5

SURVEILLANCE

A. Introduction

The scope of 'surveillance' as a covert policing resource

5.01 The Information Commissioner's *A Report on the Surveillance Society* written by Surveillance Studies Network[1] defines surveillance as 'purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection'.[2] With such a broad compass it is perhaps hardly surprising that the whole report is founded on an assumption, as the opening sentence of the report makes clear, that 'we live in a surveillance society'.[3]

5.02 It is obvious that only some of these concepts can fall within the ambit of an analysis of the law concerning covert policing. Indeed even the Information Commissioner's report concedes this, expressing surveillance for its purposes as 'a set of activities that have a similar

[1] Surveillance Studies Network, *A Report on the Surveillance Society* (2006).
[2] ibid, para 3.1.
[3] ibid, para 1.1.

characteristic [as opposed] to what the intelligence services or police may define as surveillance'.[4]

5.03 Equally, it would be wrong to limit the subject to any prescription offered by the intelligence agencies, police or other public authority that carry out surveillance. This is for at least two reasons. First, they are bound by statutory definition, informed and developed by the common law (it is this that primarily needs to be considered in the present context). Second, the evolution of the law of the United Kingdom may have presented the intelligence agencies and law enforcement with difficult operational propositions that have broadened the scope of what amounts to surveillance in investigative terms[5] and which requires some unravelling in order to attempt to understand it and practically apply it. In other words, there is that which police, intelligence agencies or relevant public authorities define as surveillance and there is that which they may not, but which may in fact amount to surveillance in any event.

5.04 A more orthodox definition of surveillance is not necessarily any more helpful generally, one that includes any conduct involving the close monitoring or observation of a person suspected of some wrongdoing,[6] for example. This is clearly too wide to capture the more discrete subject of surveillance as distinct from, say, the interception of communications or the use and conduct of covert human intelligence sources. It is clear that surveillance has a generic meaning as well as a more specific one.

5.05 From these sources, the scope of this chapter can at least be constrained by the statutory definitions of surveillance that have been conceived for the first time in United Kingdom law by the Regulation of Investigatory Powers Act 2000 (RIPA). Section 26 of RIPA creates two forms of covert surveillance—directed and intrusive—both of which are considered in detail below.[7] In addition, consideration should properly be given to ostensibly overt surveillance (such as for example, photography, CCTV,[8] as it has become known, as well as automatic number plate reading technology)[9] which may either have a covert purpose, or where the product is subsequently used covertly in the sense that the person affected by it does not know it has been retained, processed and disseminated and/or published.[10] This gives rise to the legally complex and volatile issue of the role of consent (which is unfortunately outside the scope of this work) and the evolving and surprisingly controversial question of when an expectation of privacy arises.[11]

5.06 Inevitably, brief consideration needs to be given to related topics, including the surveillance of employees, the admissibility of evidence obtained, and the problems caused by surveillance carried out by private individuals.[12]

[4] ibid, para 3.1

[5] See the discussion of *Wood v Commissioner of Police for the Metropolis* [2009] EWCA Civ 414 later in this chapter at paras 5.157–5.164.

[6] *Collins Dictionary*, 4th edn (Harper Collins, 2003).

[7] Below paras 5.63–5.129.

[8] Excluded expressly as amounting to either directed or intrusive surveillance by the Code of Practice, para 2.21.

[9] Also excluded, ibid.

[10] As in *Peck v The United Kingdom*, Application No 44647/98, ECHR 2003.

[11] See above Chapter 2 generally.

[12] Private surveillance is considered in detail below in Chapter 11.

5.07 The structure of this chapter will be to review the definitions of surveillance and then consider the authorization matrix. Thereafter it will look at non-statutory surveillance resources from a legal perspective and consider the practical implications arising from their use as well as touching on surveillance of employees and by private individuals. Finally, it will briefly look at the evidential issues that are likely to require consideration should the product of surveillance as prescribed by this chapter be needed as proof in legal proceedings.[13]

B. Surveillance Law: Statutory Sources

An overview

5.08 Like other forms of covert policing, state surveillance in the United Kingdom has historically been conducted in the absence of a legislative structure governing the basis upon which it should be carried out,[14] how the material gathered as a result of it may be used, and oversight of those carrying it out. Similarly, the evolution of a statutory framework is correlated to challenges to the domestic approach in Strasbourg, although surprisingly, few have touched on the form and nature of surveillance as it is now understood in United Kingdom law and focused instead on trespass to property[15] and the interception of communications.[16] None of the judgments offered guidance as to the definition of surveillance beyond recognizing that the level of intrusiveness of surveillance may be qualitatively different.[17]

5.09 Even the limited governance that existed prior to the enactment of legislation covering surveillance is of relatively recent origin. The first of note was the Guidelines on the Use of Equipment in Police Surveillance Operations issued by the Home Office.[18] These gave Chief Constables the power to authorize the use of listening devices in criminal investigations subject to familiar qualifying criteria, such as, the offences under investigation being really serious, other methods having been tried but failed, and a belief on the part of the officers that a conviction would result. A rudimentary proportionality assessment was required weighing the seriousness of the offence against the level of intrusiveness engaged in.

5.10 The United Kingdom's intelligence agencies have at different times been placed on a legislative footing—the Security Service (MI5) by virtue of the Security Service Act 1989 and the Secret Intelligence Service (MI6) and General Communications Headquarters (GCHQ) following the Intelligence Services Act 1994. Again, the legislation was permissive in the sense that it allowed those agencies to engage in surveillance activities in the broadest sense—including the interference with property—but there were no specific provisions, other than those relating to the interception of communications, relating the nature or type of surveillance that may be carried out.

5.11 The Home Office guidelines were placed on a statutory footing by virtue of Part III of the Police Act 1997 and in response to the challenge to the Guidelines before the European Court of Human Rights (ECtHR) in amongst others, *Khan v The United Kingdom*[19] on the

[13] Considered in detail below in Chapter 9.
[14] *Govell v The United Kingdom* [1999] EHRLR 101, ECtHR.
[15] *Khan v The United Kingdom* (2001) 31 EHRR 45.
[16] *Malone v The United Kingdom* (1985) 7 EHRR 14, ECtHR.
[17] See, eg, *Friedl v Austria* (1995) A/305-B, ECmHR, paras 49–50.
[18] House of Commons Library, 19 December 1984.
[19] (2001) 31 EHRR 45.

basis that they offended against the requirements in Article 8(2) being 'neither legally binding nor accessible'.[20] Emmerson and Ashworth[21] described the *Khan* case as 'the immediate catalyst for Part III of the Police Act 1997'.[22] This did not define or regulate surveillance per se but created a regime governing the trespass and installation of listening devices. Part III of the Police Act 1997 Act is considered in detail below in Chapter 6.

5.12 A Code of Practice on Intrusive Surveillance was issued on 27 October 1998 and revised a year later.[23] This provided guidance on the handling of confidential and privileged material, for example. This was the prevalent regime until RIPA came into force in September and October 2002.

5.13 In terms of basic principles, a number can be derived from the Strasbourg decisions. Covert surveillance is a serious interference with privacy rights[24] and must therefore be prescribed by law and be necessary and proportionate.[25] Importantly the law must be precise and clear[26] so that those who may be subjected to it have a sufficient indication as to the circumstances when it may be used.[27] As will become clear, serious questions arise about the clarity of RIPA in respect of surveillance activities and related issues. The preoccupation of the ECtHR is to achieve 'a proper balance between the defence of the institutions of democracy in the common interest and the protection of individual rights'.[28]

5.14 Principles specific to covert policing include that the use of such resources should be limited to serious and properly defined offences, it should not be exploratory or of a general nature and should be limited to cases where conventional means of enquiry are ineffective or have been unsuccessful.[29]

The Regulation of Investigatory Powers Act 2000

5.15 Chapter 1 considered the evolution of RIPA. It placed covert monitoring activities, other than the interception of communications, on a statutory footing for the first time in United Kingdom law. Ferguson and Wadham[30] described the 2000 Act in the following terms:

> On the one hand, it facilitated the use of diverse investigatory activities, while on the other, it provided a comprehensive regulatory framework, designed to respect the obligations imposed by the Human Rights Act 1993. In doing so it struck a fragile balance between the competing demands of privacy and surveillance.[31]

5.16 There is a division between other respected commentators and practitioners some of whom have said that RIPA 'goes a long way towards meeting this country's obligations, and is to

[20] ibid, para 23.
[21] Ben Emmerson QC and Andrew Ashworth QC, *Human Rights and Criminal Justice*, 1st edn (Sweet & Maxwell, 2001).
[22] ibid, 212.
[23] 18 November 1999.
[24] *Kopp v Switzerland* (1987) 27 EHRR 91, ECtHR.
[25] See, eg, *A v France* (1993) 17 EHRR 462, ECtHR.
[26] *Malone v The United Kingdom* (1985) 7 EHRR 14, ECtHR.
[27] ibid.
[28] *Brogan and Others v The United Kingdom* (1989) 11 EHRR 117, para 48.
[29] McDonald et al, *The European System for the Protection of Human Rights* (Martinus Nijhoff, 1993) 422.
[30] Ferguson and Wadham, 'Privacy and Surveillance: A Review of the Regulation of Investigatory Powers Act 2000' [2003] EHRLR Special Issue, 101.
[31] ibid.

be welcomed'[32] whilst another has argued that 'the value of privacy still finds little place in it despite the fact that the central statute now governing this area [RIPA] was introduced specifically to meet the demands of the European Convention on Human Rights'.[33]

5.17 RIPA is in five parts. Part I contains two chapters. Chapter I concerned with the interception of communications and Chapter II, the acquisition and disclosure of communications data. There are accompanying Codes of Practice issued under the provisions of section 71of RIPA.

5.18 Part II, which concerns some of the activities with which this chapter is largely concerned, relates to the regulation of surveillance activities and the use and conduct of covert human intelligence sources. It creates a two-tier authorization process to reflect the nature of the intrusiveness that is likely to be engaged in, although the legitimacy of this has been questioned.[34]

5.19 Part III is concerned with the investigation of data protected by encryption and Part IV, oversight. Part V deals with miscellaneous and supplemental provisions concerning the Act, related legislation and repeals and commencement. It also contains the Schedules referred to in earlier sections of the Act.

Section 80

5.20 Part V, although the last part of RIPA, is ironically one of the most important, particularly in the context of Part II activities, since it contains provisions that have a profound impact on how the legislation should be viewed in relation to its requirements and the protections it purports to extend. Section 80 is the best illustration, although characteristically obtuse in terms of the language employed:

> 80. Nothing in any provision of this Act by virtue of which conduct of any description is or may be authorised by any warrant, authorisation or notice, or by virtue of which information may be obtained in any manner shall be construed –
>
> (a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act;
>
> (b) as otherwise requiring –
>
> (i) the issue, grant or giving of such a warrant, authorisation or notice, or
>
> (ii) the taking of any step for or towards obtaining the authority of such a warrant, authorisation or notice,
>
> Before any such conduct of that conduct is engaged in; or
>
> (c) as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act.

5.21 The effect of this provision, once unravelled, is concerned in the most general sense with any conduct that may be engaged in under RIPA (for simplicity's sake this is referred to in this and subsequent paragraphs as 'covert conduct'). It does not make it unlawful to engage in covert conduct that would otherwise require some form of authorization or for such an authorization to be contemplated under RIPA. In other words it does not create, by virtue of providing an authorization regime for covert conduct, an unlawful act of not obtaining or

[32] Ben Emmerson QC and Andrew Ashworth QC, *Human Rights and Criminal Justice*, 1st edn (Sweet & Maxwell, 2001) 208.

[33] H Fenwick, *Civil Liberties and Human Rights*, 3rd edn (Cavendish, 2005) 635.

[34] Starmer, Strange, Whittaker et al, *Criminal Justice, Police Powers and Human Rights* (Blackstone Press, 2001).

taking steps to obtain an authorization for the covert conduct. Nor does it create a preferential legislative regime.

5.22 If a relevant public authority has the power to obtain the information another way, it is not required to use RIPA just because the information may be obtained by engaging in covert conduct. The Code of Practice provides:

> [An] authorisation under the 2000 Act is not required if a public authority has another clear legal basis for conducting covert surveillance likely to result in the obtaining of private information about a person. For example the Police and Criminal Evidence Act 1984 provides a legal basis for the police covertly to record images of a suspect for the purposes of identification and obtaining certain evidence.[35]

5.23 Although section 80 was not relied on by either party in *R (NTL Group Ltd) v Crown Court at Ipswich*[36] it is an example of the effect of the provision. An application for judicial review was brought by NTL following service on them by the police of a notice under section 9 of the Police and Criminal Evidence Act 1984 (PACE), requiring them to produce information relating to a customer's email address. In order to comply with the request, it was necessary to copy and send the emails to a separate email address, which would amount to an unlawful interception under section1 of RIPA. The Administrative Court held that the effect of the order under section 9 of PACE was to provide lawful authority under section 1(5) of RIPA and that no offence was therefore committed.

