrictive conditions apply in respect of sensitive personal data.

91. Pursuant to the fifth personal data principle, personal data should be destroyed as soon as it is no longer necessary for the PSNI to retain it for the purpose for which it was being processed.

92. The Information Commissioner, an independent regulator, oversees compliance with the DPA by data controllers. He has the power to impose a

fine of up to GBP 500,000 in the event of serious contravention of the data protection principles by a data controller.

F. Guidance relating to "appropriate adults"

93. The Police and Criminal Evidence Act 1984 Code of practice in connection with the detention, treatment and questioning by police officers of persons under section 41 of, and Schedule 8 to, the Terrorism Act 2000 sets out the circumstances in which an appropriate adult should be appointed.

94. Pursuant to paragraph 11.9 of the Code, a juvenile or person who is mentally disordered or otherwise mentally vulnerable should not be interviewed regarding their involvement or suspected involvement in a criminal offence or offences, or asked to provide or sign a written statement under caution or record of interview, in the absence of the appropriate adult.

95. According to paragraph 1.13, an appropriate adult could be a relative or guardian, or a person experienced in dealing with mentally disordered or mentally vulnerable people.

96. Paragraph 3.17 provides that the appropriate adult must be informed by police "as soon as practicable" of the arrest and detention of the mentally disordered or mentally vulnerable person and the adult must be asked to come to the police station. Paragraph 3.19 further provides that the detainee should be advised that the duties of the appropriate adult "include giving advice and assistance" and that they can "consult privately... at any time".

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

97. The applicant complained that the regime for covert surveillance of consultations between detainees and their lawyers, medical personnel, and appropriate adults was in breach of Article 8 of the Convention, which reads as follows:

> "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."

98. The Government contested that argument.

99. Following receipt of the Government's observations, the applicant accepted that he did not consult with any medical personnel until 7 May 2010, by which time the High Court had directed that consultations with his solicitor and his medical advisor should not be subject to covert surveillance (see paragraphs 20 – 21 above). He therefore accepted that he could not have suffered any interference with his Article 8 rights in this regard.

A. Lawyer/client consultations

1. Admissibility

100. The Court is satisfied that this complaint raises complex issues of fact and law, such that it cannot be rejected as manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further considers that the complaint is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

a. The parties' submissions

α. The applicant

101. The applicant argued that Article 8 was clearly engaged by the covert surveillance of consultations with his legal advisor. Although he accepted that the purposes identified in the legislation permitting covert surveillance amounted to a legitimate aim, he maintained that the relevant legal framework failed both the "quality of law" and "necessity" tests under paragraph 2 of Article 8 of the Convention.

102. The applicant submitted that the combined effect of Part II of RIPA, the Revised Code and the PSNI Service Procedure did not provide, in relation to covert surveillance of lawyer/client consultations, the "adequate and effective guarantees against abuse" required by Article 8 of the Convention, especially when compared with the clear and precise statutory guidelines outlined in Part I of RIPA in respect of the interception of communications (see *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010).

103. Unlike Part I of RIPA, Part II, read together with the Revised Code, did not indicate with sufficient clarity the test for authorising covert surveillance of lawyer-client consultations; in particular, paragraph 4.12 of the Revised Code only provided examples of when surveillance intended to result in the acquisition of legally privileged material would be permitted, for example "where there is a threat to life or limb, or to national security". In any case, the applicant argued that in view of the importance and sensitivity of the issue, any "threat to life or limb" should have to be "real or immediate".

104. Moreover, the procedures for the handling, dissemination and destruction of legally privileged material were not sufficiently precise and did not satisfy the minimum safeguards identified by the Court in *Valenzuela Contreras v. Spain*, 30 July 1998, *Reports of Judgments and Decisions* 1998-V. Although the applicant acknowledged that *Valenzuela Contreras* was an "interception case", he argued that the principles derived from the Court's "interception" case-law could be "read across" to the present case because, first, the Court had not drawn a distinction between the principles which applied in interception cases and covert-surveillance cases; secondly, it was the nature and degree of intrusion in certain types of covert surveillance cases which allowed the Court to "read across" from the principles set out in interception cases; thirdly, any distinction was therefore not appropriate when dealing with covert surveillance of the kind in issue in the present case; and finally, given that both types of case involved the handling of material obtained as a result of listening to and recording private conversations, it was difficult to see what valid distinction could be made between an interception operation and a covert-surveillance operation of the kind at issue in the present case.

105. The applicant pointed to paragraph 9.3 of the Revised Code, which provided that each public authority had to ensure that arrangements were in place for the secure handling and destruction of material obtained through directed or intrusive surveillance. This was the function of the PSNI Service Procedure, which went much further than the Code in providing for limits on dissemination, storage, access, retention and destruction. However, it was not in force at the relevant time and, in any case, the applicant contended that such important matters should not be left to the discretion of the individual public authorities.

106. The applicant acknowledged the existence of the July 2005 Criminal Procedure and Investigations Act 1996 Code of Practice for Northern Ireland ("the CIPA Code"), which set out the manner in which police officers were to record, retain and reveal to the prosecutor material obtained in a criminal investigation which may be relevant to the investigation. However, he submitted that the different legislative schemes taken together did not present a clear picture or provide sufficient clarity to enable an individual to be able to ascertain the arrangements for handling any material obtained as a result of covert surveillance of his legal consultations.

