INVESTIGATORY POWERS TRIBUNAL

Nos. IPT/02/15
IPT/02/23
IPT/02/38
IPT/04/88

Royal Courts of Justice
Strand, London WC2A 2LL

Before:

MR. JUSTICE BURTON
(Vice-President)

MR. PETER SCOTT QC

MR. ROBERT SEABROOK QC

B E T W E E N :

A
B
C
D

Applicants

- and -

METROPOLITAN POLICE SERVICE

Respondent

MR. I. STEELE (instructed by Max Bitel Greene LLP) appeared on behalf of the Applicants.

MISS A. STUDD (instructed by the Director of Legal Services) appeared on behalf of the Respondent.

MR. M. CHAMBERLAIN (instructed by the Treasury Solicitor) appeared as Counsel to the Tribunal.

Hearing date: 2nd November 2006
Judgment published: 29th November 2006

D E C I S I O N

(As approved by the Tribunal)

THE TRIBUNAL:

1 This hearing deals with questions of law arising out of four applications, which have been consolidated by the Tribunal, involving complaints which stem from investigations made by the Metropolitan Police Service ("MPS") into alleged activities by E. All four of the Applicants complain of alleged interception, on the private telecommunication system of the MPS, where E worked, of telephonic communications between E and each of them, during a period which is, for the purpose of this application, from October 2000 until January 2001. The starting point is 2nd October 2000, being the date when the main operative provisions of both the Human Rights Act 1998 ("HRA") and of the Regulation of Investigatory Powers Act 2000 ("RIPA") came into force, as explained by an earlier jurisdictional ruling of this Tribunal, issued on 13th October 2006. The first such complainant, A, makes complaint in respect of alleged interception of communications between E and X, a body of which A is President, the second and third complainants are friends of E and the fourth complainant is his father. The issue of the propriety of any alleged interception of communications so far as concerns E himself is not before this Tribunal, which is dealing only with the complaints by those with whom E had the conversations alleged to have been intercepted.

2 The hearing has been held in public, in accordance with the now well-established practice of this Tribunal to hold, exceptionally, hearings which are not in private (as provided in r.9(6) of the Investigatory Powers Tribunal Rules 2000) where no national security implications are involved, and where it would not be against the public interest on any other ground to hold a public hearing and to publish the Decision, but rather it would be in the public interest that important points of law, dealt with in oral and written argument and in the Tribunal's Decision, should not be kept private. In those circumstances, the Tribunal has made no determination of the facts, and this hearing has been carried out upon the basis of agreed assumed facts. What the real facts are will, or may, be the subject of further examination and findings by the Tribunal hereafter in accordance with its ordinary processes. The assumed facts for the purposes of this hearing are that interceptions on the private telecommunications system of the MPS ("private side intercepts") were carried out for the purpose of intercepting communications relating to, *inter alia*, suspected drugs offences on the part of E. The context of these agreed assumed facts will become clear, but their agreement is for the purpose of resolving the legal issues at this hearing. For this purpose

it would be common ground that, if the private side intercepts were, for example, wholly for the purpose of investigating alleged corruption by E in his capacity as a police officer, or alleged manipulation of expenses in his capacity as a police officer, the same issues would or might not arise. It should also be made clear that any interception of communications on a public telecommunication system is not in issue at this hearing.

3 We have been assisted by the written and oral submissions of counsel for the MPS, Miss Studd, and, for the Applicants, the written submissions of their solicitor, Mr. Keith Jarrett, and the oral submissions at the hearing of Mr. Ian Steele of counsel, and in particular both the parties and ourselves have been greatly assisted by the submissions of Mr. Martin Chamberlain as counsel to the Tribunal.

The law as to private side intercept

4 Criminal liability is not in question in this case, given that any private side intercept was with the consent, indeed at the instance, of the owner/operator of the private telecommunication system, the MPS. Sections 1(2) and (6) of RIPA are the governing provisions in this regard.