5.24 Section 80 arguably makes RIPA no more than a voluntary code, indeed, the Investigatory Powers Tribunal has referred to it as such expressly.[37] It provides protection from allegations of unlawfulness or impropriety, although this is clearly not its effect.[38] This is fundamental and its absence in many of the judgments in this area worrying. It could reasonably be expected to be a feature of any prosecution response to challenges by the defence that the provisions of the Act have been breached or not applied at all, although in a number of cases the provision has not been referred to.[39]

Section 27

5.25 Where an authorization is granted under Part II, section 27 of RIPA is engaged and the surveillance will be considered to be lawful 'for all purposes',[40] providing a Part II authorization 'confers an entitlement to engage in that conduct on the person whose conduct it is'[41] (ie the conduct engaged in under the terms of the authorization is by the person referred to in the authorization) and 'his conduct is in accordance with the authorisation'[42] (ie the conduct does not exceed that specified in the authorization). Importantly, it does not confer immunity from criminal activity.

5.26 No civil liability arises out of the conduct authorized under Part II or which is incidental to it[43] and 'is not itself conduct an authorisation or warrant for which is capable of being

[35] Code of Practice, para 1.15.
[36] [2002] 3 WLR 1173.
[37] *C v Police and Secretary of State*, No IPT/03/32/H, 14 November 2006.
[38] See *R v Sutherland* (unreported) 29 January 2002 as just one example.
[39] See, by way of just one glaring example, *R v Rosenberg* [2006] EWCA Crim 6.
[40] RIPA, s 27(1).
[41] ibid, s 27(1)(a).
[42] ibid, s 27(1)(b).
[43] ibid, s 27(2)(a).

granted under a relevant enactment and might reasonably have been expected to have been sought in the case in question'.[44] This latter element of what would limit civil liability is almost impenetrable but appears to extend to conduct that cannot in fact be authorized under 'a relevant enactment' (RIPA and the legislation discussed in paragraphs 5.08–5.12 above) even if there may have been a reasonable expectation that such an authorization (one that could not in fact be given) should have been sought. If anything is clear from this provision, it is simply that it is entirely gratuitous.

5.27 The conduct that may be authorized under Part II includes conduct outside the United Kingdom.[45] This does not necessarily make the conduct lawful outside the jurisdiction, this will depend on the law of the country where the conduct takes place but it will make it lawful for the purposes of United Kingdom law.[46]

The Code of Practice

5.28 A Code of Practice on Covert Surveillance (the former Code of Practice) was published following but some considerable time after RIPA came into force. A revised Code of Practice was introduced on 6 April 2010[47] (the Code of Practice) which incorporated expressly guidance on property interference. Surprisingly, in its introduction, it states that 'where covert surveillance activities are unlikely to result in the obtaining of private information about a person or where there is a separate legal basis for such activities, neither the 2000 Act nor this Code need apply'.[48] This is a remarkably primitive analysis of one of the most complex laws on the statute book, which does not appear in the former Code of Practice and those public authorities engaged in covert activities will need to be cautious in approaching the regulation of covert surveillance this simplistically.

5.29 The Code of Practice is admissible in criminal and civil proceedings. If relevant to an issue before a court or tribunal or the Office of the Surveillance Commissioner, the Code of Practice must be taken into account.[49]

C. Statutory Definitions of Surveillance

Surveillance

5.30 RIPA creates a regulatory regime for two types of surveillance—directed and intrusive. In typical form, some of the most important elements of the definition of surveillance are found in the last section of Part II.

5.31 Surveillance includes (so is not limited to) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.[50] It extends to the recording of such activity[51] and the use of a surveillance device (defined as 'any apparatus

[44] ibid, s 27(2)(b).
[45] ibid, s 27(3).
[46] Code of Practice, paras 1.20–1.23.
[47] Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2010, SI 2010/463.
[48] Code of Practice, para 1.5.
[49] ibid, para 1.6.
[50] RIPA, s 48(2)(a).
[51] ibid, s 48(2)(b).

designed or adapted for use in surveillance')[52] either wholly or in part to carry out any of the surveillance activity.[53]

5.32 It also extends to the interception of communications in the course of their transmission subject to the strict requirement that either the sender or recipient consents to the interception[54] and there is no warrant issued in connection with the interception[55] (although why a warrant would be issued in such circumstances is not clear).

5.33 It excludes any conduct of a covert human intelligence source whether he or she is wearing a surveillance device or not or information disclosed in the presence of a source[56] and the use of a source for obtaining or recording information.[57] It also excludes trespass to and interference with property or wireless telegraphy.[58]

Matters common to both directed and intrusive surveillance

5.34 Section 26(9) sets out matters common to both forms of surveillance. The surveillance, whether directed or intrusive, must be carried out covertly and involve the acquisition of private information.

5.35 Surveillance is carried out covertly if and only if 'it is carried out in a manner that is calculated to ensure that persons that are subject to the surveillance are unaware that it is or may be taking place'.[59] This may create difficulties. On the one hand, the intention of the relevant officers falls to be examined (what they intended the effect of the surveillance would be on those targeted by it) but on the other, the issue may be whether the target was aware first, that it was taking place in fact or secondly, that it may have been. The latter was the approach preferred by the Court of Appeal in *R v Rosenberg*,[60] although it is respectfully submitted that the former is the correct interpretation.

5.36 Private information is an express element of directed surveillance[61] but it is axiomatic that it is also an element of intrusive surveillance. Private information in relation to a person includes any information relating to his or her private or family life.[62] This places it squarely within the scope of Article 8 and should be read so as to encompass the broad definition given to concepts of private and family life in accordance with domestic law and the jurisprudence of the ECtHR.[63]

5.37 The Code of Practice helpfully makes it clear that even in a public place an expectation of privacy may exist, particularly 'where a record is being made by a public authority of that person's activities for future consideration or analysis'.[64] Further examples are given where

[52] ibid, s 48(1).
[53] ibid, s 48(2)(c).
[54] ibid, s 48(4)(a).
[55] ibid, s 48(4)(b).
[56] ibid, s 48(3)(a).
[57] ibid, s 48(3)(b).
[58] ibid, s 48(3)(c)(i)–(ii).
[59] ibid, s 26(9)(a).
[60] [2006] EWCA Crim 6.
[61] RIPA, s 26(2)(b).
[62] ibid, s 26(10).
[63] See above Chapter 2, Privacy, Proportionality and Human Rights Principles, in particular paras 2.13–2.65.
[64] Code of Practice, para 2.5.

the effect of information gathering may amount cumulatively to an interference with privacy.[65]

5.38 A request for an authority that combines an application for the use of directed surveillance (or use and conduct of a covert human intelligence source) and an application for the use of intrusive surveillance must be considered separately by the appropriate authorizing officer.[66] If the application includes an application to the Secretary of State for the use of intrusive surveillance the combined application must be made to the Secretary of State.[67]

5.39 The Code of Practice incorporates the modern concept of 'collaborative working'. This suggests that those granting authorizations should be aware 'of particular sensitivities in the local community where surveillance is taking place',[68] something akin but hopefully not a precursor to Privacy Impact Assessments, which may not be appropriate in the covert policing arena.[69]

5.40 In addition, where one public authority is acting on behalf of another, the tasking authority should obtain or provide the authorization. If operational support is required at the planning stage this should be specified in the authorization.[70] Duplication of authorizations should be avoided.[71]

Directed surveillance

5.41 Section 26 creates amongst other things two forms of surveillance—directed and intrusive.[72] The section cryptically provides that 'surveillance is directed . . . if it is covert but not intrusive' and meets three criteria. First, it is carried out for the purposes of a specific investigation or a specific operation.[73] Secondly it is carried out in such a manner as is likely to result in the obtaining of private information about a person (whether specifically identified as part of the specific investigation or operation, so in fact, *any* person).[74] Thirdly it is carried out other than by way of an immediate response to events or circumstances that is such that it would be reasonably impracticable to obtain an authority to engage in the surveillance activity.

5.42 There is an exception to what may amount to directed surveillance provided for in section 26(6) which on one view could be considered quite extraordinary. Activities relating to the detection of television licence evasion do not amount to directed surveillance and are singled out as such even though it is difficult to see how determining whether a household is in possession of a television set using this technology could ever amount to the obtaining of private information about a person.

C v Police and Secretary of State

5.43 There has been only one authority considering the issue of what qualifies as 'directed surveillance'. In *C v Police and Secretary of State*[75] a case before the Investigatory Powers Tribunal, an

[65] ibid, paras 2.6–2.7.
[66] RIPA, s 43(2); see also the Code of Practice, paras 3.12–3.14.
[67] RIPA, s 30(2)(a)–(b).
[68] Code of Practice, para 3.15.
[69] V Williams, 'Privacy Impact Assessments and Public Space Surveillance' [2007] Covert Policing Review 2, 4–18; the editorial in the same issue at 3 is critical of their use in covert policing technologies.
[70] Code of Practice, para 3.16.
[71] ibid, para 3.17.
[72] See generally ibid, Chapter 2.
[73] RIPA, s 26(2)(a).
[74] ibid, s 26(2)(b).
[75] No IPT/03/32/H, 14 November 2006.

issue arose as the whether the conduct engaged in amounted to directed surveillance and if so whether it needed to be authorized. C was a retired police officer suspected of malingering and had been subjected to surveillance by enquiry agents instructed by his employer. C complained that the surveillance should have been authorized under RIPA. In the course of its judgment the Tribunal considered the definition of directed surveillance and in particular the requirement that the surveillance was undertaken for a specific investigation or operation in accordance with section 26(2)(a).

5.44 The Tribunal interpreted the provision narrowly as limiting directed surveillance 'to the discharge of the public authority's particular public or "core functions" specific to it'.[76] It went on to state that 'the definition of "directed surveillance" in section 26 must be read in the context of the scheme of RIPA as a whole'.[77] In this connection a relevant factor was whether an authorization could have been sought and obtained *in principle*. This is a useful test and one which, if applied to cases where the question of authorization arises, will assist the court in resolving the issue.

5.45 The Code of Practice covers the effect of the decision in *C*.[78] Difficulties will arise where the investigation may be both criminal and disciplinary and each case will need to be decided on its own facts. This is likely to be a challenging area for police professional standards departments who should seek advice in every case. Those representing officers or advising disciplinary panels may also need to consider the issue carefully in order to determine whether an authorization should have been put in place.

Other cases

5.46 In *R v Rosenberg*[79] the appellant had been convicted at first instance of drug-related offences following the admission of video footage obtained by her neighbours (they had erected a CCTV camera in their garden which filmed activities inside Ms Rosenberg's living room). On appeal it was argued that the surveillance should have been authorized under RIPA as the police had been complicit in the acquisition of it. The Court of Appeal dismissed the appeal on the basis that the camera was 'ostentatious' and therefore not covert but a simpler and more forensic approach would have been, applying *C*, to determine whether the surveillance could have in fact been authorized and obtained in principle. Since it was not in fact carried out by the police, it is likely that this alone would have been a determinative factor in itself.

5.47 A similar issue arose in *R v Leadbetter*,[80] a case in the lower courts where the defendant argued that surveillance carried out on animal rights activists should have been authorized under RIPA. The District Judge concluded that 'the Regulation of Investigatory Powers Act 2000 applies' (although did not specify which provisions applied or how). Again, if the issue was approached in the way suggested in *C*, it is respectfully submitted that it would have been determined differently. The issue of whether the facts give rise to a basis upon which to authorize the activity as use and conduct of a covert human intelligence source is considered below in Chapter 7.

[76] ibid,para 57.
[77] ibid, para 61.
[78] Code of Practice, paras 2.25–2.26.
[79] [2006] EWCA Crim 6.
[80] (Unreported), decided by District Judge Parsons in Bournemouth Magistrates Court on 4 November 2009.

Intrusive surveillance

5.48 The matrix for authorizing intrusive surveillance creates a system of independent review and the possibility that any application granted may not be approved and therefore takes effect. This has received some tentative support from Fenwick who has said 'the standard of scrutiny may be variable, but the very fact that an authorisation will be checked independently may tend to foster rigour in preparing the papers'.[81]

5.49 Surveillance is intrusive if it is carried out in relation to anything taking place on any residential premises or in any private vehicle[82] and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.[83]

5.50 Residential premises are defined in section 48(1):

> '[R]esidential premises' means . . . so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used).