107. Finally, the applicant argued that even if the interference with his Article 8 rights was "in accordance with the law", it was not "necessary in a democratic society". Consultations between a detainee and his legal advisor were particularly sensitive in view of the fundamental rights at stake, and yet the detainee could only avoid covert surveillance by electing not to speak to his lawyer. As such, the legislation had the potential to undermine

some of the basic protections underlying the criminal justice system in the United Kingdom.

β. The Government

108. The Government accepted that the applicant could claim to be a victim of an alleged violation of Article 8 in relation to his legal consultations with his solicitor between 4 May 2010 and 6 May 2010. It also noted that it did not appear to be in dispute that the surveillance pursued a legitimate aim for the purposes of Article 8 § 2 of the Convention.

109. The Government argued that any interference was "in accordance with the law": it had its basis in domestic law; the law in question was accessible as it took the form of primary and secondary legislation and a published Revised Code (the Government accepted that it could not rely on the PSNI Service Procedure in the present case as it was not issued until 22 June 2010); and finally, the law was sufficiently foreseeable.

110. In particular, the law at issue indicated the scope of the PSNI's discretionary power with sufficient clarity, as it afforded citizens an adequate indication of the circumstances in which the PSNI was empowered to authorise intrusive surveillance of legal consultations in police stations. Insofar as the applicant argued that the Revised Code did not satisfy the detailed requirements set out in *Valenzuela-Contreras v. Spain* (because it did not make provision for the destruction of legally privileged material obtained as a result of intrusive surveillance and did not set a test for the circumstances in which retention or onward dissemination could occur), the Government contended that that case concerned interception powers and had not been applied by the Court in cases concerning covert surveillance. Indeed, the Government maintained that in view of the wide range of surveillance powers, and the wide range of circumstances in which they might properly be deployed, it would be inappropriate as a matter of principle to be overly prescriptive as to the specific features that must be present within any surveillance regime.

111. In the Government's submission, the true test was therefore whether the "manner of [the] exercise" of the PSNI's discretionary power to conduct surveillance of legal consultations was indicated in the law with sufficient clarity to give the individual adequate protection against arbitrary interference; and that test was clearly satisfied in the present case. The Revised Code obliged the PSNI to put in place arrangements for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance; if the PSNI obtained legally privileged material through intrusive surveillance of legal consultations, that material had to be kept separate from any criminal investigation or prosecution and handled in accordance with the Revised Code; pursuant to the fifth data protection principle in the Data Protection Act 1998, the retained material would in general need to be destroyed once its retention was no longer

necessary for the purpose for which the PSNI had been processing it; if legally privileged material was disseminated by the PSNI to another body, it had to be accompanied by a clear warning that it was subject to legal privilege, the Surveillance Commissioners would have to be notified during their next inspection and any dissemination would have to be compatible with the Data Protection Act; and finally, insofar as intrusive surveillance by the PSNI resulted in the acquisition of material that was not legally privileged, its retention and potential use or disclosure in any subsequent criminal proceedings was governed by the detailed Criminal Procedure and Investigations Act 1996 Code of Practice.

112. The Government referred to *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 92 – 92, 28 June 2007, which indicated that the Court should consider evidence of the actual operation of the system of surveillance, in particular whether it was working properly or whether it was subject to abuse. In the United Kingdom only one intrusive surveillance order had been granted in the three years since the 2010 Order came into force. It was therefore clear that in practice authorisations were only being granted in highly exceptional cases.

113. In the alternative, the Government argued that if the standards developed in the context of interception of communications ought to be applied in the present case, the above regime satisfied them.

114. The Government further submitted that the regime satisfied the requirement of "necessity". Indeed, the Contracting States enjoyed a wide margin of appreciation in determining the precise conditions under which a system of covert surveillance was to be operated; and in the present case the safeguards offered adequate and effective guarantees against abuse: only the Chief Constable or Deputy Chief Constable could in general grant an authorisation for intrusive surveillance of legal consultations; save in cases of urgency, such authorisation would not take effect unless and until it was approved by a Surveillance Commissioner; even in urgent cases the ordinary Surveillance Commissioners retained the power to quash any order retrospectively and order the destruction of any relevant records; the regime was overseen by the Chief Surveillance Officer, who was independent of the PSNI and had to have held high judicial office; the regime was subject to further judicial oversight in the form of the Investigatory Powers Tribunal, which had jurisdiction to hear complaints by any person regarding the operation of the regime and had power to order appropriate relief; and finally, the Revised Code required that knowledge of matters subject to legal privilege be kept separate from law enforcement investigations or criminal prosecutions.

b. The Court's assessment

α. The existence of an interference

115. Insofar as the applicant's complaints concern the regime for conducting covert surveillance of consultations between detainees and their legal advisors, the Government have accepted that he can claim to be a victim of the alleged violation.