5 However, even in the absence of any criminal offence, civil liability in respect of private side intercept can arise. Section 1(3) of RIPA provides as follows:

"Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority and is either—

(a) an interception of that communication in the course of its transmission by means of that private system; or

(b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system."

6 There are four ways in which a party carrying out private side intercept can be protected from civil liability, and these are set out in s.1(5) of RIPA. The fourth of these, contained in ss.(c), is not relevant for the purposes of this hearing and we disregard it:

"(5) Conduct has lawful authority for the purposes of this section if, and only if—

(a) it is authorised by or under s.3 or s.4;
(b) it takes place in accordance with a warrant under s.5 ("an interception warrant"); ...

and conduct (whether or not prohibited by this section) which has lawful authority for the purposes of this section by virtue of paras.(a) or (b) shall also be taken to be lawful for all other purposes."

7 These three routes can be described as the Warrant route (s.5), the Regulations route (s.4(2)) and the Consent route (s.3). It is not suggested in this case that any warrant was sought, and we do not deal further with the Warrant route. The issue in these proceedings was whether the MPS could establish, in respect of the assumed interceptions, the protection of the Regulations route or the Consent route. It was common ground that, if either route can be established, that is not the end of the question for this Tribunal; questions of whether the course taken by the MPS was appropriate or proportionate would still fall to be decided as a matter of fact, but that would be a question for the ordinary processes of this Tribunal hereafter, and not for decision by a hearing such as this in open court. It was common ground that the onus on establishing that one or other of these routes was available for the MPS lay upon them. Further, although this was not conceded until almost the outset of the hearing, it was no longer, if it ever was, contended by the MPS that if they could not establish the protection of either route they had any separate defence by reference to Art.8(2) of the Human Rights Convention, which provides:

"There shall be no interference by a public authority with the exercise of this right [under Art.8(1)] *except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of*

health or morals, or for the protection of the rights and freedoms of others."

It is now accepted that if neither of these two routes is or was available to the MPS, then any alleged private side intercept was not *"in accordance with law"*, such that none of the various protections offered to a public authority in Art.8(2) would be available to them.

8 MPS reserve the right, if unsuccessful at this hearing, to contend in the future that, if they were thus in breach of Art.8 and/or subject to civil liability, that on the facts, and in the circumstances of this case, no loss has been suffered and/or no or minimal compensation should be paid: these issues too will be dealt with in due course, if they arise, by way of the ordinary processes of this Tribunal.

The Regulations Route

9 The Regulations derive from s.4 of RIPA, which provides in material part as follows:

"(2) Subject to subsection (3), the Secretary of State may by regulations authorise any such conduct described in the regulations as appears to him to constitute a legitimate practice reasonably required for the purpose, in connection with the carrying on of any business, of monitoring or keeping a record of –

(a) communications by means of which transactions are entered into in the course of that business; or
(b) other communications relating to that business or taking place in the course of its being carried on.

(3) Nothing in any regulations under subsection (2) shall authorise the interception of any communication except in the course of its transmission using apparatus or services provided by or to the person carrying on the business for use wholly or partly in connection with that business."

10 The grant of this regulatory power arose from Directive 97/66/EC, now superseded by Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002. Article 5 of that Directive reads in material part:

"1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1)…

2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication."

This was in materially the same form both in the earlier and most recent Directive.

11 Article 14(1) of the earlier, and Art.15(1) of the present, Directive make clear that the rights and obligations provided for in those Directives may be curtailed for various purposes, including national security and the prevention and detection of crime. Article 15 reads as follows:

"Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5 … of this Directive when such restriction constitutes a necessary, appropriate, proportionate and temporary measure within a democratic society to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system…"

12 The Regulations consequently enacted are the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("the Regulations"). We set out the whole of the material part of para.3 of the Regulations, as amended by SI 2003/2426 (by the addition of subparagraph 3):