5.51 This is subject to a qualification in respect of common areas to which the person may have or be allowed access in connection with the use or occupation of the premises.[84] The Code of Practice provides examples of what would and would not qualify. A rented flat, prison cell or hotel room are examples of the former;[85] the communal stairwell of a block of flats, police canteen or hotel reception examples of the latter.[86] Fenwick has expressed concern about whether this reflects correctly a sophisticated approach to surveillance activities:

> [T]he distinction between directed surveillance and 'general law enforcement' functions, such as observing persons entering or leaving a house, turns on the question whether or not the observation can be viewed as an immediate response—another instance in which fine lines may be drawn. If observation of a house occurs over a period of time, it can be argued that an invasion of privacy is occurring that can no longer be viewed as an immediate response and which requires therefore a statutory underpinning.[87]

5.52 Private vehicles are also defined in section 48(1) as 'any vehicle which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it'. It excludes a person using a taxi (but not the taxi driver) or other vehicle where they have paid for the use of the vehicle and driver for a journey.[88] Other examples are provided in the Code of Practice.[89]

5.53 Again, monitoring for the purposes of investigating television licence evasion is excluded from conduct that would amount to intrusive surveillance[90] as it is the product from a device that monitors anything taking place on residential premises or in a private vehicle[91] but where the device is not located on the premises or in the vehicle unless 'it consistently

[81] H Fenwick, *Civil Liberties and Human Rights*, 3rd edn (Cavendish, 2005) 698.
[82] RIPA, s 26(3)(a).
[83] ibid, s 26(3)(b).
[84] ibid, s 48(7)(b).
[85] Code of Practice, para 2.15.
[86] ibid, para 2.16.
[87] H Fenwick, *Civil Liberties and Human Rights*, 3rd edn (Cavendish, 2005) 699.
[88] RIPA, s 48(7)(a).
[89] Code of Practice, para 2.17.
[90] RIPA, s 26(6).
[91] ibid, s 26(5)(a).

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'.[92] Any surveillance by way of a device adapted for the purpose of providing information about the location of a vehicle[93] or which amounts to an interception of a communication[94] as falls within section 48(4) is not intrusive surveillance. The Code of Practice provides guidance that either forms of conduct may amount to directed surveillance.[95]

5.54 If the surveillance involves trespass to or interference with property or wireless telegraphy, Part III of the Police Act 1997 or the Intelligence Services Act 1994 applies.[96]

5.55 The Information Commissioner, in response to the draft Bill,[97] expressed the view that intrusive surveillance should include 'any premises or location where the individual has a legitimate expectation of privacy' such as a doctor's surgery. Some commentators have also been critical of the definition suggesting that 'the attempt to draw a line between "directed" and "intrusive" surveillance may bring the operation of RIPA 2000 into conflict with the requirements of Article 8'.[98] Whittaker has argued that 'some directed surveillance may nonetheless be considered sufficiently intrusive to warrant greater protection from misuse than is currently provided for under RIPA 2000'.[99] This was a pointed analysis. In the later case of *In Re McE*[100] the House of Lords held that RIPA permitted covert surveillance of consultations between solicitors and their clients although directed surveillance authorizations should be treated as if the conduct was intrusive. Subsequently, the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010[101] was approved by Parliament.

D. Applications for Authorization: Requirements

General best practice

5.56 There is guidance in the Code of Practice to what is referred to as 'general best practice'.[102] Although there is no statutory requirement, it is also essential that a proper regime of review is in place within any relevant public authority, a matter upon which the Office for the Surveillance Commissioner has commented in his Annual Report.[103] The Code of Practice properly notes that there is 'a 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'.[104]

---

92 ibid, s 26(5)(b).
93 ibid, s 26(4)(a).
94 ibid, s 26(4)(b).
95 Code of Practice, paras 2.8 and 2.20.
96 See RIPA, s 48(3) and generally below Chapter 6, Property Interference.
97 *Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill* (March 2000).
98 Starmer et al, *Criminal Justice, Police Powers and Human Rights* (Blackstone Press, 2001) 66.
99 ibid.
100 [2009] UKHL 15.
101 SI 2010/461.
102 Code of Practice, paras 3.27–3.30.
103 Office of the Surveillance Commissioner, Annual Report, 2005, section 4.
104 Code of Practice, para 3.22.

5.57 The frequency of reviews should be considered at the outset of the operation and should be 'as frequently as is considered necessary and practicable'.[105] The authorizing officer may delegate the reviewing function but the Code of Practice warns against this as the authorizing officer is 'usually best placed to assess whether the authorisation should continue or whether the criteria on which he based the original decision . . . have changed sufficiently to cause the authorisation to be revoked'.[106]

5.58 Whoever carries out the review must be alert to any unforeseen changes to the nature or extent to which the level of interference with privacy has changed, or any proposed changes. The whole basis of the granting of the authority may need to be reconsidered, including its necessity and/or proportionality.[107] This is particularly important where the identity of the target of the operation was not known but is later established.[108]

5.59 The best practice guidance in relation to the applications for authorization includes avoiding unnecessary information[109] and the repetition of information, keeping detailed records of decisions granted orally under urgent procedures, detailing the involvement of other agencies and avoiding duplication of authorizations already given.[110] In addition, the senior responsible officer (someone who holds the rank or position of an authorizing officer) should be responsible for the integrity of the internal processes, managing and compliance with authorisations, and engaging with the Office for the Surveillance Commissioner.[111]

5.60 Local authorities are advised to ensure the senior responsible officer is a member of the 'corporate leadership team' and should ensure compliance with the Annual Reports of the Office of the Surveillance Commissioner and that the reports form part of an annual policy review. These are all matters that can be introduced into the evidence in any case and in respect of which appropriate witnesses can be cross-examined.[112]

5.61 In practice there are a number of questions that can be set out and answered by way of a basic framework for operational planning: is it a public authority authorized under RIPA to carry out surveillance; is it entitled to authorize the conduct that it proposes to engage in; have the rules governing authorization been observed (including those relating to urgent applications and renewals); is the wording of the authority sufficiently precise; is the analysis of necessity and proportionality sound?

Directed surveillance authorizations

Designated persons

5.62 Designated persons (or authorizing officers) within relevant public authorities have the authority to grant directed surveillance authorizations.[113] Relevant public authorities are set

[105] ibid, para 3.23.
[106] ibid, para 3.24.
[107] ibid, para 3.25.
[108] ibid, para 3.26.
[109] Information should be limited to that required by the relevant information, ibid, para 3.27.
[110] ibid.
[111] ibid, para 3.28.
[112] ibid, paras 3.29 and 3.30.
[113] Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000, SI 2000/2417, Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Amendment) Order 2002, SI 2002/1298 as amended by SI 2003/3173, SI 2005/1084, SI 2006/594.

out in Parts I and II of Schedule 1 to RIPA[114] and range from any police force, any of the intelligence agencies and Her Majesty's forces at one end of the spectrum to the National Assembly for Wales, the Post Office and the Royal Pharmaceutical Society of Great Britain at the other. Public authorities can be removed from, or added to, the list of relevant public authorities[115] by Order, a draft of which must be laid before Parliament and approved by a resolution of each House.[116] In Northern Ireland this power may be exercised subject to qualifications by the First Minister and Deputy First Minister (in conjunction with the Secretary of State).[117]

5.63 Designated persons are identified by Order[118] and may be subject to restrictions on the authorizations they may grant[119] and the circumstances in which or the purposes for which they may grant authorizations.[120] Frustratingly, the provisions relating to designated persons are found after those relating to authorizations. Within a police force the designated person must hold the rank of a superintendent or in urgent cases an inspector, an officer in the Security Service must hold the position of General Duties 3 or be any other officer at Level 3 and within the Post Office, the designated person is the Territorial Security Officer.[121]

5.64 Authorizations for directed surveillance are governed by section 29. Designated persons for the purposes of this section have power to grant authorizations for the carrying out of directed surveillance but can only do so if they believe there are grounds to do so[122] and the proposed surveillance to be authorized is proportionate[123] to what is sought to be achieved by carrying it out.[124] The Chief Surveillance Officer has emphasized that this exercise must be carried out conscientiously by authorizing officers[125] and they should expect to be rigorously tested on it in cross-examination in appropriate cases.

Applications: form and content

5.65 The grounds upon which an authorization may be granted are any of the following—the interests of national security,[126] for the purpose of preventing or detecting crime or of preventing disorder,[127] the interests of the economic well-being of the United Kingdom,[128] the interests of public safety,[129] for the purpose of protecting public health,[130] for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable

[114] RIPA, s 30(4)(a); and Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).
[115] RIPA, s 30(5).
[116] ibid, s 30(7).
[117] ibid, s 31 generally.
[118] The Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000 (SI 2000/2417).
[119] RIPA, s 30(3)(a); and Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).
[120] RIPA, s 30(3)(b); detecting crime is the only ground subject to elaboration in the 'general interpretation' section of the Act: see s 81(5).
[121] Part I of the Schedule to the Order.
[122] RIPA, s 28(2)(a); the grounds are set out in s 28(3)(a)–(g).
[123] The Code of Practice provides some guidance on necessity and proportionality at paras 3.3–3.7.
[124] RIPA, s 28(2)(b).
[125] Annual Report of the Chief Surveillance Officer, 2000–2001, para 4.13.
[126] RIPA, s 28(3)(a).
[127] ibid, s 28(3)(b).
[128] ibid, s 28(3)(c).
[129] ibid, s 28(3)(d).
[130] ibid, s 28(3)(e).

to a government department,[131] or for any purpose other than the above which is specified for the purposes of this subsection by any later order made by the Secretary of State[132] which must be laid before Parliament and approved by a resolution of each House.[133]

5.66 Applications for directed surveillance in national security cases are, in general, the province of the Security Service, whose statutory functions include the protection of national security.[134] The only exceptions are where the operations are carried out by police units with a formal counter-terrorism role (for example, Special Branch, Counter-Terrorism Units, Counter-Terrorist Command) or where the Security Service has agreed that, in the discharge of its functions, another public authority can carry out the surveillance on its behalf.[135] Her Majesty's forces undertake surveillance in connection with the military threat to national security, in support of the Security Service and, where necessary, the Police Service of Northern Ireland.[136]

5.67 Not all public authorities are able to seek authorizations on the available grounds.[137] The Serious Organised Crime Agency (SOCA) can only conduct directed surveillance for the purposes of the prevention or detection of crime or disorder.[138]

5.68 The conduct that is authorized by a directed surveillance authorization is the directed surveillance as specified in the authorization[139] provided it is carried out in the circumstances described in the authorization and for the purposes of the investigation or operation specified or described in the authorization.[140] It follows therefore that conduct outside the terms of the authorization is *de facto* unlawful insofar as section 27 purports to make such surveillance lawful for all purposes. However section 27(2) may still operate to create immunity from civil suit.

5.69 Police and customs authorizations may only be granted by designated persons within a police force, SOCA or Revenue and Customs on applications from within the same organization (ie the power to grant an authorization is not transferable as between relevant public authorities).[141] This is also covered in the Code of Practice.[142]

5.70 The Code of Practice identifies 10 matters that need to be covered in an application and it is against this list that authorizations should be checked by authorizing officers, reviewed by the Office for the Surveillance Commissioners on an inspection, or subjected to examination in legal proceedings. It comprises the reasons why the application is necessary and the grounds upon which it is based, the nature of the surveillance engaged in, the identities of the targets, a summary of the intelligence case, the information it is hoped will be acquired

131 ibid, s 28(3)(f).
132 ibid, s 28(3)(g).
133 ibid, s 28(5).
134 Security Service Act 1989, s 1.
135 Code of Practice, fn 31 summarizes the position.
136 ibid, fn 32 summarizes the position.
137 A matter about which the Chief Surveillance Commissioner has expressed concern in his Report for 2006–2007, paras 10.2–10.3.
138 Serious Organised Crime and Police Act 2005 (Consequential and Supplementary Amendments to Secondary Legislation) Order 2006, SI 2006/594.
139 RIPA, s 28(4)(a).
140 ibid, s 28(4)(b).
141 ibid, ss 33(1)–(2).
142 Code of Practice, para 3.20.

as a result of the deployment, an assessment of collateral intrusion and why it is justified in the circumstances, any confidential information at risk of being acquired, an assessment of the proportionality of the proposed operation, the level of authority required and the record of decision and the date and time of this.[143]

5.71 The Chief Surveillance Officer has emphasized the need for language to be used carefully and precisely, in applications for authorizations.[144]

5.72 Harfield and Harfield offer investigators the following practical advice:

> Thus investigators must seek detailed authority for all the conduct they wish to engage in, and authorising officers must ensure that their authorities specify in detail all conduct that they are content to authorise. Where authorising officers authorise more than has been applied for they must state their reasons for doing so. Similarly they must record their reasons for not authorising all or any of the conduct detailed in an application.[145]

Urgent cases

5.73 Authorization can be granted or renewed orally in an urgent case or must otherwise be in writing.[146] It should consider the matters referred to in the preceding paragraph. In typically opaque language, the person's entitlement to authorize or renew in an urgent case 'is not confined to urgent cases'.[147] In his annotation to RIPA, Cape has extrapolated this as meaning that a person entitled to act for a senior authorizing officer in an urgent case who also makes an application must do so in writing.[148] It is not clear from the section that this is the effect in urgent cases and it is difficult to comprehend why someone with delegated powers to handle urgent cases would then as a consequence of how the section is drafted, be prevented from doing so, other than in writing.