116. In this regard, it is now well-established that an individual may under certain conditions claim to be the victim of a violation occasioned by the mere existence of legislation permitting secret measures without having to demonstrate that such measures were in fact applied to him (*Klass and Others v. Germany*, 6 September 1978, § 34, Series A no. 28).

117. Consequently, the Court will proceed on the basis that there has been an "interference", within the meaning of Article 8 § 2 of the Convention, with the applicant's right to respect for his private life.

β. Was the interference justified?

118. In order to be justified under Article 8 § 2 of the Convention, the interference must be "in accordance with the law", in pursuit of a legitimate aim, and "necessary in a democratic society".

119. In respect of Part I of RIPA the Court considered that the interception regime pursued the legitimate aims of the protection of national security and the prevention of disorder and crime (*Kennedy v. the United Kingdom*, no. 26839/05, § 155, 18 May 2010). The Court considers that the surveillance regime under Part II of RIPA pursues the same legitimate aims and this has not been disputed by the parties. It therefore falls to the Court to consider the remaining two questions: was the regime "in accordance with the law", and was it "necessary" to achieve the legitimate aim pursued?

120. The requirement that any interference must be "in accordance with the law" under Article 8 § 2 will only be met when three conditions are satisfied: the impugned measure must have some basis in domestic law; the domestic law must be compatible with the rule of law and accessible to the person concerned; and the person concerned must be able to foresee the consequences of the domestic law for him (see, among many other authorities, *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000-V, *Liberty and Others v. the United Kingdom*, no. 58243/00, § 59, 1 July 2008, and *Iordachi and Others v. Moldova*, no. 25198/02, § 37, 10 February 2009).

121. In the present case it is not in dispute that the surveillance regime had a basis in domestic law, namely RIPA and the Revised Code of Practice. Moreover, both RIPA and the Revised Code were public documents – like the Interception of Communications Code of Practice, the Revised Code is available on the internet. This being so, the Court accepts

that the relevant domestic law was adequately accessible for the purposes of Article 8 of the Convention.

122. In the special context of secret surveillance measures, the Court has found that "foreseeability" requires that domestic law be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see, for example, the admissibility decision in *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 93, ECHR 2006-XI). This is very similar to – and at times considered together with – the test for deciding whether an interference is "necessary in a democratic society" in pursuit of a legitimate aim; namely, whether the minimum safeguards set out in statute law in order to avoid abuses of power are adequate (see *Klass and Others v.* Germany, cited above, § 50; and *Weber and Saravia v. Germany*, cited above, § 95).

123. In *Valenzuela Contreras v. Spain*, cited above, § 59, an interception-of-communications case, the Court set the standard high, finding that the relevant legislation was not adequately foreseeable because neither the Constitution nor the Code of Criminal Procedure included

> "the conditions regarding the definition of the categories of people liable to have their telephones tapped by judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations and the use and destruction of the recordings made."

124. Similarly, in considering whether an interception of communications was "necessary in a democratic society, in *Weber and Saravia v. Germany*, cited above, § 95 the Court stated:

> "In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig*, cited above, p. 56, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, pp. 1924-25, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003)."

125. Consequently, in *Kennedy v. the United Kingdom*, cited above, § 155 the Court examined in some detail the provisions of both RIPA and the Interception of Communications Code of Practice insofar as they concerned the definition of the categories of people liable to have their telephones tapped by judicial order; the nature of the offences which might give rise to such an order; a limit on the duration of telephone tapping; the provisions on duration, renewal and cancellation of intercept warrants; the procedure for examining, using and storing the data; the general safeguards

which applied to the processing and communication of intercept material; the destruction of intercept material; the keeping of records of intercept warrants; and the supervision of the RIPA regime.

126. However, the Government have argued that in its case-law the Court has distinguished between the minimum safeguards required in interception-of-communication cases and those required in other surveillance cases. As the present case concerns covert surveillance and not the interception of communications, so the Government submitted, the relevant test should be less strict; namely, whether the manner of the exercise of the authorities' discretionary power to conduct surveillance of legal consultations was indicated in the law with sufficient clarity to give the individual adequate protection against arbitrary interference.

127. It is true that the Court has generally only applied the strict criteria in *Valenzuela-Contreras* in the context of interception of communication cases. However, it has suggested that the precision required by the legislation will depend on all the circumstances of the case and, in particular, the level of interference with the individual's rights under Article 8 of the Convention.

128. In *Bykov v. Russia* [GC], no. 4378/02, § 78, 10 March 2009, a case which concerned the recording of a private conversation by way of a radio transmitting device, the Court made it clear that the degree of precision required of the law would depend upon the particular subject-matter of the case. It held that in terms of the nature and degree of the intrusion involved the recording of the conversation in that case was "virtually identical" to telephone tapping and, this being so, it should assess the relevant legislation using the same principles as applied to the interception of communications. Nevertheless, although it cited *Valenzuela-Contreras*, it defined the relevant test as being whether the law was sufficiently clear to give citizens an adequate indication of the circumstances in which and the conditions on which public authorities were empowered to resort to a secret interference with the right to respect for private life and correspondence. It did not refer to the stricter requirements set out in that judgment, although it is arguable that it was not necessary on the facts of that case as the legal discretion of the authorities to order the interception had not been subject to any conditions and the scope and manner of its exercise had not been defined.