"(1) For the purpose of section 1(5)(a) of the Act, conduct is authorised, subject to paras.(2) and (3) below, if it consists of interception of a communication, in the course of its transmission by

means of a telecommunication system, which is effected by or with the express or implied consent of the system controller for the purpose of —

(a) monitoring or keeping a record of communications —

(i) in order to —

(aa) establish the existence of facts, or

(bb) ascertain compliance with regulatory or self-regulatory practices or procedures which are—

applicable to the system controller in the carrying on of his business or

applicable to another person in the carrying on of his business where that person is supervised by the system controller in respect of those practices or procedures, or

(cc) ascertain or demonstrate the standards which are achieved or ought to be achieved by persons using the system in the course of their duties, or

(ii) in the interests of national security, or

(iii) for the purpose of preventing or detecting crime, or

(iv) for the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system…

(2) Conduct is authorised by para.(1) of this regulation only if —

(a) the interception in question is effected solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the system controller's business;

(b) the telecommunication system in question is provided for use wholly or partly in connection with that business;

(c) the system controller has made all reasonable efforts to inform every person who may use the telecommunication system in question that communications transmitted by means thereof may be intercepted;

...

(3) Conduct falling within para.(1)(a)(i) above is authorised only to the extent that Article 5 of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector(1) so permits."

13 The interpretation paragraph, para.2, is of central significance for the purposes of constructing para.3(2), and subparagraph 2(b) reads as follows:

"a reference to a communication as relevant to a business is a reference to –

(i) a communication –

(aa) by means of which a transaction is entered into in the course of that business, or

(bb) which otherwise relates to that business, or

(ii) a communication which otherwise takes place in the course of the carrying on of that business;"

14 There is an Explanatory Note to the Regulations, which does not appear to us to take the matter much further, save by emphasising that the purpose of the Regulations is indeed to implement the Directive:

"These Regulations authorise certain interceptions of telecommunication communications which would otherwise be prohibited by s.1 of the Regulation of Investigatory Powers Act 2000. To the extent that the interceptions are also prohibited by Art.5.1 of Directive 97/66/EC [the then current Directive]*, the authorisation does not exceed that permitted by Arts.5.2 and 14.1 of the Directive.*

The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government

departments, public authorities and others exercising statutory functions) for purposes relevant to that person's business and using that business's own telecommunication system."

15 The fact that the Regulation route is available only if the interceptions are *"solely"* for the permitted purpose referred to in Reg.3(2)(a) is what has led to the formulation of the assumed facts in this case (see para.2 above), the issue being whether the Tribunal concludes that private side intercepts which were at least in part for the purpose referred to in the assumed facts would fall within the Regulations.

16 The MPS contend that private side intercept for such purpose, that is to investigate alleged drug offences said to involve a serving police officer, would indeed be within the Regulations. There are, as appears from the interception para.2(b), three ways in which an interception can be for the purpose of *"monitoring … communications relevant to the system controller's business"* within para.3(2)(a). By para.2(b)(i)(aa) a communication can be relevant to a business if it is a communication *"by means of which a transaction is entered into in the course of that business"*. It is not suggested that such an issue arises in this case. That leaves two respects in which, by statutory definition, a communication can be *relevant to a business* (in this case of course being the business as defined in para.2(a) of the Regulations, namely *"activities of a government department, of any public authority or of any person or officeholder on who functions are conferred by or under any enactment*").

17 Miss Studd relied upon the third such limb, namely *"a communication which otherwise takes place in the course of the carrying on of that business"*. She submitted that if the communication did not fall within the second limb, namely as being a communication *"which otherwise relates to that business"*, then, because the third limb is described as *"a communication which <u>otherwise</u> takes place in the course of the carrying on of that business"*, the use of the word *"otherwise"*, in the definition of the third limb, must mean that the communication in question does <u>not</u> relate to the business. Thus it is *"a communication which* [does not relate to that business but] *takes place in the course of the carrying on of that business"*. It is here that she takes issue with the submission, to which we will refer below, put forward by Mr. Chamberlain as counsel to the Tribunal, that the phrase *"in the course of the carrying on of that business"* means the