5.74 The term 'urgent' is not defined in RIPA but the Code of Practice offers the following guidance:

> 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 was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's or applicant's own making.[149]

5.75 The record of an urgent application that has been granted should include the identities of the targets, the nature of the surveillance, the reasons why the authorizing officer considered the case sufficiently urgent so as to approve it orally and, where it was not considered by the authorizing officer but an officer entitled to authorize in his or her absence, why it was not reasonably practicable to for the application to be considered by the authorizing officer.[150]

143 ibid, para 5.8.
144 Annual Report of the Chief Surveillance Officer, 2003–2004, para 12.
145 C Harfield and K Harfield, *Covert Investigation*, 2nd edn (Oxford University Press, 2008) 38.
146 RIPA, s 43(1).
147 ibid, s 34(1)(a); see also SI 2003/3171, SI 2005/1084, SI 2006/594 and SI 2006/1874.
148 Edward Cape, *RIPA 2000, Related SIs and Codes of Practice* (Thomson Sweet & Maxwell, 2005).
149 Code of Practice, para 5.6.
150 ibid, para 5.9.

5.76 The authorizing officer should not generally be involved in any operation he or she authorizes but where this is unavoidable, the centrally retrievable record of authorizations should highlight this and it should be brought to the attention of either the Commissioner or Inspector on the next inspection.[151]

Duration, renewal and cancellation

5.77 In cases where authorization is given in writing it lasts for three months,[152] or in the case of an authorization granted by an intelligence agency six months.[153] An urgent application may be authorized for up to 72 hours[154] before it is required to be renewed and if not renewed the authorization ceases to have effect.

5.78 A directed surveillance authorization may be renewed for a further period of three months[155] or where it has been granted by one of the intelligence agencies it can be renewed for a further period of six months[156] by an authorizing officer (providing the criteria for granting it continues to exist). An application to renew 'should not be made until shortly before the authorisation period is drawing to an end'[157] or there is a material change in circumstances.

5.79 A decision to renew should record as a minimum whether it is the first renewal, or the date and details of every previous renewal, any significant changes to the information since the application for authorization was made, the reasons why it should continue, an assessment of what intelligence has been obtained so far and its value to the operation and the results of any reviews.[158]

5.80 No renewal should be granted unless the authorizing officer is satisfied that a review has been carried out and the results of it considered.[159] There are obtuse provisions about the timing of authorizations in section 43(9). It seems that the granting of authorization takes effect on the day of authorization and the renewal on the day the authorization would otherwise have expired. There is no limit to the number of applications for renewals that can be made and approved providing the criteria one met on each occasion and the renewals are centrally recorded.[160]

5.81 An authorization must be cancelled if the grounds upon which it was granted are no longer satisfied,[161] although the authorizing officer (or other person entitled) can modify an application on reviewing it so as to cease surveillance against someone no longer of interest or they can stop using a particular tactic that is not effective.[162] Once cancelled, surveillance should cease immediately. The date of cancellation should be centrally recorded and good practice seems to be also to record what was acquired by the surveillance and whether or not the operational objectives were met.[163]

[151] ibid, para 5.7.
[152] RIPA, s 43(3)(c).
[153] ibid, s 44(5).
[154] ibid, s 43(3)(a)(i).
[155] ibid, s 43(4).
[156] ibid, s 44(7).
[157] Code of Practice, para 5.14.
[158] ibid, para 5.15.
[159] RIPA, s 43(6).
[160] Code of Practice, para 5.16.
[161] RIPA, s 45(1)(a).
[162] Code of Practice, para 5.17.
[163] ibid, para 5.18.

Intrusive surveillance

Senior authorizing officers

5.82 Section 32 of RIPA provides, subject to exceptions, that the Secretary of State or senior authorizing officers shall have power to grant authorizations for the carrying out of intrusive surveillance.[164] Senior authorizing officers are listed in section 32(6) and include Chief Constables, Provost Marshalls of each branch of the armed forces and the Director General of SOCA.

5.83 Neither the Secretary of State nor a senior authorizing officer can grant an authorization for the carrying out of intrusive surveillance unless he believes it necessary on grounds provided and it is proportionate to what is sought to be achieved by carrying it out to do so.[165] This requires an assessment to be carried out as to whether the information derived from the conduct to be engaged in could reasonably be obtained by other means.[166]

Applications: form and content

5.84 Unlike applications for directed surveillance or use and conduct of covert human intelligence sources, there are only three grounds upon which an intrusive surveillance authorization may be granted. They are the interests of national security,[167] for the purpose of preventing or detecting serious crime,[168] or the interests of the economic well-being of the United Kingdom.[169]

5.85 The conduct that is authorized by an intrusive authorization is any conduct that consists in the carrying out of intrusive surveillance of any such description as is specified in the authorization,[170] is carried out in relation to the residential premises specified or described in the authorization or in relation to the private vehicle so specified or described[171] and is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.[172]

5.86 A senior authorizing officer within a police force, SOCA or Revenue and Customs must not grant an authorization for the carrying out of intrusive surveillance except on an application from within their own organizations and where this includes conduct relating to residential premises these are within the area of operation of that organization.[173] Areas of operation and residential premises are separately defined in respect of those organizations capable of granting intrusive surveillance.[174] There is guidance provided in the Code of Practice under the somewhat popular heading 'collaborative working'.[175]

5.87 It is permissible for one authorization to combine both an intrusive surveillance authorization made by or on the application of an individual who is a member of a police force or

[164] RIPA, s 32(1).
[165] ibid, s 32(2)(a)–(b).
[166] ibid, s 32(4).
[167] ibid, s 32(2)(a).
[168] ibid, s 32(2)(b).
[169] ibid, s 32(2)(c).
[170] ibid, s 32(5)(a).
[171] ibid, s 32(5)(b).
[172] ibid, s 32(5)(c).
[173] ibid, s 33(3) and (4).
[174] ibid, s 33(6) generally.
[175] Code of Practice, paras 3.15–3.21 and paras 6.9–6.10.

SOCA, or who is a customs officer and an authorization given by, or on the application of, that individual under Part III of the Police Act 1997. Where a combined authorization is sought the applicable provisions of both RIPA and the Police Act 1997 apply to the respective aspects of the authorization.[176]

5.88 Where the authorizing officer or designated deputy within a police force, SOCA or Revenue and Customs is unavailable (section 34 defines unavailable as being 'not reasonably practicable, having regard to the urgency of the case, for the application to be considered by any person who is a senior authorising officer'; the term 'reasonably practicable' is elaborated upon in the Code of Practice at footnote 43 and includes absence on leave but is likely to exclude pressure of work) and the request for authorization is urgent, the application can be made to and considered by any person listed in section 34(4)[177] (subject to the limitations set out in section 34(5)). This includes, for example, an assistant Chief Constable or deputy Provost Marshall.[178]

5.89 A person who considers an application in the absence of the authorizing officer or his or her designated deputy has the same power to grant an authorization as the person for whom he or she is entitled to act.[179]

Notification requirements

5.90 Any authorization or cancellation by the police or customs[180] must be notified as soon as is reasonably practicable to what is referred to as 'an ordinary Surveillance Commissioner'[181] (presumably this means a Commissioner other than the Chief Surveillance Commissioner). The obligation to do so is the responsibility of the person granting or cancelling the authorization.[182]

5.91 There are a number of notification requirements. It must be given in writing (but can be transmitted electronically)[183] as soon as reasonably practicable after the grant or, as the case may be, cancellation of the authorization to which it relates,[184] it must be given in accordance with any such arrangements made for the purposes of this paragraph by the Chief Surveillance Commissioner as are for the time being in force,[185] and it must specify such matters as the Secretary of State may by later Order prescribe[186] (the usual provision is made that no Order shall be made unless a draft of the Order has been laid before Parliament and approved by a resolution of each House: section 35(5). This is subject to an exception in section 35(6) that it does not apply to the first Order made. Under section 35(7) this Order must be approved by both Houses within 40 days or it will cease to have effect).[187]

176 RIPA, s 33(5).
177 ibid, s 34(2).
178 See Code of Practice, para 6.5.
179 RIPA, s 34(3).
180 The usual definitions extend to the references to police, SOCA and customs officers and to those officers who grant or cancel authorizations in the absence of the senior authorizing officer and his or her deputy: ibid, s 35(10).
181 ibid, s 35(1).
182 ibid.
183 ibid, s 35(9).
184 ibid, s 35(2)(a).
185 ibid, s 35(2)(b).
186 ibid, s 35(2)(c).
187 See also ibid, s 35(8).

The arrangements can be found in the Regulation of Investigatory Powers (Notification of Authorisations etc) Order 2000.[188]

5.92 A notice must either state that the approval of a Surveillance Commissioner is required by section 36 before the grant of the authorization will take effect[189] or state that the case is one of urgency and set out the grounds on which the case is believed to be one of urgency.[190]

Urgent cases

5.93 An urgent case is subject to the same criteria as in cases of directed surveillance (risk of endanger to life, etc).[191] The Code of Practice makes it clear that the provisions in relation to urgent applications should not be used routinely.[192] If the senior authorizing officer or his or her designated deputy is not available, an authorization may be granted by a person entitled to act in urgent cases. In police forces out of hours officers of assistant Chief Constable rank or above are entitled to act in this capacity.[193] The decision to grant an authority in an urgent case must be recorded in writing by the person who applied for it as soon as reasonably practicable.[194] It takes effect from the time it is granted providing proper notice is given to the Surveillance Commissioner.[195]

5.94 Where a case becomes urgent after approval has been sought, the authorizing officer should notify the Surveillance Commissioner that the case is urgent and the authorization will take effect immediately.[196] The Code of Practice is ambiguous on whether it takes effect on notification to the Surveillance Commissioner or once the authorizing officer determines it is in fact an urgent case. The legislation presumably prevails and the latter interpretation is correct since the senior authorizing officer retains the statutory power to grant an urgent authorization if the criteria are met.

Role of the Surveillance Commissioner

5.95 There are obligations on the Surveillance Commissioner who receives a notice that an intrusive surveillance authorization has been granted. He or she must, as soon as practicable, scrutinize the authorization[197] and in a case where notice has been given that approval is required before the authorization will take effect, decide whether or not to approve the authorization.[198]

5.96 Where an authorization for the carrying out of intrusive surveillance has been granted on the application of a member of a police force, SOCA or a customs officer, the authorization does not take effect until such time (if any) as it has been approved by an ordinary Surveillance Commissioner[199] and written notice of this has been given to the person who granted the authorization.[200] The Code of Practice states that it 'will not take effect until the notice has

[188] SI 2000/2563.
[189] RIPA, s 35(3)(a).
[190] ibid, s 35(3)(b).
[191] See above para 5.75.
[192] Code of Practice, para 6.15.
[193] ibid, para 6.7.
[194] ibid, para 6.6.
[195] ibid, para 6.12.
[196] ibid, para 6.13.
[197] RIPA, s 35(4)(a).
[198] ibid, s 35(4)(b).
[199] ibid, s 36(2)(a).
[200] ibid, s 36(2)(b).

been received in the office of the person who granted the granted the authorisation',[201] although this seems an overly zealous interpretation of RIPA and unlikely to bind the courts if the senior authorizing officer happens to receive notice of approval somewhere other than in his or her office. This does not apply to urgent cases providing the provisions relating to urgent cases have been complied with.[202]

5.97 The Surveillance Commissioner can only give his approval to the grant of authorization if, and only if, he is satisfied that there are reasonable grounds for believing that it is necessary and proportionate to do so.[203] Written notice of the Commissioner's decision should be given to the person who granted the authorization as soon as reasonably practicable.[204] Any notice can be provided electronically.[205]

5.98 If the Surveillance Commissioner decides not to approve an authorization he or she must make a report of his findings to the most senior relevant person within the organization who sought it. The most senior relevant person is defined in section 36(6) and (7).

5.99 Where an intrusive surveillance authorization has been granted on the application of a member of a police force, SOCA or a customs officer, and a Surveillance Commissioner is at the time or later satisfied that, at the time when the authorization was granted or at any time when it was renewed, there were no reasonable grounds for believing that it was neither necessary nor proportionate, he or she may quash the authorization with effect, as he thinks fit, from the time of the grant of the authorization or from the time of any renewal of the authorization.[206]

5.100 If a Surveillance Commissioner is satisfied at any time while the authorization is in force that there are no longer any reasonable grounds for believing that it was necessary and proportionate, he may cancel the authorization with effect from the time when the basis for its being granted ceased to exist.[207] Those who drafted RIPA have found it necessary to specify that in these circumstances, the Surveillance Commissioner does not have to give notice of cancellation to his or her own office.[208]

5.101 Where an urgent authorization has been granted and the appropriate notice has been given,[209] the Surveillance Commissioner may quash the authorization from the time of the grant of the authorization or from the time of any renewal of the authorization, if he or she is satisfied that at the time of the grant or renewal of the authorization there were no reasonable grounds for believing that the case was one of urgency.[210] Providing any records relating to the authorization are not required for either civil or criminal proceedings, the Surveillance Commissioner may also order their destruction in part or full.[211] A similar power to order destruction of records exists in respect of an authorization that has ceased to have effect and where the Commissioner

[201] Code of Practice, para 6.11.
[202] RIPA, s 36(3).
[203] ibid, s 36(4)(a); the Commissioner must be satisfied s 32(2)(a) and (b) has been met.
[204] ibid, s 36(4)(b).
[205] ibid, s 36(8).
[206] ibid, s 37(2).
[207] ibid, s 37(3).
[208] ibid, s 37(10).
[209] In accordance with ibid, s 35(3)(b).
[210] ibid, s 37(4).
[211] ibid, s 37(5).

concludes that for some of the time whilst it was in force, grounds did not exist for the granting of the authorization.[212] No destruction can take place until the period for appealing has expired[213] or any appeal has been later dismissed by the Chief Surveillance Officer.[214]

Quashing authorizations and appeals

5.102 There are reporting requirements imposed on the Surveillance Commissioner exercising the power to quash authorizations who must as soon as reasonably practicable make a report of his exercise of that power, and of his reasons for doing so.[215] These must be sent to the most senior relevant person[216] and to the Chief Surveillance Commissioner.[217] Where an authorization is quashed or cancelled by a Surveillance Commissioner those involved in the operation must be instructed immediately to cease carrying out the surveillance. The date and time the instruction is given must be recorded and retained for at least three years.[218]

5.103 A senior authorizing officer may appeal to the Chief Surveillance Commissioner against a refusal of a Surveillance Commissioner to approve an authorization for the carrying out of intrusive surveillance,[219] a decision of such a Commissioner to quash or cancel such an authorization[220] and/or a decision of such a Commissioner to make an order under section 37 for the destruction of records.[221] The right to appeal extends to persons entitled to act for a senior authorizing officer.[222]

5.104 Any appeal must be brought within the period of seven days beginning with the day on which the refusal or decision appealed against is reported to the appellant.