129. In *Uzun v. Germany*, no. 35623/05, § 66, ECHR 2010 (extracts) the Court accepted that the monitoring of a car's movements by GPS interfered with the applicant's Article 8 rights. However, it distinguished this kind of surveillance from other methods of visual or acoustic surveillance which were generally more susceptible of interfering with Article 8 rights because they disclosed more information on a person's conduct, opinions or feelings. Therefore, the Court indicated that, while it would not be barred from drawing inspiration from the principles set up and applied in the specific context of surveillance of telecommunications, those principles would not

be directly applicable in a case concerning surveillance of movements in public places via GPS because such a measure "must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations". Instead, the Court applied the more general principles on adequate protection against arbitrary interference with Article 8 rights (see, for example, *Weber and Saravia*, cited above, § 94, and the test applied in *Bykov*, set out at paragraph 128 above).

130. The Court has not, therefore, excluded the application of the principles developed in the context of interception cases in covert-surveillance cases; rather, it has suggested that the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference.

131. The present case concerns the surveillance of legal consultations taking place in a police station, which the Court considers to be analogous to the interception of a telephone call between a lawyer and client. The Court has recognised that, while Article 8 protects the confidentiality of all correspondence between individuals, it will afford "strengthened protection" to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential (*Michaud v. France*, no. 12323/11, § 118, ECHR 2012). The Court therefore considers that the surveillance of a legal consultation constitutes an extremely high degree of intrusion into a person's right to respect for his or her private life and correspondence; higher than the degree of intrusion in *Uzun* and even in *Bykov*. Consequently, in such cases it will expect the same safeguards to be in place to protect individuals from arbitrary interference with their Article 8 rights as it has required in cases concerning the interception of communications, at least insofar as those principles can be applied to the form of surveillance in question.

132. The Court has emphasised that although sufficient detail should be provided of the nature of the offences in question, the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception (see, for example, *Kennedy v. the United Kingdom*, cited above, § 159). In Part II of RIPA, section 32 provides that intrusive surveillance can take place where the Secretary of State or senior authorising officer believes it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom. In this respect it is almost identical to section 5 in Part I of RIPA. Paragraph 4.12 of the Revised Code further clarifies that where the surveillance is likely to result in the acquisition of knowledge of matters subject to legal privilege, it is subject to an enhanced authorisation regime and the circumstances in section 32 will arise only in a very restricted range

of cases, such as where there is a threat to life or limb, or to national security, and the surveillance is reasonably regarded as likely to yield intelligence necessary to counter that threat see paragraph 75 above).

133. In *Kennedy*, the Court accepted that the reference to national security and serious crime in section 5, together with the interpretative clarifications in RIPA, gave citizens an adequate indication as to the circumstances in which and the conditions on which public authorities were empowered to resort to interception. As noted in *Kennedy*, though the term "national security" is not defined in RIPA, it is frequently employed in national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. The terms "serious crime" and "detecting" are defined in the interpretive provisions of RIPA (see paragraphs 57 and 58 above), which apply to both Part I and Part II. In fact, the only discernible difference between the authorisation of the interception of communications provided for in Part I and the authorisation of intrusive surveillance in Part II is that under Part I authorisation is given by the Secretary of State whereas under Part II it may be given by a senior authorising officer (see paragraph 49 above). However, in view of the fact that authorisation by a senior authorising officer generally only takes effect when it has been approved by the Surveillance Commissioner, an independent officer who must have held high judicial office (see paragraph 76 above), the Court does not consider that this fact by itself merits a departure from its conclusions in *Kennedy*. Consequently, the Court considers that, having regard to the provisions of RIPA, the nature of the offences which may give rise to intrusive surveillance is sufficiently clear.

134. RIPA does not provide any limitation on the persons who may be subjected to intrusive surveillance. Indeed, it is clear from section 27(3) that the conduct that may be authorised under Part II includes conduct outside the United Kingdom. However, as indicated in paragraphs 48 – 49 above, the RIPA regime does set out the relevant circumstances which can give rise to intrusive surveillance, which in turn provides guidance as to the categories of person likely in practice to be subject to such surveillance (see also *Kennedy*, cited above, § 160). As already noted, those circumstances are further restricted where the surveillance is intended to result in the acquisition of knowledge of matters subject to legal privilege (see paragraph 75 above).

135. In *Kennedy*, the Court noted that the warrant authorising interception specified the person or premises in respect of which it had been ordered. Although intrusive surveillance is not usually authorised by virtue of a warrant, pursuant to paragraph 6.19 of the Revised Code the application for authorisation must set out the nature of the surveillance; the residential premises or private vehicle in relation to which the surveillance will take place, where known; the identities, where known, of those to be the subject of the surveillance; an explanation of the information which it is desired to

obtain as a result of the surveillance; details of any potential collateral intrusion and why that intrusion is justified; details of any confidential information likely to be obtained as a consequence of the surveillance; the reasons why the surveillance is considered proportionate to what it seeks to achieve; and a record of whether authorisation was given and refused, by whom, and the time and date when this happened (see paragraph 48 above). The senior authorising officer may only grant authorisation if he considers it necessary and proportionate, and, unless it is an urgent case, this decision is subject to further scrutiny by a Surveillance Commissioner before the authorisation takes effect (see paragraph 56 above).