same as, or similar to, *"in the course of that business"*, to be defined by reference to the authorities in the tortuous context on *"in the course of employment"* [e.g. **Harrison v. Michelin Tyre Co Limited** [1985] ICR 696]. If, Miss Studd submits, the communication is *in the course of the business*, by reference to such a definition as is put forward by Mr. Chamberlain, it is difficult to see how anything failing within such concept will not also be held to be *relevant to* [that] *business:* whereas in this case a communication must be identified which is not relevant to the business and yet is *"in the course of the carrying on of that business"*. Miss Studd submits that this can only relate to a communication which is irrelevant to the business, and yet is made in business hours, or at any rate from the business premises. Her argument could be further supported by reference to the statute itself, when with regard to ss.3(2)(b) it could be said that an even clearer dichotomy appears there between *"relating to that business"* and *"taking place in the course of its being carried on".*

18 Miss Studd did not rely on the availability of the second limb. The Tribunal however put to Miss Studd that the second limb might, on her contention, also be available to her, and she adopted that case. The case would be that, in relation to what is here the business of a police force, a communication by a serving officer, on a police system, relating to matters, namely the potential commission of drugs offences, which it would ordinarily be the very business of the police to prevent, might be said to be *to be a communication which relates to that business.*

19 Mr. Chamberlain in his written submissions opposed the width of construction of the Regulations for which Miss Studd then contended (and a fortiori the contention for which, by adoption of the argument relating also to the second limb she now contends): and Mr Steele for the complainants supports and adopts those written submissions by Mr. Chamberlain. Mr. Chamberlain reminded us of the context in which regulation of interception of communication arose. So far as public intercept is concerned, this derives from the decision of the European Court in **Malone v. UK** [1984] 7 EHRR 14, which concluded that since as previously found by Megarry VC in **Malone v. Metropolitan Police Commissioner** [1979] CH 344, telephone tapping could be carried out in the UK without any breach of the law, and requiring no authorisation by statute or common law, that very

absence of regulation meant that any such interference was not *"in accordance with law"*, so as to be justified within Art.8(2); and the Interception of Communications Act 1985 ("the 1985 Act") was consequently enacted relating to public intercept. A similar series of events occurred by reference to **Halford v. UK** [1997] 24 HER 523, in relation to the absence of regulation by domestic law of private side intercept, rendering any defence under Art.8(2) unavailable, which prompted the enactment of RIPA, the statutory regime now covering private side intercept. Against that background, he submitted that there are significant features of the Regulations which, as he pointed out in para.17 of his written submissions, could have used plain words to make clear, but did not, that:

- interception of all communications on a private telecommunication system, or all communications on such a system made during working hours, is authorised, or

- all interceptions whose purpose is the prevention or detection of crime are authorised – as opposed to the imposition of the additional requirement that the interception in question is effected *"solely for the purpose of monitoring ... communications relevant to the system controller's business".*

20 He then set out his critique of Miss Studd's case. Relying, as he did, on the *"course of employment"* analogy, which he submitted gave a restrictive interpretation to the third limb, he gave, in paras.21 and 22 of his submissions of 27th October what he called two reasons which suggested that Miss Studd's contention could not be correct:

"21. <u>First</u> if it were [correct], *then the Regulations would authorise interception of <u>every</u> call made by an employee on the private telecommunication of his employer, save for those made outside working hours. If that was the intention, it is hard to see why the legislator adopted the complicated formulation in Reg.2(b). Indeed if the MPS construction were correct there would have been no need for any definition of 'relevant to business' at all. Regulation 3(2)(a) could simply have referred to 'communications made during working hours'.*

"22. <u>Secondly</u>, the MPS construction involves giving the concept of the communication made 'in the course of business' in Reg.(2)(b)(i)(aa)