5.105 The Chief Surveillance Commissioner must allow an appeal if he or she is satisfied that there were reasonable grounds for believing that the authorization was necessary and proportionate[223] and was properly urgent[224] at the time it was granted and he or she is not satisfied that the authorization is one of which notice was given in accordance with section 35(3)(b) without there being any reasonable grounds for believing that the case was one of urgency. Where the appeal is allowed the Chief Surveillance Commissioner must also quash any related order for the destruction of records.[225]

5.106 Even if the Chief Surveillance Officer dismisses an appeal he or she may modify the Commissioner's decision to quash or cancel the authorization, and any related decision for the destruction of records. To do so he or she must be satisfied that grounds exist to justify the quashing or cancellation of the authorization but that it should have been quashed or cancelled from a different time from that from which it was quashed or cancelled.[226]

212 ibid, s 37(6).
213 ibid, s 37(9)(a).
214 ibid, s 37(9)(b).
215 ibid, s 37(8).
216 ibid, s 37(8)(a); within the meaning of s 36(6).
217 ibid, s 37(8)(b).
218 Code of Practice, para 6.35.
219 RIPA, s 38(1)(a).
220 ibid, s 38(1)(b).
221 ibid, s 38(1)(c).
222 ibid, s 38(2); the relevant provisions are set in s 34(6).
223 ibid, s 38(4)(a); the grounds are set out in s 32(2)(a) and (b).
224 ibid, s 38(4)(b).
225 ibid, s 38(6).
226 ibid, s 38(5).

5.107 Notice of the determination of an appeal must be provided by the Chief Surveillance Commissioner to the person who brought the appeal and the Surveillance Commissioner who made the decision appealed against.[227] If the appeal is dismissed, a report must, in addition, be made to the Prime Minister.[228] No reasons must be given other than notification in any report and any matters that may be prejudicial to the prevention and detection of serious crime must also be excluded pursuant to section 107(3) and (4) of the Police Act 1997.[229]

5.108 Every member of a police force, SOCA and customs must comply with any request of a Surveillance Commissioner for documents or information required by that Commissioner for the purpose of enabling him or her to carry out his or her functions.[230]

Applications by the intelligence agencies, the Ministry of Defence and Her Majesty's forces

5.109 The authorization regime for the intelligence agencies, the Ministry of Defence and Her Majesty's forces[231] and any other designated public authority is different.[232] Applications for authorization are made to the Secretary of State and do not need the approval of the Surveillance Commissioner. Section 32 (the grounds and basis upon which authority may be granted) applies to the Ministry of Defence and Her Majesty's forces other than the grounds[233] upon which authorization may be granted by either organization are limited to the interests of national security and the prevention and detection of serious crime.

5.110 Where an intelligence agency applies for an authorization which is granted it must be by way of a Ministerial warrant.[234] This can combine an intrusive surveillance authorization and a warrant issued under the Intelligence Services Act 1994 (property interference)[235] but the two legislative regimes must be considered and applied separately in relation to the appropriate parts of the application before the Secretary of State.[236]

5.111 Applications by the Secret Intelligence Service (SIS or MI6) or GCHQ for an intrusive surveillance warrant may only be granted on the basis that it is necessary in the interests of national security or the economic well-being of the United Kingdom unless either are acting in support of a law enforcement agency in relation to the prevention and detection of serious crime.[237]

5.112 The functions of the Security Service (MI5) are extended by section 42 of RIPA. Providing it is acting within powers exercisable by SIS or GCHQ other than anything done in support of the prevention and detection of serious crime,[238] it may act on either agency's behalf in relation to any application for a Part II authority (ie not limited to intrusive surveillance) and if granted, carrying out the conduct authorized.[239]

[227] ibid, s 39(1)(a)–(b).
[228] ibid, s 39(2)(b).
[229] ibid, s 39(3) and (4).
[230] ibid, s 40.
[231] But excluding, in relation to the Ministry of Defence and Her Majesty's forces, their respective police forces who are governed by the provisions in relation to police forces.
[232] The provisions relating to designated public authorities are found in RIPA, s 41(4)–(6).
[233] ibid, s 32(3).
[234] ibid, s 42(1).
[235] See generally below Chapter 6, Property Interference.
[236] ibid, s 42(2).
[237] ibid, s 42(3).
[238] ibid, s 42(5).
[239] ibid, s 42(4).

5.113 All applications must provide, as a minimum, the information listed in the Code of Practice. This consists of the reasons why the authorization is necessary and the grounds upon which it is made, the nature of the surveillance, the residential premises or private vehicle if known, in relation to where surveillance is to take place, the identities of the targets of the surveillance if known, a description of the information it is hoped will be acquired, an assessment of collateral intrusion and its justification, details of any confidential information likely to be acquired and an assessment of the proportionality of the operation. A record of the decision and the date and time it was reached should be made and kept in relation to each application.[240]

5.114 If the case is urgent, in addition to the information required in the preceding paragraph which may be given orally, certain information must be recorded as soon as reasonably practicable including, the identities of the targets of the surveillance if known, the nature and location of the proposed surveillance, the reasons why the authorizing officer or the officer entitled to act considered the case appropriate to be treated as urgent and the reasons why it was not reasonably practicable for it to be considered by the authorizing officer.[241]

Duration, renewal and cancellation

5.115 An authorization may be granted or renewed orally in urgent cases[242] or otherwise must be granted in writing.[243] If an urgent authorization is granted orally, a record that the authorizing officer has expressly authorized must be kept by him or noted by the applicant.

5.116 If it is a combined application the separate provisions within RIPA must be considered as appropriate to those aspects of the application to which they relate.[244]

5.117 In general an authorization that was granted or renewed on the basis that it was urgent will cease to have effect after 72 hours from the time of granting or renewing it if it has not been renewed by someone with the authority to do so or was last renewed orally by such a person.[245] This is subject to a series of qualifications that appear in subsections and subsubsections of section 43 of RIPA.

5.118 Where the case is not urgent and relates to an authorization for the use and conduct of a covert human intelligence source, the authority will cease to have effect after a period of 12 months.[246] In the case of directed and intrusive surveillance authorizations that are not urgent, the authority will cease to have effect after a period of three months from the date it was granted or if renewed from the date of latest renewal.[247] There are different time periods for cases requiring Ministerial warrants involving the intelligence agencies.

5.119 The first qualification, itself subject to qualification (but in respect of covert human intelligence sources, so outside the scope of this chapter),[248] is that the authorization may be

[240] Code of Practice, para 6.19.
[241] ibid, para 6.20.
[242] RIPA, s 43(1)(a); note that the person who grants or renews it must be entitled to do so in cases other than urgent cases, although the reasons for this are confusing.
[243] ibid, s 43(1)(b).
[244] ibid, s 43(2).
[245] ibid, s 43(3)(a).
[246] ibid, s 43(3)(b); see also below Chapter 7, Covert Human Intelligence Sources.
[247] RIPA, s 43(3)(c).
[248] See below Chapter 7, Covert Human Intelligence Sources.

renewed before it ceases to have effect by someone entitled to grant it.[249] Renewals are, naturally, subject to the same provisions (sections 28–41 of RIPA) that applied to the substantive authorization.[250]

5.120 The second qualification is that the Secretary of State may by order later provide a different time period within which authorizations cease to have effect.[251]

5.121 The time of the commencement of an authorization is dealt with in section 43(9). Other than cases where authorization requires prior approval in writing of a Surveillance Commissioner,[252] an authorization takes effect on the day it was granted at the time it was granted[253] and a renewal the day the authorization would have ceased to have effect but for the renewal.[254] Where the authorization or renewal requires prior approval from a Surveillance Commissioner it takes effect on the day and at the time it is approved and written notice has been given to the person who granted the authorization.[255]

5.122 There are special rules over and above those covered above in relation to authorities granted by or warrants issued to the intelligence agencies.[256] Only the Secretary of State can issue or renew a warrant containing an intrusive surveillance authorization.[257] In urgent cases where the Secretary of State has expressly authorized the issue of a warrant, it may be issued (but not renewed) by a senior official.[258] In such circumstances if it is not renewed the warrant will cease to have effect at the end of the second working day following the day of issue[259] (as opposed to the 72 hours in other cases).[260]

5.123 A warrant that has not been renewed ceases to have effect after a period of six months beginning with the day it was issued.[261] Where renewed, at the end of the period of six months beginning with the day on which it would have ceased to have effect if not renewed again.[262] The same time periods apply to directed surveillance. Any renewal must be endorsed by the person entitled to renew confirming that he or she believes that the, or one of the grounds upon which it was granted continues to exist.[263] A warrant for this purpose includes a combined authorization to carry out directed and intrusive surveillance.[264]

5.124 Any applications for renewal must include details of any previous renewals, any significant changes to the facts upon which the original application was based, the reasons why it is necessary to continue with the surveillance, an assessment of the content and value of the

[249] RIPA, s 43(4).
[250] ibid, s 43(5).
[251] ibid, s 43(8).
[252] ibid, s 43(9)(a); per s 36(2).
[253] ibid.
[254] ibid, s 43(9)(b).
[255] ibid, s 43(9)(c).
[256] ibid, s 43(10).
[257] ibid, s 44(1).
[258] ibid, s 44(2).
[259] ibid, s 44(3).
[260] ibid.
[261] ibid, s 44(4)(a).
[262] ibid, s 44(4)(b).
[263] ibid, s 44(5)(a)–(b).
[264] ibid, s 44(7).

intelligence gathered so far and the results of any review.[265] There is no limit on the number of renewals providing the criteria are met.[266]

5.125 The Secretary of State may by Order change the periods of time within which an authorization may cease to have effect.[267]

5.126 An authorization or renewal must be cancelled by the person who granted or renewed it (or a person entitled to act or that person's deputy)[268] if he or she is satisfied that the requirements which were met when it was granted or renewed are no longer satisfied.[269] The Secretary of State is empowered to make regulations to provide for the procedure to be adopted where the person is no longer available.[270] Once an authority has been cancelled instruction should be given to those involved to stop carrying out the surveillance. The date the authorization was cancelled should be centrally recorded and the documentation retained.[271] The Surveillance Commissioner must be notified of the cancellation.[272]

5.127 There are restrictions that apply to conduct that may take place in Scotland. No authorization or renewal can be granted unless it relates to the protection of national security or the economic well-being of the United Kingdom[273] and all of the conduct authorized is likely to take place in Scotland.[274] The public authorities capable of doing so are set out in section 46(3) and include the intelligence agencies, the Ministry of Defence, Her Majesty's forces, Customs and the British Transport Police. Otherwise the Regulation of Investigatory Powers (Scotland) Act 2000 applies.