136. Bearing in mind the fact that intrusive surveillance under Part II of RIPA concerns the covert surveillance of anything taking place on residential premises or in private vehicles by a person or listening device, the Court accepts that it will not necessarily be possible to know in advance either on what premises the surveillance will take place or what individuals will be affected by it. However, Part II requires the application to set out in full the information that is known, and the proportionality of the measure will subsequently be scrutinised at two separate levels (by the senior authorising officer and by the Surveillance Commissioner). In the circumstances, the Court considers that no further clarification of the categories of persons liable to be subject to secret surveillance can reasonably be required.

137. With regard to the duration of intrusive surveillance, unless renewed a written authorisation will cease to have effect after three months from the time it took effect (see paragraph 66 above). The senior authorising officer or designated deputy may grant a renewal for a period of three months if it is considered necessary for the authorisation to continue for the purpose for which it was issued; however, except in urgent cases the authorisation will only take effect once it has been approved by a Surveillance Commissioner (see paragraph 67 above). Applications for renewal must record whether it is the first renewal or every occasion on which the authorisation was previously renewed; any significant changes to the information contained in the original application; the reason why it is necessary to continue with intrusive surveillance; the content and value to the investigation or operation of the product so far obtained by the authorisation; and the results of any reviews of the investigation or operation. Furthermore, regular reviews of all authorisations must be undertaken and the senior authorising officer who granted or last renewed an authorisation must cancel it if he or she is satisfied that it no longer meets the criteria upon which it was authorised (see paragraph 68 above). The Court therefore considers that the provisions of Part II of RIPA and the Revised Code which deal with duration, renewal and cancellation are sufficiently clear.

138. In contrast, fewer details concerning the procedures to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which recordings may or must be erased or the tapes destroyed are provided in Part II of RIPA and/or the Revised Code. Although material obtained by directed or intrusive surveillance can normally be used in criminal proceedings and law enforcement investigations, paragraph 4.23 of the Revised Code makes it clear that material subject to legal privilege which has been deliberately acquired cannot be so used (see paragraph 75 above). Certain other safeguards are included in Chapter 4 of the Revised Code with regard to the retention and dissemination of material subject to legal privilege (see paragraph 75 above). Paragraph 4.25 of the Revised Code provides that where legally privileged material has been acquired and retained, the matter should be reported to the authorising officer by means of a review and to the relevant Commissioner or Inspector during his next inspection. The material should be made available during the inspection if requested. Furthermore, where there is any doubt as to the handling and dissemination of knowledge of matters which may be subject to legal privilege, Paragraph 4.26 of the Revised Code states that advice should be sought from a legal advisor before any further dissemination takes place; the retention or dissemination of legally privileged material should be accompanied by a clear warning that it is subject to legal privilege; it should be safeguarded by taking "reasonable steps" to ensure there is no possibility of it becoming available, or it contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings; and finally, any dissemination to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

139. These provisions, although containing some significant safeguards to protect the interests of persons affected by the surveillance of legal consultations, are to be contrasted with the more detailed provisions in Part I of RIPA and the Interception of Communications Code of Practice, which the Court approved in *Kennedy* (cited above, §§ 42 – 49). In particular, in relation to intercepted material there are provisions in Part I and the Code of Practice limiting the number of persons to whom the material is made available and restricting the extent to which it is disclosed and copied; imposing a broad duty on those involved in interception to keep everything in the intercepted material secret; prohibiting disclosure to persons who do not hold the necessary security clearance and to persons who do not "need to know" about the material; criminalising the disclosure of intercept material with an offence punishable by up to five years' imprisonment; requiring intercepted material to be stored securely; and requiring that intercepted material be securely destroyed as soon as it is no longer required for any of the authorised purposes.

140. Paragraph 9.3 of the Revised Code does provide that each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through directed or intrusive surveillance. In the present case the relevant arrangements are contained in the PSNI Service Procedure on Covert Surveillance of Legal Consultations and the Handling of Legally Privileged Material. The Administrative Court accepted that taking together the 2010 Order, the Revised Code and the PSNI Service Procedure Implementing Code, the arrangements in place for the use, retention and destruction of retained material in the context of legal consultations was compliant with the Article 8 rights of persons in custody. However, the Service Procedure was only implemented on 22 June 2010. It was therefore not in force during the applicant's detention in May 2010.

141. The Court has noted the statement of the Government in their observations that only one intrusive surveillance order had been granted up till then in the three years since the 2010 Order (introducing the Revised Code) had come into force in April 2010 (see paragraphs 11 and 12 above). Nevertheless, in the absence of the "arrangements" anticipated by the covert surveillance regime, the Court, sharing the concerns of Lord Phillips and Lord Neuberger in the House of Lords in this regard (see paragraphs 36 – 37 above) is not satisfied that the provisions in Part II of RIPA and the Revised Code concerning the examination, use and storage of the material obtained, the precautions to be taken when communicating the material to other parties, and the circumstances in which recordings may or must be erased or the material destroyed provide sufficient safeguards for the protection of the material obtained by covert surveillance.