(which applies not to all transactions, but only those made 'in the course of that business') a meaning which differs from that in Reg.2(b)(ii) (which covers communications which takes place 'in the course of carrying on that business'. If the 'course of business' means 'working hours' in the latter case, why should it not bear the same meaning in the former. It could not mean 'working hours' in Reg.(2)(b)(i)(aa) (since, otherwise, it could cover purely personal transactions, such as the case where the employer[sic] *purchases train tickets or opera tickets on his employer's telephone), so there is no reason to suppose that it has that meaning in Reg.2(b)(ii) either."*

21 However, by way of second and further thoughts, Mr Chamberlain produced, at the outset of the hearing, some further well researched submissions by reference to the Directive, which caused him to conclude that *"relevant to the system controller's business"* might well have a wider meaning in this context, contrary to his initial submissions. He referred not only to the obvious fact that the Regulations arose out of the Directive, and to the Explanatory Note above, but to the words of the then Minister, Lord Bassam, in the House of Lords, reported in Hansard on 17th June 2000 (613HL Official Report 1425), when introducing the Bill which subsequently became RIPA, when he said that the extension of the 1985 Act by the Bill *"seeks to implement the requirement of Art.5 of the European Telecommunications Directive"*.

22 He points out that there are two strands in the Directive. The first is that referred to in Art.5 of the Directive (with the caveat in Art.5(2)), which leads primarily to the provisions of para.3(1)(a)(i) of the Regulations, with regard to business communications, which not only of itself echoes the provisions of Art.5, but is further strengthened by the cross-reference in para.5(3) whereby, as set out above *"conduct falling within para.1(a)(i) above is authorised only to the extent that Art.5 of the Directive ... permits"*.

23 He submits that subparagraphs (a)(ii) [national security], (a)(iii) [preventing or detecting crime] and (c)(iv) [investigating or detecting the unauthorised use of that or any other telecommunication system] reflect the expressly permissive provisions of Art.15(1) of the Directive referred to above. Particularly given the inclusion in such permitted purposes of monitoring of <u>unauthorised</u> use of a system, he accepts that it may well be, notwithstanding what he pointed out about

the fact that the Regulations could so easily have been less opaque or apparently restrictive, that either the words *"relevant to the ... business"* in the domestic Regulations may have a different meaning depending on the purpose for which the interpretation is effected or, in any event, *"relevant to the ... business"* may have a wider meaning than he had previously contended, and in any event may well go wider than the business related communications which otherwise fall within Art.5, provided that one of the purposes in Art.15(1) is established.

24 It can be seen that issue is joined in relation to the Regulations route, as to whether the MPS can or cannot take advantage of that route by reference to para.3(2)(a), and we have not had the benefit in this case, as we did in **C v. The Police** (IPT/03/32) of submissions from counsel instructed by the Treasury Solicitor on behalf of the Secretary of State for the Home Department.

25 There is, however, before the MPS can avail itself of the Regulation route, the need for it not only to establish that para.3(3)(a) is satisfied, but also that the other subparagraphs, of which for our purposes the relevant one is subparagraph 3(2)(c), are similarly so satisfied.

26 This latter subparagraph requires, as set out in para.12 above, that MPS must show that it has *"made all reasonable efforts to inform every person who may use the telecommunications system in question that communications transmitted by means thereof may be intercepted"*. The question of whether this condition was satisfied was raised by Mr. Jarrett on behalf of the Applicants for the first time in their submissions of 20th September 2006, and provision was made in the Tribunal's Directions Order of 16th October that it should be dealt with by MPS. Their response was to concede that, in relation to the material period, October 2000 to January 2001, MPS could not show that they had complied with para.3(2)(c), such that they could not satisfy the requirements of para.3(2), and in those circumstances could not avail themselves of the Regulations route.