5.128 The Secretary of State is empowered to modify the descriptions of what may amount to surveillance that is neither directed nor intrusive surveillance or provide that any description of directed surveillance to be treated for the purposes of this Part as intrusive surveillance by Order that can only be made under this section unless a draft of it has been laid before Parliament and approved by a resolution of each House.[275]

E. Other Matters Relating to Authorization

Record keeping

5.129 There is guidance as to the retention of records. Every public authority must maintain a centrally retrievable record of directed and intrusive authorizations for a period of at least three years from the time at which an authorization ceases to have effect. The record must be made available to the Office of the Surveillance Commissioner on request. The record should contain the type and date of authorization, the name and rank of the authorizing officer and

[265] Code of Practice, para 6.30.
[266] ibid, para 6.31.
[267] RIPA, s 44(6).
[268] ibid, s 45(2)(a)–(b); the list of such persons is set out in s 45(6).
[269] ibid, s 45(1)(a)–(b).
[270] ibid, s 45(4).
[271] Code of Practice, para 6.33.
[272] ibid, para 6.34.
[273] This provision is cryptically set out in ibid, s 46(2) and seeks to limit the activity in Scotland of those public authorities acting other than on these grounds.
[274] ibid, s 46(1)(a)–(b).
[275] ibid, s 47.

whether he was directly involved in the operation, the unique reference number, the operational name and a brief description of the targets if known, whether the authorization was treated as urgent and if so why, details of any renewals, whether confidential information was acquired and the date on which the authorization was cancelled.[276]

5.130 In addition there is a requirement to retain documentation, including the application and authorization and any subsequent related documentation, a record of the period of which surveillance took place, the number of reviews as prescribed by the authorizing officer and the record of any reviews that took place, any renewal and supporting documentation, the date and time when surveillance ceased as well as the date and time of any other instruction given by the authorizing officer.[277]

5.131 The public authority must also ensure there are arrangements for the secure handling, storage and where appropriate destruction of the product of directed and intrusive surveillance deployments. The intelligence agencies must ensure that arrangements exist that ensure no information is held other than is necessary for the discharge of their statutory functions.[278] The Data Protection Act 1998 (DPA)[279] and Criminal Procedure and Investigations Act 1996 apply.[280] Material obtained through the deployment of directed or intrusive resources may be used in connection with other investigations.[281]

Special circumstances arising during the authorization process

Legal professional privilege

5.132 There are a number of circumstances that need to be considered in relation to the use of covert surveillance resources, principally the potential or actual acquisition of confidential and privileged material.

5.133 The issue of privilege in the context of covert policing operations generally is discussed further below in Chapter 9.

5.134 RIPA makes no provision for the acquisition of privileged material and the House of Lords has recently interpreted this as permissive.[282] The Code of Practice emphasizes that 'particular care' should be taken in cases which it categorizes as involving a high degree of privacy or where the acquisition of confidential material, defined as including legal and journalistic privilege and confidential personal information may be at stake.[283] Legal professional privilege is given the definition set out in section 98 of the Police Act 1997, or in Scotland the definition contained in section 33 of the Criminal Law (Consolidation) (Scotland) Act 1995. In Northern Ireland the definition is the same as that provided for in Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989.

5.135 This is an unfortunate or careless use of the English language; the activities of public authorities engaging in the use of *any* of the covert resources available to them under RIPA deserve particular care being exercised in relation to their use. Assuming compliance with the

[276] Code of Practice, para 8.1.
[277] ibid, para 8.2.
[278] ibid, para 9.7.
[279] ibid, para 9.3.
[280] ibid, paras 9.4 and 9.6.
[281] ibid, para 9.5.
[282] *Re McE* [2009] UKHL 15.
[283] Code of Practice, 81.

Act and the Code of Practice, the issue in the present context is one of proportionality. Where confidential material is likely to be acquired a higher level of authority is required.[284] Following *Re McE* the level of authorization in such cases ought to be the same as intrusive surveillance, although at the time the case was heard by the Supreme Court the appropriate Order had yet to be placed before Parliament. This was the subject of some criticism in *Re McE*.[285]

5.136 The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 gives effect to the decision in *Re McE*.[286] In summary, directed surveillance that is likely to capture the content of legal consultations must be treated for the purposes of Part II of RIPA as intrusive surveillance.

5.137 Legal consultation is a narrower concept than legal privilege, a matter that is likely to cause confusion to an already confused area of the law. It is defined as:

(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.[287]

5.138 If this is not problematic enough, there is no distinction between consultations that may be wholly or partly protected by legal privilege and those which take place in the furtherance of a criminal purpose (and therefore matters that would not attract the protection of privilege, such as it is now after *Re McE*.[288] This is an extraordinary position which at least in theory could lead to a large number of consultations taking place that are covertly recorded but where nothing of relevance is obtained. The material in such circumstances remains privileged (as the Code of Practice accepts)[289] and the risk that investigating teams may come into possession of material that they should not have is significantly increased. Where it does, the implications are potentially catastrophic. This can be illustrated by reference to actual cases. In *R v Sutherland*[290] police had installed listening devices at two police stations in Lincolnshire. Contrary to the terms of the authorizations, the devices were installed in the exercise yards where it was accepted that it was common practice for solicitors to hold consultations with their clients, since this was the only place they could smoke. Consequently, the risk of picking up conversations attracting legal professional privilege was high and in fact occurred. The authorizations expressly stated that the risk of picking up confidential material was low. After a lengthy voir dire Newman J concluded that officers had been dishonest in the deployment, dissemination and retention of the privileged material obtained. An indictment containing counts of murder and conspiracy to murder was stayed. In a later case emanating from the same area and where the same officers were involved, the rationale of the trial judge was approved by the Court of Appeal in *R v Grant*.[291]

[284] Set out in Annex A of the Code of Practice.
[285] [2009] UKHL 15.
[286] ibid.
[287] Code of Practice, para 4.6.
[288] [2009] UKHL 15.
[289] Code of Practice, para 4.9.
[290] (Unreported) 29 January 2002.
[291] *R v Grant* [2005] EWCA Crim LR (Nov). See also Ormerod and Waterman, 'Abusing a Stay for Grant?' [2005] Covert Policing Review 5–14.

5.139 The decision in *Re McE*[292] did not consider *Grant* and, as is discussed below in Chapter 9, it is difficult to reconcile the two decisions. Nor did it consider other authorities of relevance. In *R v Robinson*[293] for example, the Court of Appeal considered the propriety of the police using solicitors or their clerks as sources. In this case, which related to significant and widespread legal aid fraud by a solicitor and where the police had used an employee of the firm as a source, the court reiterated the sanctity of legal privilege by relying on the dicta of Lord Bingham of Cornhill in *R (Daly) v Secretary of State for the Home Department*:[294]

> Among the rights which, in part at least, survive are three important rights, closely related but free-standing, each of them calling for appropriate legal protection: the right of access to a court; the right of access to legal advice; and the right to communicate confidentially with a legal adviser under the seal of legal professional privilege. Such rights may be curtailed only by clear and express words, and then only to the extent reasonably necessary to meet the ends which justify curtailment.[295]

5.140 The court then considered it a serious breach of legal privilege by the solicitor or his clerk and, if encouraged by the police, an infringement of a defendant's or suspect's rights if they were committed or were induced to commit the breach. The Crown did not resist the lack of integrity that surrounded the practice but the Chief Constable of Gloucestershire Police intervening (at the court's invitation) relied on the then Code of Practice in relation to the conduct and use of covert human intelligence sources. At paragraph 3.5 the Code stated:

> The 2000 Act does not provide any special protection for legally privileged information. Nevertheless, such information is particularly sensitive and any source which acquires such material may engage article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the right to a fair trial) as well as article 8.

5.141 The Court in *Robinson*[296] expressed concern about the use of covert human intelligence sources in this area. It received reassurance from the Chief Constable's counsel that the references to *Daly* were kept in mind and that the risk assessments carried out were 'fraught with danger'. It emphasized the need for members of the public to be able to obtain legal advice without the danger that these confidential communications would pass between their lawyers and the police. It also recognized that privilege did not extend 'to communications made with the intention of furthering a criminal purpose'[297] and that decisions to deploy sources in this area would be difficult ones.

5.142 Moreover, the decision in *Re McE*[298] is clearly incompatible with Strasbourg jurisprudence on the issue.[299] In *Kopp v Switzerland*[300] a lawyer's telephone communications were intercepted on the basis that he had contact with the subjects of the investigation. The Court held that the law in Switzerland did not make it clear how legal professional privilege was protected in practice. The current position in this jurisdiction is now significantly worse being both confusing and arguably representing no protection at all. A challenge to Strasbourg

[292] [2009] UKHL 15.
[293] The Times, 13 November 2002.
[294] [2001] 2 AC 532.
[295] ibid, paras 537–8.
[296] The Times, 13 November 2002.
[297] Former Code of Practice, para 3.4.
[298] [2009] UKHL 15.
[299] See, by way of one example, *S v Switzerland* (1991) 14 EHRR 667, ECtHR.
[300] (1998) 27 EHRR 91.

seems as likely as the outcome predictable unless the Supreme Court is prepared to re-visit the issue. However, at the time of writing the position remains as set out in the Code of Practice.

5.143 The Code of Practice provides details of what it describes as the 'tests to be applied when authorising covert surveillance . . . likely or intended to result in the acquisition of knowledge of matters subject to legal privilege'.[301] No test is in fact set out, rather there is a series of four requirements. First, any application that if granted is likely to result in the acquisition of privileged material should specify whether this is intentional.[302] If it is likely but not intentional (and therefore arguably still intentional) then the application should set out the steps that will be taken to mitigate the risks of acquiring it and how it will be handled if still acquired (ie how it will be ensured that anyone connected to the investigation or prosecutor does not have access to it).[303] Thirdly, if the acquisition of the material is intentional, the authorizing officer, Surveillance Commissioner or Secretary of State must be satisfied there are exceptional and compelling circumstances that make it necessary to do so.[304] Fourthly, they must also believe it is proportionate to what is sought to be achieved.[305]

5.144 Interestingly, 'exceptional' and 'compelling' are given different meanings depending on whether the acquisition is intended or not. In the case of the former it includes the existence 'of a threat to life or limb' a somewhat casual and ambiguous term which may be difficult to satisfy the exacting standards arising out of the jurisprudence on necessity[306] and national security. In the latter category, national security, the economic well-being of the United Kingdom and the prevention and detection of serious crime are all capable of justifying what is described as the unintentional acquisition of privileged material.

5.145 The Code of Practice sets out the position in relation to the use and handling of privileged material.[307] Nothing in *Re McE*[308] changes the evidential status of privileged material; it remains inadmissible. Where there is any doubt about the nature of the material acquired, legal advice must be sought before any dissemination takes place. The material should be clearly marked as legally privileged. It should be protected to a high level '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'.[309]

5.146 This is an extraordinary state of legal affairs which has derived from a decision that the Supreme Court was asked to decide in questionable circumstances (the appellants had in fact succeeded in the court below) and in the absence of significant and material authorities. That an issue of such constitutional importance is then eroded yet further in secondary legislation assisted by a poorly drafted Code of Practice is unacceptable. It is an area that requires to be urgently reviewed again by the higher courts or it may, without fear of hyperbole, endanger the integrity of the criminal justice system.

[301] Code of Practice, 38.
[302] ibid, para 4.10.
[303] ibid, para 4.11.
[304] ibid, para 4.12.
[305] ibid,,para 4.13.
[306] See above Chapter 2, Privacy, Proportionality and Other Human Rights Principles.
[307] Code of Practice, paras 4.22–4.26.
[308] [2009] UKHL 15.
[309] Code of Practice, para 4.26.

Other confidential information

5.147 There are special provisions in relation to journalistic material and confidential personal information. The latter is defined in the Code of Practice as information 'held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it'.[310] Spiritual counselling means conversations between an individual and a minister of religion acting in an official capacity. The individual being counselled must be seeking or the minister must be imparting 'forgiveness, absolution or the resolution of conscience with the Devine Being(s) of their faith'.[311]

5.148 Confidential journalistic material is defined as including 'material acquired or created for the purpose 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'.[312] There is no reference in RIPA and there was none in the former Code of Practice in relation to privilege arising out of the relationship between a Member of Parliament and a member of the public. The revised Code of Practice now deals with it expressly and extends the protection of confidentiality to 'communications between a Member of Parliament and constituent in respect of constituency matters'.[313]

5.149 The view of one respected commentator is that the Code of Practice 'fails to introduce any independent check into the process even where the material is not most clearly of a private nature'.[314] This is a fair criticism and another area where RIPA and the Code of Practice are found wanting.

F. Overt Photography, CCTV and Related Issues

Photography

5.150 Taking photographs of persons or places overtly inexorably falls outside the legislative regime that governs covert policing. The determinative element of whether RIPA is engaged in an activity that is either directed or intrusive surveillance is its covert nature.[315] This does not prevent arguments that RIPA applies being made even if they are unsuccessful as in *R v Rosenberg*[316] for example. But this is not the end of the matter; such activities may amount to surveillance within the meaning of section 48(2). Police and other public authorities in terms of the legislation at the very least have the aspiration to act lawfully and will be vulnerable legally if they do not. The Code of Practice may lure them into a false sense of security stating implacably as it does, if there is no interference with privacy, there is no need to seek authorization.[317] The problem is not necessarily a breach of RIPA but the inability to authorize in accordance with law any surveillance other than that which is carried out covertly since no law in fact governs it.

[310] ibid, para 4.28.
[311] Code of Practice, para 3.11.
[312] ibid, fn 30.
[313] ibid, para 4.29.
[314] H Fenwick, *Civil Liberties and Human Rights*, 3rd edn (Cavendish, 2005) 701.
[315] RIPA, s 26(2) and (3).
[316] [2006] EWCA Crim 6.
[317] Code of Practice, para 1.14, eg.

5.151 The usefulness of the present state of the law in this area is threefold. First, as discussed at length above in Chapter 2, the cases are instructive as to the approach to take in order to determine whether there is an interference with privacy (the test is the same, whether the conduct is covert or not). Secondly, it alerts public authorities to the fact that if they engage in activity that is an interference with privacy they are exposed to a claim under the Human Rights Act 1998 (HRA) and/or the common law for damages, although it is unlikely to impact on admissibility. Thirdly, it identifies a legislative lacuna that needs to be filled, just as it did in relation to the interception of communications and other forms of surveillance.