142. Consequently, the Court considers that, to this extent, during the relevant period of the applicant's detention (4 – 6 May 2010 – see paragraphs 18 – 20 above), the impugned surveillance measures, insofar as they may have been applied to him, did not meet the requirements of Article 8 § 2 of the Convention as elucidated in the Court's case-law.

143. There has therefore been a breach of Article 8 of the Convention.

B. Consultations between a detainee who is a "vulnerable person" and an appropriate adult

1. Admissibility

144. The Court is satisfied that this complaint raises complex issues of fact and law, such that it cannot be rejected as manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further considers that the complaint is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

a. The parties' submissions

α. The applicant

145. The applicant contended that the regime covering covert surveillance between a detainee who was a "vulnerable person" within the meaning of the Code of Practice and an "appropriate adult" (see paragraph 13 above) was not "in accordance with the law" as required by paragraph 2 of Article 8 of the Convention. In particular, he submitted that even though these consultations were not protected by legal professional privilege, in view of the vulnerability of the detainee they should be as frank as possible. As such, they were analogous to consultations with legal and medical advisors and their covert surveillance should also have been treated as intrusive – rather than directed – surveillance.

146. On account of being treated as directed surveillance, the present regime allowed for surveillance where it was necessary for one of six purposes set out in section 28(3) of RIPA, including for the purpose of assessing any tax, duty, or levy, and the authorisation was proportionate to what was sought to be achieved; the authorisation could be made by a large number of public authorities; the authorisation did not have to be made by officers at a very senior level within those authorities (a Superintendent within the PSNI); and there was no requirement for prior or subsequent supervision or scrutiny of the individual authorisation by a Surveillance Commissioner or any other independent person or body.

147. The applicant further argued that section 28(6) identified a broad range of circumstances in which covert surveillance of consultations with an appropriate adult could take place, and those circumstances were ill-defined in the legislation; the statutory scheme entitled an extensive number of public authorities to engage in such surveillance and therefore reduced the level of foreseeability in terms of an individual being able to regulate their conduct; the number of individuals within those public authorities who could authorise the use of directed surveillance was not narrowly circumscribed; there were no meaningful limitations on the circumstances in which such material could be deployed; and there was a significant absence of any limits in relation to the retention, storage, transmission, dissemination and destruction of such material.

148. The applicant also submitted that the aims identified under section 28(3) of RIPA were not "legitimate"; this was particularly the case in respect of the aim of furthering the collection of taxes, levies and other duties.

149. Finally, and in any case, the applicant contended that the regime in respect of the covert surveillance of the detainee's consultation with an appropriate adult did not satisfy the test of "necessity" in Article 8 § 2 of the

Convention. In particular, there was no reason why the authorisation of such surveillance could not be carried out by an independent person with a judicial background.

B The Government

150. The Government accepted that the applicant could claim to be a victim of an alleged violation of Article 8 of the Convention in relation to his consultations with his appropriate adult from 4 May 2010 to 8 May 2010 (consultations with the appropriate adult were not affected by the court's direction on 6 May 2010 that the applicant's consultations with his solicitor and medical advisor should not be subject to surveillance).

151. The Government argued that the surveillance of consultations between a detainee and an appropriate adult pursued a legitimate aim. The applicant had only sought an assurance from the PSNI that his consultations would not be subject to covert surveillance. He could therefore only complain about potential surveillance by the PSNI and that body was not permitted to conduct such surveillance to further the collection of taxes, levies or other duties.

152. Furthermore, the Government submitted that the interference with the applicant's Article 8 rights was similarly justified. There was no close analogy between the meetings with an appropriate adult and consultations with doctors or solicitors, the latter two being subject to legal privilege. This was the reason why consultations with doctors and solicitors were brought within the intrusive surveillance regime and made subject to a test of exceptionality. Appropriate adults, however, were not lawyers and their function was not to provide legal advice or to assist in the preparation of a criminal defence.

153. In any case, the Government argued that the directed surveillance regime contained adequate safeguards against abuse: the PSNI's use of directed surveillance powers was subject to oversight by the Chief Surveillance Commissioner; any individual could complain to the IPT if he was concerned that he might have been subject to directed surveillance and the IPT had the power to grant appropriate relief if any such complaint was found to have substance; and, if criminal proceedings followed, under the court's abuse of process jurisdiction any relevant use of directed surveillance would be subject to further control by the trial judge, both in relation to admissibility of material obtained thereby and in the event of any allegation of abuse or unlawfulness.

b. The Court's assessment

α. The existence of an interference

154. Insofar as the applicant complains about the regime for conducting covert surveillance of consultations between detainees and their appropriate

adults, the Government have accepted that he can claim to be a victim of the alleged violation.

155. For the reasons set out in paragraphs 115 – 117 above, the Court would agree that there has been an "interference", within the meaning of Article 8 § 2 of the Convention, with the applicant's right to respect for his private life.

β. Was the interference justified?