27 This meant that any decision, or even expression of view by this Tribunal, would be obiter; and would be obiter in circumstances in which (i) as set out above, we would have had the benefit of argument, as we might well wish to have in a case in which the resolution of such point would be determinative, from the Secretary of State, as repository of the legislation; (ii) the arguments by reference

to the Directive have not been fully developed before us, and in particular counsel for the Applicants has been in no position to deal with them. After discussion with counsel at the outset of the hearing, it was agreed that the issues would merely be canvassed before us and that, given that MPS have now conceded the unavailability of the Regulations route, we should not reach a decision on the point, nor express any provisional view. The Applicants accepted, through counsel, that resolution, either way, of such point could have no impact on the quantification of compensation, and the MPS also did not invite us to give any decision, so that they could consider further the implications of the arguments that had been put, in case the matter arose in the future.

The Consent Route

28 Section 3 of RIPA reads in material part as follows:

"(1) Conduct by any person consisting in the interception of a communication is authorised by this section if the communication is one which, or which that person has reasonable grounds for believing, is both —

(a) a communication sent by a person who has consented to the interception; and

(b) a communication the intended recipient of which has so consented.

(2) Conduct by any person consisting in the interception of a communication is authorised by this section if —

(a) the communication is one sent by, or intended for, a person who has consented to the interception; and

(b) surveillance by means of that interception has been authorised under Part II."

29 The reference to Part II is to the statutory provisions relating to the system of authorisation of surveillance commencing in paras.26-30 of RIPA. Section 48(4) makes it clear that surveillance, which for the purposes of RIPA generally does not normally include interception,

does for the purposes of Part II *"include references to the interception of a communication in the course of its transmission by means of a … telecommunications system"*, if it is a situation falling within s.3. There were, as had been disclosed by the MPS as attachments to its written submissions of 23rd October 2006, three authorisations each of which was an *"Application for Interception of Communications Conveyed on a Private Telecommunications System"*, seeking *"authority for Private Side Interception of the telephones used by* [E]", successively on 25th September, 18th October and 21st December 2000; to which applications authorisations were in each case given. Such authorisations differ from a warrant under s.5, not only because the statutory requirements are different, with which for these purposes we do not need to concern ourselves, but also because authorisation is given, not by the Secretary of State as with a warrant, but by one of those persons entitled to grant authorisations under s.28 and s.29, as specified pursuant to s.30 of RIPA.

30 Section 3(1) does not of course apply in this case, as the four complainants are not asserted to have given any such consent: it is a subsection which applies only in the case where both parties to the communication have consented. It is s.3(2) upon which MPS relies. They do not of course rely on an express consent in respect of the particular interception. There was some exchange of submissions in the course of the hearing in this regard, but it is clear to us that it cannot have been intended or required, in the context of interception, and of the purposes for which lawful interception is permitted, that there must be a particular express consent in relation to each such occasion of interception. The MPS rely upon what can be called "generic consent".

31 As Miss Studd submitted, the best way to establish the giving of such generic consent by someone in the position of E, using his employer's telecommunication system, would be to point to an express term in a contract of employment, setting out an employee's consent to the fact that such communications would or may be the subject of interception. Of course the Police are not employees, but, in their position as quasi employees, there would no doubt be capable of being drafted and agreed, by way of analogy with incorporation into a contract of employment, a set of Conditions of Service to similar effect. We have been told that many Notices are regularly distributed to police officers. Such Notices, in very clear terms, putting police

officers on notice that their communications may be monitored or recorded, were within our papers, although they seem to have post-dated the period which is relevant to us. However, during the hearing a yet earlier similar Notice was produced (emphasising that such a Notice has been issued to the Police on a regular basis) which seems to have been the form of it relevant at the time, having been issued on 16th June 1999 as Police Notice 24 of 99. This reads as follows:

"Expectation of Privacy

"If the person making communications is fully aware that monitoring or tape recording of communications may take place, then their expectation of privacy can, in principle, no longer exist. Accordingly, the following warning is issued:

"You work within an organisation which deals with sensitive matters. Your job requires you to maintain high professional and ethical standards. In order to ensure that these sensitivities and high standards are maintained by all employees, telephone conversations, fax, modem and e-mail transmissions may be recorded or monitored.