5.152 The Strasbourg position was considered in 1996 by SH Naismith, Solicitor to the Secretariat of the European Commission of Human Rights, in 'Photographs, Privacy and Freedom of Expression'.[318] It remains a current analysis of the key principles governing this area, subsequent cases simply re-stating the position[319] or confirming Naismith's predictions as to how the law would evolve.[320]

5.153 The test, in terms of whether Article 8 of the European Convention on Human Rights (ECHR) is engaged by virtue of a public authority taking a photograph of an individual is twofold. First, did the taking of the photograph involve an invasion of privacy in a restricted sense (for example, trespass to property) and was it whilst the person was engaged in a private or public act? Secondly, the ECHR requires an analysis of the purpose, use and dissemination of the photographs.

5.154 An example of the first type of case is *Jones v University of Warwick*,[321] although sadly it was not considered as such by the Court of Appeal. The claimant had suffered an injury at work. Her employers engaged the services of private enquiry agents to undertake surveillance of her as they suspected she was exaggerating the impact the injury may have had on her ability to work. Agents attended her address and gained admittance by deception, purporting to be carrying out market research. They filmed her secretly and sought to rely on the footage as evidence of her dishonesty. In due course she applied to exclude the evidence. The District Judge excluded the evidence but this was reversed on appeal. This ruling was upheld by the Court of Appeal but the judgment did not take the more sophisticated approach advocated by Naismith and the case is authority less on the question of the principles to be applied to such cases and more on the question of censuring parties to litigation engaging in ambush tactics.[322] An approach, if not principles, can be identified from the judgment.[323] First, each case will always be determined on its own facts and in resolving the competing public interests the weight to be attached to each will vary according to the circumstances. The significance of the evidence will differ as will the gravity of the breach of Article 8, according to the facts of the case. The decision on whether to admit the evidence or not will depend on all the circumstances.

Wood v Commissioner of Police for the Metropolis[324]

5.155 An example of the second type of case is *Wood v Commissioner of Police for the Metropolis*.

318 [1996] EHRLR, Issue 2, 150.
319 See, eg, *Peck v The United Kingdom*, Application No 44647/98, ECHR 2003.
320 See, eg, *Von Hannover v Germany* (2005) 40 EHRR 1.
321 [2003] EWCA Civ 151.
322 ibid, para 30.
323 ibid, para 28.
324 [2009] EWCA Civ 414.

5.156 The claimant, Wood, a member of the Campaign against the Arms Trade was photographed leaving the annual general meeting (AGM) of a company concerned in the organization of trade fairs for industries including the arms industry. He had acquired shares in the company for the sole purpose of being eligible to attend the AGM. Other individuals had also done so and had previously caused incidents of a criminal nature at exhibitions and property owned by the company. These individuals were also in attendance and known to the claimant, who spoke to them at the AGM. The claimant himself had no previous convictions and had never been arrested for an offence.

5.157 After leaving the meeting the claimant was not only photographed but was also followed and spoken to by police officers. Enquiries were also subsequently made in order to ascertain the claimant's identity.

5.158 The Court of Appeal held that the mere taking of an individual's photograph in a public street itself breaches no rights, 'unless something more is added'.[325] This 'something more' was later described as 'aggravating circumstances'. These included harassment and hounding and possibly assault.[326]

5.159 The 'real issue' was 'whether the taking of the pictures, along with their actual and/or apprehended use, might amount to a violation'.[327] It is noteworthy, since it is consistent with the Strasbourg approach, that the Court of Appeal did not draw a distinction between the act of taking the picture and its use and retention—such a view was considered 'too simplistic'.

5.160 A distinction was drawn between the facts in *Wood*[328] and the two leading Strasbourg authorities on the issue, *X v United Kingdom*[329] (photographs taken of the applicant at a public demonstration at which she was voluntarily attending and retention limited for the purposes for which they were taken) and *Friedl v Austria*[330] (photographs of the applicant taken at a public demonstration with assurances from the government that they were anonymous, retained for the sole purpose for which they were taken and not processed). The Court was unanimous that Article 8(1) was engaged, although was divided on whether Article 8(2) was satisfied.

5.161 It was not in issue that the taking of the photographs was in the pursuit of a legitimate aim (prevention and detection of crime). Nor was there significant disagreement on the question of whether the activities of the police were in accordance with the law.[331] It was ultimately an issue of proportionality.

5.162 In the view of the majority, the taking and retention of the photographs by the police was disproportionate and Article 8(2) was not satisfied. The interference was sought to be justified on the grounds of protecting the community from low level criminality or the risk of public disorder, no offence had been committed at least as far as the appellant was concerned so there was no basis to retain the photographs, a position that was not likely to change weeks

[325] ibid, para 35.
[326] ibid, para 36.
[327] [2009] EWCA Civ 414, para 38.
[328] [2009] EWCA Civ 414.
[329] Application No 5877/72 (1973).
[330] (1996) 21 EHRR 83.
[331] Dyson LJ, ibid, at paras 80 and 81, expressed 'reservation' about Law LJ's analysis of *R (Gillan) v Commissioner of Police for the Metropolis* [2006] UKHL 12; [2006] 2 AC 307.

or even months after the AGM had taken place. Furthermore, trouble-makers had in fact been ejected from the meeting and these did not include the appellant. If there had been a justification for keeping the photographs based on the conversation the appellant had with one of the protagonists, this could only have been for a few days after the meeting had taken place.[332]

5.163 The judgment in *Wood* established a 'cluster of values' inherent in Article 8 that were balanced against the need that they are not 'read so widely that its claims become unreal and unreasonable'.[333] Three safeguards, or qualifications to Article 8 claims existed; antidotes to the risk of its overblown use. First, the actual, proposed or alleged threat to an individual's personal autonomy must attain 'a certain level of seriousness'. Secondly, adopting the terminology in *Campbell v MGN Limited*,[334] the touchstone for Article 8(1)'s engagement is whether on the facts, the individual concerned has a reasonable expectation of privacy, without which there is no interference that falls to be considered. Finally, the scope of Article 8(1) is curtailed in certain circumstances by the justifications available to the state under Article 8(2).[335]

Campbell v Mirror Group Newspapers Limited[336]

5.164 The most significant decision in this area remains *Campbell*, a case involving the publication of details, including photographs taken covertly of supermodel Naomi Campbell's attendance at Narcotics Anonymous. The claim was based on breach of confidence and a claim for damages under the Data Protection Act 1998.

5.165 The House of Lords identified a test for whether the activity in question amounted to a breach of privacy. Lord Hope considered the 'touchstone of private life' to be whether in the circumstances of the case, the 'person in question had a reasonable expectation of privacy'.[337]

5.166 The test is twofold; the acquisition of the material and then the publication or disclosure of it. If the material is obviously private, then it follows that it is likely to be highly offensive to proceed to publication and/or disclosure of it. As Randerson J stated in *Hosking v Runting*,[338] 'the taking of photographs in a public street must be taken to be one of the ordinary incidents of living in a free community'. The real issue is whether publicizing the content of the photographs would be offensive.[339] The test is also an objective one. In order to assess whether the disclosure would be objectionable it is necessary 'to put oneself into the shoes of a reasonable person who is in need of that treatment'.[340] Questions of proportionality will arise, collateral intrusion, indeed the use and effect of acquiring the information obtained.

5.167 The decision in *Campbell* has, unsurprisingly, since been applied in a number of cases.[341] In *Murray v Big Pictures (UK) Limited*,[342] the child of Joanne Murray (otherwise known as author JK Rowling) brought proceedings against the defendant company for a breach of

[332] ibid, paras 86–90.
[333] ibid, para 22.
[334] [2004] UKHL 22.
[335] ibid, para 22.
[336] [2004] UKHL 22.
[337] [2004] UKHL 22, para 21.
[338] [2003] 3NZLR 385.
[339] ibid, para 165.
[340] ibid, para 98, fn 142.
[341] *McKennitt v Ash* [2006] EWCA Civ 1714; [2008] QB 73.
[342] [2008] EWCA Civ 446.

confidentiality as his right to respect for privacy had allegedly been infringed following the publication of a photograph of the child with his parents which was published by the *Sunday Express* Magazine. The claim was struck out at first instance but was the subject of an appeal as a result of the decision in *Van Hannover v Germany*[343] which raised an important point about the relationship between that case and *Campbell*,[344] notwithstanding that as a matter of law where there is a conflict between the two decisions, the Court of Appeal is bound to follow the domestic decision.[345]

5.168 After some review of the dissenting opinion in *Campbell*, the Court of Appeal was able to identify some commonality between the totality of the appellate committee, at least as to what the first limb of any test should be:

> In these circumstances, so far as the relevant principles to be derived from Campbell are concerned, they can we think be summarised in this way. The first question is whether there is a reasonable expectation of privacy. This is of course an objective question. The nature of the question was discussed in Campbell. Lord Hope emphasised that the reasonable expectation was that of the person who is affected by the publicity. He said at [99]: 'The question is what a reasonable person of ordinary sensibilities would feel is she was placed in the same position as the claimant and faced with the same publicity'. We do not detect any difference between Lord Hope's opinion in this regard and the opinions expressed by the other members of the appellate committee.[346]

5.169 The Court of Appeal in *Murray* provided further guidance:

> As we see it, the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case. They include the attributes of the claimant, the nature of the activity in which the claimant was engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant in which and the purposes for which the information came into the hands of the publisher.[347]

5.170 The principles set out above need as a minimum to form part of a public authority's policy on the circumstances under which photographs may be taken by them (which should be accessible to members of the public) and to what use they may be put as well any retention or destruction protocols that exist. But they can be sensibly imported across to covert policing operations in determining whether the public authority is engaging in activity likely to interfere with privacy rights. Public authorities will need to risk-manage the inevitable increase in civil actions where their activities meet the *Wood* criteria. Finally it should be a call to action to place such activities on a proper legislative footing.

CCTV

5.171 CCTV (closed circuit television) is in fact a misnomer, most systems not being closed circuit and networked digitally[348] but it remains a convenient term that is easily understood by the general public. It is not necessarily covert but where it is used as part of a specific investigation

---

[343] (2005) 40 EHRR 1.
[344] [2004] UKHL 22.
[345] *Kay v Lambeth LBC* [2006] UKHL 10; [2006] 2 AC 465.
[346] *Murray v Big Pictures Limited* [2008] EWCA Civ 446, para 35.
[347] ibid, para 36.
[348] Royal Academy of Engineering, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*, March 2007,

or covert operation it may require a directed surveillance authorization pursuant to RIPA.[349] The same principle applies to the use of automatic number plate recognition.[350]

5.172 The Venice Commission[351] in its report on *Video Surveillance in Public Places by Public Authorities and the Protection of Human Rights*[352] concluded that:

> Video surveillance of public places by public authorities or law enforcement agencies can constitute an undeniable threat to fundamental rights such as the right to privacy and the right to respect for his or her private life, home and correspondence, his/her right to freedom of movement and his/her right to benefit from specific regarding personal data collected by such surveillance.[353]

5.173 The Commission made a number of recommendations, including the enactment of specific regulations at both a national and international level[354] which should incorporate compliance with Article 8 and observance of Directive 95/46/EC.[355] In addition, it recommended that the public should be notified of surveillance in public places unless obvious and a specific independent authority established as in the Contracting States of France, Italy and Netherlands.[356]

5.174 These issues are not the musings of a discrete EU think tank. The civil liberties organization JUSTICE have expressed concern about CCTV more generally and the United Kingdom's 'dubious reputation' in this area, including the country's number of CCTV cameras per capita[357] and the inadequacy of existing legislation to protect privacy rights.[358]

5.175 There is no legislative basis for the use of CCTV in the United Kingdom. It is governed *post facto* by DPA, which unlike RIPA, is not permissive (facilitating and authorizing the use of CCTV) but requires the individual to be proactive (by making a complaint or bringing an action under DPA). There is a Code of Practice[359] which provides guidance and advice for CCTV users on how to comply with DPA and includes a checklist for users of some systems.[360]

5.176 The expectation of privacy an individual has in private is qualitatively different to that which they enjoy in public places but where there is no attempt to identify individuals from the images and they are not entered into a data processing system, there is unlikely to be an interference with privacy.[361] As Fenwick has observed, 'even where it is arguable that an invasion of privacy has not occurred, the use of the information later on may create one'.[362] The expectation extends to companies as well as individuals so the unjustified filming on a

[349] Code of Practice, para 2.28.
[350] ibid.
[351] Council of Europe, European Commission for Democracy through Law.
[352] CDL-AD(2007)014, 23 March 2007.
[353] ibid, para 79.
[354] ibid, para 81.
[355] ibid, para 82.
[356] Council of Europe, European Commission for Democracy through Law, para 83.
[357] The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their relationship with the State, submission to the House of Lords Constitution Committee, June 2007.
[358] ibid, para 16.
[359] CCTV Code of Practice (2008).
[360] It is available on the Information Commissioner's website <http://www.ico.gov.uk>.
[361] *Friedl v Austria* (1996) 21 EHRR 83.
[362] H Fenwick, *Civil Liberties and Human Rights*, 3rd edn (Cavendish, 2005) 703.

company's premises could amount to an interference with privacy, particularly where they are not asked to consent or expressly withhold it.[363]

Peck v The United Kingdom[364]

5.177 The leading judgment on the legality of CCTV is *Peck v United Kingdom*. The applicant had been filmed by CCTV operators employed by Brentwood Borough Council walking down Brentwood High Street carrying a knife (he was attempting to commit suicide). The police were contacted who arrived at the scene, disarmed him and later detained him under the Mental Health Act 1983. He was subsequently released without charge.