156. The Court has already noted that in order to be justified under Article 8 § 2 of the Convention the interference must be "in accordance with the law", in pursuit of a legitimate aim, and "necessary" in a democratic society.

157. As with the regime for surveillance of lawyer/client consultations, the Court considers that the regime in question pursues the legitimate aims of protection of national security and the prevention of disorder and crime (see paragraph 119 above). Furthermore, for the reasons set out at paragraph 121 above, the Court finds that the regime had a basis in domestic law, namely Part II of RIPA and the Revised Code of Practice, and that that law was sufficiently accessible. It therefore falls to the Court to decide if the law was adequately foreseeable and whether the interference was "necessary in a democratic society". As the lawfulness of the interference is closely related to the question of its "necessity", the Court will jointly address the foreseeability and the "necessity" requirements (see also *Kennedy*, cited above, § 155).

158. The Court has indicated at paragraph 130 above that the subject-matter of the surveillance and the degree of intrusion will determine the degree of precision with which the law must indicate the circumstances in which and the conditions on which the public authorities are entitled to resort to covert measures. The surveillance of consultations between a vulnerable detainee and an appropriate adult, appointed to assist him or her following an arrest, undoubtedly constitutes a significant degree of intrusion. As such, the present case is distinguishable from that of *Uzun*, cited above, which concerned the monitoring of a car's movements by GPS and, as a consequence, the collection and storage of data determining the applicant's whereabouts and movements in the public sphere.

159. That being said, the surveillance was not taking place in a private place, such as a private residence or vehicle. Rather, it was being conducted in a police station. Moreover, unlike legal consultations, consultations with an appropriate adult are not subject to legal privilege and do not attract the "strengthened protection" accorded to consultations with lawyers or medical personnel. The detainee would not, therefore, have the same expectation of privacy that he or she would have during a legal consultation. Consequently, the Court does not consider it appropriate to apply the strict standard set down in *Valenzuela-Contreras* and will instead focus on the more general

question of whether the legislation adequately protected detainees against arbitrary interference with their Article 8 rights, and whether it was sufficiently clear in its terms to give individuals adequate indication as to the circumstances in which and the conditions on which public authorities were entitled to resort to such covert measures (*Bykov*, cited above, § 76).

160. As it is classified as directed rather than intrusive surveillance, the surveillance of consultations with appropriate adults is permissible in a wider range of circumstances than the surveillance of legal consultations (see paragraph 44 above). In Part II of RIPA, section 28 provides that directed surveillance can take place where the authorising officer (in this case a PSNI officer of the rank of Superintendant or above) believes it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime, in the interests of the economic well-being of the United Kingdom, in the interests of public safety, for the purposes of protecting public health, for the purposes of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, and for any other purpose specified for the purposes of this subsection by an order of the Secretary of State. Nevertheless, the differences are not so great as they might first appear. The PSNI could not authorise the surveillance of a consultation with an appropriate adult for the purposes of assessing or collecting any tax or levy, and the Secretary of State has not specified any other purpose by way of an order. Consequently, consultations with an appropriate adult can only be subject to surveillance on two additional grounds: the interests of public safety, and protecting public health. Like "national security", both terms are frequently employed in national and international legislation and constitute two of the legitimate aims to which Article 8 § 2 refers. Consequently, the Court considers that, having regard to the provisions of RIPA, the nature of the offences which may give rise to intrusive surveillance is sufficiently clear.

161. As with intrusive surveillance, RIPA does not provide any limitation on the persons who may be subjected to directed surveillance. However, paragraph 5.8 of the Revised Code, which sets out the information to be included in an application for directed surveillance, is drafted in identical terms to paragraph 6.19, which concerns intrusive surveillance (see paragraph 41 above), and, similarly, the authorising officer may only authorise directed surveillance if he considers it necessary and proportionate. It is true that fewer safeguards exist than in respect of the surveillance of legal consultations. First, the surveillance is not subject to the enhanced authorisation regime which applies to surveillance intended to result in the obtaining of information subject to legal privilege. Secondly, surveillance carried out by the PSNI may be authorised by a police officer at the level of Superintendent or above, whereas intrusive surveillance may only be authorised by a senior authorising officer, namely the Chief

Constable of the PSNI or the Secretary of State. Thirdly, authorisation does not have to be approved by a Surveillance Commissioner. However, while the Court believes these safeguards to be important in the context of intrusive surveillance, particularly that of legal consultations, in the context of surveillance of consultations with appropriate adults the Court considers that no further clarification of the categories of persons liable to be subject to secret surveillance can reasonably be required.

162. With regard to additional safeguards, the Court notes that authorisations for directed surveillance must be regularly reviewed to assess the need for the surveillance to continue (see paragraph 62 above). During a review, the authorising officer who granted or last renewed the authorisation may amend specific aspects of it. He must cancel the authorisation if satisfied that it no longer meets the criteria on which it was authorised. As soon as the decision is taken that it be discontinued, the instruction must be given to stop all surveillance of the subject and the date of the cancellation should be directly recorded.