"All officers, civil staff and contract employees are therefore reminded that their conversations and communications using the aforementioned Metropolitan Police Service facilities may not be private.

"The Metropolitan Police Service is emphatic in its determination that integrity is and will remain non-negotiable. In so saying, should it be deemed appropriate, recorded communications will be used in criminal and/or discipline proceedings.

"Monitoring of the type described will be used only where necessary and the level of intrusion will be proportional to the issue being investigated and/or evaluated for compliance with professional standards. Interception will be considered on an individual basis as to whether it is the appropriate method of investigation and monitoring. The authority to monitor internal communication within the Metropolitan Police Service will be given by the Deputy Commissioner or Association of Chief Police Officers [or] *officers nominated by him."*

32 Although there is not any document such as we could have expected which establishes the status, or the effect on police officers, of the content of such Notices, whether read or not, similar to the incorporation into a contract of employment if a police officer were employed, there is a paragraph apparently from a 1998 booklet or manual called "Service Conditions", which Miss Studd described as the "Police Instruction Manual", which reads as follows:

"9. Service Orders and Instructions

"9.1Copies of Notices and Service manuals are supplied to all sections of the Service. They are instructions and are to be complied with by all ranks. The contents are not to be disclosed to any person outside the police service."

A similar clause appeared in the 1992 Manual, a copy of which was subsequent to the hearing supplied to us by the Applicants.

33 The only other document upon which the MPS relied during the hearing was the copy of the Police Regulations 1999 which, by para.21, imposed upon every member of the police force an obligation to carry out all lawful orders.

34 If we were satisfied in the ordinary case that a Notice of this kind was automatically incorporated into the contract of employment of an employee, under which we were then satisfied he continued to be employed, we would have little doubt in concluding that there was thereby consent to such interception as consequently took place. Whatever the status of the "Police Instruction Manual", we are told by Mr. Steele that his instructions are that E had no knowledge of it. In the absence of such a provision or quasi-contractual mechanism, then we would need to consider the issue in relation to the particular party, here E. In an everyday case, by reference for example to someone who listens to a recorded message at the outset of a telephone call, which informs him or her that, if he proceeds with that call, it may be recorded, then by the carrying on with that call it seems to us that that person would be consenting to the risk of interception. If someone is told that if he or she acts in a certain way, there are the following consequences, then it appears to us trite that, if that person then so acts, he or she is consenting to the consequences. We are not persuaded by Mr. Steele's submission that the absence in s.3(2) of

RIPA of the words *"express or implied"* in relation to consent which are included in a different context in s.1(3) makes any difference: if anything s.1(3) emphasises that consent can indeed by either express or implied.

35 It would, in our judgment, simply need to be shown to the satisfaction of the Tribunal that E, when he used the telephone system of the MPS, had, as it would inevitably seem likely that he had as a senior officer, knowledge of the contents of these particular Notices relating to the risk of recording of calls. However such is not accepted by Mr. Steele on E's behalf, who makes the submission that there were many such Notices, and that it should not be assumed as against his client, even as a senior officer, that he should know of, never mind acquiesce in, the contents of every such Notice, particularly if it cannot be shown that it is likely that such Notice in fact reached all officers, although he apparently accepts that the Notices were published on an internal website or intranet. Mr. Chamberlain reminded us that, as the giving of consent could amount to a waiver of Art.8 rights, we would need to be careful in concluding that there was consent. However it seemed clear to us that in the resolution of this factual issue E, as such a senior officer, might well have credibility problems if he asserted a lack of knowledge that the telephone system might be intercepted. Nevertheless, we remained of the view at the conclusion of the hearing that we could not resolve that issue without carrying out some enquiry so as to arrive at a factual conclusion, which could not be carried out at the hearing (see para.2 above).