5.178 The council published two still and unedited photographs of Mr Peck in a press bulletin concerned with advancing the positive aspects of using CCTV in the community. One of these appeared in an edition of the Brentwood Weekly News and another local newspaper. Later, elements of the footage appeared on local television and then national broadcasts. The highest audience viewing figures for one of the programmes was 9.2 million. There had been some attempt to mask Mr Peck during the later broadcasts but this was inadequate. Neighbours, friends and family of the applicant told him they had seen him on television. Mr Peck lodged a complaint with the Broadcasting Standards Commission alleging that the publication of the photographs and footage were a breach of his right to privacy.

5.179 His complaint was upheld and apologies were published and broadcast. A further complaint to the Independent Television Commission was also upheld. However a complaint to the Press Complaints Commission was rejected on the basis that, since the events took place in public, there could be no infringement of Mr Peck's privacy.

5.180 The decision of the Press Complaints Commission was the subject of an application for judicial review. The High Court dismissed the application on the ground that the local authority concerned had acted lawfully. The application was determined prior to HRA coming into force and the court conceded that the position may have been different had the Act applied.

5.181 Mr Peck petitioned the European Court of Human Rights (ECtHR) alleging a breach of Article 8 arising out of disclosure of the CCTV footage, which had led to their widespread publication by the local and national media.

5.182 Upholding his application, the court held that although the monitoring of individuals by CCTV cameras which did not record the data did not in itself give rise to an interference with private life, the systematic recording or creation of a permanent record of the data did and as such a breach of Article 8(1) arose on the facts of the case. Although Mr Peck was in a public street at the material time, he was not participating in a public event,[365] nor was he a public figure.[366] There had been no effective attempt to prevent his being identified. In addition the dissemination of the data was very considerable, particular that which had been broadcast on television.

5.183 The next consideration for the Court was whether the interference was justified under Article 8(2). It was accepted that the disclosure had a proper legal basis and was therefore in

[363] *R v Broadcasting Standards Commission, ex parte, British Broadcasting Corporation* [2000] 3 WLR 1327.
[364] Application No 44647/98, para 57, ECHR 2003.
[365] As in the *Friedl v Austria* judgment of 31 January 1995, Series A no 305-B.
[366] *Von Hannover v Germany* (2005) 40 EHRR 1.

accordance with the law. However, the justification failed on proportionality grounds. It was possible to advance the cause of CCTV by using the footage but this could have been done without disclosing Mr Peck's identity. There were not relevant or sufficient reasons for the disclosures being made in the circumstances. He was not a public figure and had no public role. Nor was he a criminal or a missing person; the objective behind showing the footage could have been achieved by using less intrusive images or by suitably masking Mr Peck's identity.

5.184 There are a number of issues arising out of the use of CCTV, particularly in light of the decision in *Wood* (acquisition not unlawful, use and retention an interference with privacy not in accordance with law) which have implications for covert and other operations, although more in terms of civil liability than the admissibility of evidence. The increasing attempts to import RIPA into the sphere of private relationships as illustrated by cases like *Rosenberg*[367] and *Leadbetter*[368] is a developing area, likely to be the subject of a number of future challenges. As with the decisions relating to photographs, the law in this area is instructive to evolving methodology of approach in terms of operational planning.

Surveillance of employees

5.185 Surveillance of employees falls outside the compass of RIPA and is essentially an issue of employment law. Employee calls may be lawfully intercepted without external authorization under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[369] for the purposes of investigating unauthorized use, or establishing facts and checking compliance for example.[370] The only requirement is that it is undertaken for the sole purpose of monitoring or keeping records relevant to the business, that the system is used partly or wholly in connection with the business and all reasonable efforts have been made to inform those who may use the system that communications may be intercepted.[371]

5.186 The Data Protection Code on Employment Practices also applies.[372] This imposes obligations to assess the need to monitor, including whether the objective could be achieved by other means. There are notification requirements so that employees know what constitutes an unacceptable use of email, the internet and telephone calls. Employees should also know when monitoring may be carried out and are reminded of the existence of the policy and any changes to it. There are also rules about the circumstances under which covert monitoring can be undertaken.[373]

5.187 As has already been discussed, RIPA does not apply to a public authority's ordinary functions.[374]

Admissibility

5.188 The question of admissibility is considered in detail below in Chapter 9. There have been a small number of decisions involving breaches or alleged breaches of RIPA. Broadly speaking, where the

[367] [2006] EWCA Crim 6.
[368] (Unreported) decided by District Judge Parsons in Bournemouth Magistrates Court on 4 November 2009.
[369] SI 2000/2699.
[370] ibid, reg 3(1).
[371] ibid, reg 3(2).
[372] Available on the Information Commissioner's website, <http://www.ico.gov.uk>.
[373] Part 3 of the Data Protection Code on Employment Practices.
[374] *C v Police and Secretary of State*, 14 November 2006, IPT/03/32/H.

breaches have been made in good faith, the evidence has not been excluded. In *R v Linda Rosenberg*[375] the appellant was convicted of drug-related offences and appealed on the basis that the trial judge had erred in admitting CCTV footage passed to the police by her neighbours. It was the appellant's case that the surveillance ought to have been authorized under Part II of RIPA. The Court of Appeal held that the nature of the surveillance could never be considered covert for the purposes of section 29(9)(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 surveillance are unaware that it is or may be taking place').[376] Even if the trial court was satisfied that there had been a breach of Article 8, the judge would have been entitled to admit it since it was, on carrying out the necessary review, fair to admit it. The Court was not invited to consider the European jurisprudence in the area and the arguments before it were not particularly sophisticated. There was no consideration of section 80. Nor was there was no attempt to explore whether the relationship the police shared with the Brewers may have amounted to use and conduct of covert human intelligence sources, which—based on the facts as revealed by the judgment—it may have been.

5.189 In *R v Sutherland*[377] police had installed listening devices at two police stations in Lincolnshire. Contrary to the terms of the authorizations, the devices were installed in the exercise yards where it was accepted that it was common practice for solicitors to hold consultations with their clients, since this was the only place they could smoke. Consequently, the risk of picking up conversations attracting legal professional privilege was high and in fact occurred. The authorizations expressly stated that the risk of picking up confidential material was low. After a lengthy voir dire Newman J concluded that officers had been dishonest in the deployment, dissemination and retention of the privileged material obtained. An indictment containing counts of murder and conspiracy to murder was stayed. In a later case emanating from the same area and where the same officers were involved, the rationale of the trial judge was approved by the Court of Appeal.[378]

5.190 In *Mason and Others*,[379] a case determined before RIPA came into force, the Home Office Guidelines were not followed in that normal methods of investigation had not been tried and failed before a covert police surveillance operation was launched, which included listening devices being placed in the police cells of suspects arrested and the home of another suspect. Having heard extensive arguments on this issue (and other issues not relevant to the present analysis) the Court of Appeal held that the judge had exercised his discretion not to exclude the surveillance evidence correctly since he had found that there was no bad faith on the part of the Chief Constable or his officers. This case is also authority for it not being necessary to actually try traditional policing methods and fail before deploying covert policing resource. The court was of the view that it was only necessary to consider conventional policing methods and to ensure reasons could be advanced for ruling them out.

5.191 In *R v Button and Tannahill*,[380] the Court of Appeal dismissed an attempt to reverse a ruling by the trial judge to admit evidence where the form of authority had failed to include visual

[375] [2006] EWCA Crim 6.
[376] ibid, para 20.
[377] (Unreported) 29 January 2002.
[378] *R v Grant* [2005] EWCA Crim LR (Nov). See also Ormerod and Waterman, 'Abusing a Stay for Grant?' [2005] Covert Policing Review 5–14.
[379] [2002] EWCA Crim 385.
[380] [2005] EWCA Crim 516.

as well as audio surveillance by mistake. There was no requirement on the part of the court to exclude evidence obtained in breach of Article 8.

5.192 More recently in *R v Harmes and Crane*[381] a case relating to the use and conduct of undercover police officers as covert human intelligence sources, the Court of Appeal described their actions and the authorization process as being 'serious breaches of the Act and Code'.[382] Despite this the court was, on balance, of the view that 'the officers' conduct viewed as a whole, did not stray beyond that which was permissible to investigate and prosecute crime'.[383]

5.193 These decisions are broadly consistent with the common law position before RIPA came into force[384] and Strasbourg jurisprudence.[385]

G. Other Practical Issues

Observation posts

5.194 The fact that surveillance has been carried out is unlikely to be a fact that will need to be kept from the defence. In *R v Sutherland*,[386] Newman J noted that 'as a general rule, I can see no sound basis for withholding the fact of and content of covert surveillance of a defendant's activities and conversation'. The same can generally be said of non-sensitive parts of the authorities granted.

5.195 However where surveillance is carried out from a static position, in particular residential premises, there may be a requirement to protect both the identity of those who have facilitated this as well as the address, particularly if there is either a threat or perceived threat of violence or harassment.[387] This is so even where the accused says that it goes to his or her innocence, providing the Crown can establish an evidential foundation for it to be admitted.[388] The leading case is *R v Johnson*,[389] which established the following guidance:

> The police officer in charge of the observations to be conducted, no one of lower rank than a sergeant should usually be acceptable for this purpose must be able to testify that beforehand he visited all observation places to be used and ascertained the attitude of the occupiers of premises, not only to the use to be made of them, but to the possible disclosure thereafter of the use made and facts which could lead to identification of the premises thereafter and of the occupiers. He may of course in addition inform the court of difficulties, if any, usually encountered in the particular locality of obtaining assistance from the public.
>
> A police officer of no lower rank than a chief inspector must be able to testify that immediately prior to the trial he visited the places used for observations, the results of which it is proposed to give in evidence, and ascertained whether the occupiers are the same as when the observations took place and whether they are or are not, what the attitude of those occupiers is to the

[381] [2006] EWCA Crim 928.
[382] ibid, para 42.
[383] [2006] EWCA Crim 928, para 54.
[384] See, eg, *R v Jelen* (1989) 90 Cr Ap R 456; *R v Bailey* [1993] 3 All ER 513; *R v Ali* (1991) The Times, 19 February 1991.
[385] See *Khan v The United Kingdom* (2001) 31 EHRR 45 and *PG and JH v The United Kingdom* [2002] Crim LR 308 as just two examples.
[386] (Unreported) 29 January 2002.
[387] *Blake v DPP* (1993) 97 Cr App R 169.
[388] *R v Rankine* [1986] QB 861.
[389] [1988] 1 WLR 1377.

possible disclosure of the use previously made of the premises and of facts which could lead at the trial to identification of premises and occupiers.[390]

5.196 Where the observation post is an unmarked police car the protection is unlikely to be afforded.[391]

Surveillance product and voice identification

5.197 As to the reliance on surveillance product as voice analysis see: *R v Flynn and St John*.[392]

H. The Future of Surveillance

5.198 There needs to be an awakening to the fact that the approach to planning and authorizing of covert surveillance operations as well as the legal audit of them requires more sophistication. This is the responsibility of all the actors involved in the process: police and public authority personnel, lawyers and judges.

5.199 The plethora of reports that have been published over recent years demonstrates that surveillance is a political issue and is likely to be the subject of legislative change in politically temperamental times. Outside of the politics of surveillance there are opportunities for reform and evolution in the areas of overt photography, CCTV and private surveillance.

5.200 The challenges of responding to the activities of increasingly versatile, innovative and resourced criminals and terrorists requires a unified and practical working legal framework within which covert responses can be authorized, reviewed and overseen. At present RIPA does not achieve this. Ferguson and Wadham have opined that 'areas of questionable Convention compliance were identified prior to the enactment of RIPA and subsequent experience of the Act has done little to assuage those concerns'.[393] Fenwick has added her own concerns—'the value of individual privacy is it is argued, consistently and readily overcome, at almost every point in the arrangements at which a choice was made'.[394] It is not necessary to go back to the drawing board but refining the legislation and educating those working in this arena or grappling with its legal consequences is essential.

[390] ibid, 1385–6.
[391] *R v Brown* (1987) 87 Cr App R 52.
[392] [2008] 2 Cr App R 266.
[393] G Ferguson and J Wadham, 'Privacy and Surveillance: A Review of the Regulation of the Investigatory Powers Act 2000' [2003] EHRLR, Special Issue, 101, 108.
[394] H Fenwick, *Civil Liberties and Human Rights*, 3rd edn (Cavendish, 2005) 724.