163. In any case, the written authorisation will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the time it took effect (see paragraph 63 above). Written renewals may only be granted for three months at a time, and in order to grant them the authorising officer must be satisfied that it is necessary for the authorisation to continue for the purposes for which it was given (see paragraph 64 above). All applications for renewal should record whether it is the first renewal or every occasion a renewal was previously authorised; any significant changes to the information in the initial application; the reasons why the authoristion should continue; the content and value to the investigation or operation of the information so far obtained; and the results of regular reviews of the investigation or operation (see paragraph 65 above).

164. Detailed records pertaining to all authorisations must be centrally retrievable within each public authority and be retained for at least three years from the end of each authorisation (see paragraph 73 above). Moreover, it is the role of the surveillance commissioners to keep under review the exercise and performance of the powers and duties conferred by Part II of the Act. In doing so, they have the power to quash authorisations and order the destruction of any records relating to information obtained by authorised conduct (see paragraph 78 above).

165. Other than that which is subject to legal professional privilege, information obtained by secret surveillance may be used in evidence in criminal proceedings. However, the admissibility of such evidence would be subject to the control of the trial judge. In certain circumstances it would also be open to the trial judge to stay a prosecution for abuse of process (see paragraph 153 above).

166. Finally, any citizen who believes that they have wrongfully been subject to surveillance may bring a claim to the IPT and, save for vexatious or frivolous claims, the latter tribunal must determine any such claim. The IPT has the power to award compensation and make such orders as it thinks fit, including the quashing or cancelling of any order and the destruction of any records (see paragraph 79 above).

167. The foregoing considerations are sufficient to enable the Court to conclude that the provisions concerning directed surveillance, insofar as they related to the possible surveillance of consultations between detainees and appropriate adults, were accompanied by adequate safeguards against abuse.

168. Accordingly, no violation of Article 8 of the Convention can be found under that head.

II. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

169. The applicant complained of a violation of 6 of the Convention, which provides as relevant:

> "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....
>
> ... ...
>
> 3. Everyone charged with a criminal offence has the following minimum rights:
>
> ... ...
>
> (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."

170. In particular, he complained that his ability to communicate effectively with a solicitor in private was damaged in breach of Article 6 § 3(c) of the Convention and that his ability to communicate with an appropriate adult was compromised in breach of Article 6 generally.

171. Although the applicant was charged with the offence of withholding information, he did not stand trial for this or any other offence. Consequently, he cannot complain that any "restriction" imposed on him by virtue of the possibility of covert surveillance deprived him of a fair hearing in breach of Article 6.

172. Furthermore, even if the possibility of covert surveillance of his legal consultations could give rise to an issue under Article 6 § 3(c) of the Convention, the Court recalls that on 6 June 2010 the Administrative Court ordered that there should be no surveillance of the applicant's consultations with his lawyer or doctor pending the outcome of the judicial review proceedings. Consequently, the applicant would have had ample opportunity

to consult with both his legal and medical advisors safe in the knowledge that those consultations would not be subject to covert surveillance.

173. In light of the above, the Court considers that the applicant's complaints under Article 6 of the Convention are manifestly ill-founded within the meaning of Article 35 § 3(a) of the Convention.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

174. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

175. The applicant made no claim for pecuniary damage. However, he claimed six thousand euros (EUR 6,000) in respect of non-pecuniary damage. In particular, he argued that as a vulnerable person with a history of drug and alcohol abuse, anxiety and depression the concern that his legal consultations might be subject to covert surveillance caused him significant distress.

176. The Government argued that a declaration of a breach would be sufficient just satisfaction. In particular, they argued that there was no evidence that the applicant had experienced any suffering or distress related to the possibility that his legal consultations might have been subject to covert surveillance.

177. The Court agrees that the applicant has submitted no evidence to substantiate his claim that the possibility that his legal consultations were subject to covert surveillance caused him any real suffering or distress. Nevertheless, the applicant was undoubtedly a vulnerable young man at the time of his arrest and the Court is therefore prepared to accept that the possibility of not being able to speak freely with his solicitor was capable of having caused him some anguish. However, the possibility of covert surveillance only existed from 4 May 2010 to 6 May 2010, on which date the Administrative Court ordered that his legal consultations should not be subject to surveillance.

178. The Court therefore awards the applicant EUR 1,500 in respect of non-pecuniary damage.

B. Costs and expenses

179. The applicant also claimed GBP 26,126.08 for the costs and expenses incurred before the Court.

180. The Government argued that that sum was excessive.

181. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only insofar as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 15,000 covering costs under all for the proceedings before the Court.

C. Default interest

182. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the complaints under Article 8 of the Convention admissible and the remainder of the application inadmissible;

2. *Holds* that insofar as the applicant complains about the covert surveillance of legal consultations, there has been a violation of Article 8 of the Convention;

3. *Holds* that insofar as the applicant complains about the covert surveillance of consultations between detainees and their appropriate adults, there has been no violation of Article 8 of the Convention;

4. *Holds*

(a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:

(i) EUR 1,500 (one thousand five hundred euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;

(ii) EUR 15,000 (fifteen thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;

(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 27 October 2015, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Fatoş Aracı	Guido Raimondi
Deputy Registrar	President