36 Our scepticism as to the chance of a successful outcome for E in the resolution of such factual issue has only been fortified by what has been produced by MPS subsequent to the hearing. They have belatedly supplied apparent transcripts of recorded conversations by E with others, including of the Applicants, in which E is apparently recorded as fully appreciating, and on occasion indicating to the other party to the conversation, that the telephone line of which they are speaking was not "secure", and may be monitored.

37 However, once again, irrespective of the above, more than one question is involved in the determination of the availability of the Consent route.

38 The further provision, which again the MPS must satisfy in addition to that of consent under s.3(2)(a) is that *"surveillance by means of that interception has been authorised under Part II"*. In this context, we return to a fuller consideration of the interpretation section for Part II under s.48(4) which provides:

"References in this Part to surveillance include references to the interception of a communication in the course of its transmission by a … telecommunication system if <u>*and only if*</u> [our underlining]:

> *(a) the communication is one sent by … a person who has consented to the interception of communications sent by … him."*

39 We have indicated that there have been produced by the MPS the three applications for authorisations, all of which are in materially the same form. They all refer – and refer only – to the <u>Regulations</u>, a matter to which Mr. Chamberlain has drawn attention: but that would not, it seems to us, of itself invalidate reliance on the authorisations for the purposes of s.3(2)(b), not least because there is in fact no provision in the Regulations for the obtaining of any such authorisations, as we have seen.

40 But the matter which has caused us considerable concern is that the authorisations specifically recite that: *"No party to the monitoring and recording consents. Therefore, authority from an officer of the rank of Assistant Commissioner is sought to initiate the PSI request".* It is not simply the fact that the making of such a statement is completely contrary to the basis of the case now put forward by the MPS before us, in reliance on s.3(2)(a), that E did consent. Difficult as it might be, no doubt if it became clear that E did not know of the Notices referred to above and thereby acquiesced in and consented to the likelihood of interception, such a mistaken statement could be overridden. But the problem we have is that it is totally clear that the authorisations were sought <u>on the basis that</u> there was not such consent, i.e. (particularly bearing in mind the passage in s.48(4) underlined by us in para.36 above) that this was not consent sought under s.3(2) of RIPA. If all the facts were in place, then it may be that we could conclude that, even if the parties did not express themselves correctly, all the necessary premises for the operation of s.3 were in fact established. But reasonable belief in the consent of a party,

sufficient for s.3(1), is not sufficient for s.3(2), where consent itself must be found; and in this case there could not even have been such reasonable belief, given the express statement to the contrary in the application for authorisation. A fortiori, and particularly in the light of the still unresolved factual dispute to which we have referred above, there can be no question of there having been satisfaction on the part of the authoriser under s.30 of RIPA that E had consented, when he was told expressly that E had not consented. The authoriser under Part II was in fact bound to refuse his authorisation when informed that the communication to be intercepted was not one *"sent by, or intended for, a person who* [had] *consented to"* it.

41 In those circumstances, we are quite unable to find that there was an authorisation under Part II of RIPA, such that s.3(2)(b), and thus s.3, of RIPA is not satisfied. Hence, without our making, or needing to make, at this stage any finding in relation to the matters set out in paras.31-36 above, the Consent route is in any event also not available to the MPS.

42 Our conclusion therefore is that there was no lawful ground for the assumed private side intercepts of communications involving these Claimants, if they occurred. We shall now proceed, following what we have referred to above as the usual processes of this Tribunal, to consider: (i) whether any such private side intercepts took place; (ii) if they did, there being no lawful justification for them, what if any compensation should be awarded to the Applicants. It will be open, as we have canvassed with the parties, for the MPS to assert, and for the Claimants in any further written submissions to deny, that the availability or question of such compensation could or would be affected by the fact, if such be the case, that a lawful route to the intercepts could have been properly taken. We shall also consider at that stage the questions of proportionality and appropriateness to which we have referred above.

_____